An Inclusive and Scalable Crypto Economy

Blockchain for Green and Sustainable Economic Growth

Nikoletta Matsur

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisor: Prof. Catherine Ellen Anne Mulligan

Examination Committee

Chairperson: Prof. Alberto Manuel Rodrigues da Silva
Supervisor: Prof. Catherine Ellen Anne Mulligan
Member of the Committee: Prof. William Knottenbelt

November 2022

This work was created using LaTeX typesetting language
in the Overleaf environment (www.overleaf.com).

Acknowledgments

I would like to thank my supervisor, prof. Catherine Mulligan, for encouraging my development in research, for bringing fascinating subjects to our meetings, putting me in touch with several experts, and sharing invaluable knowledge on economic matters. I would also like to thank prof. Kevin Gallagher, prof. Alfio Puglisi, for being present in multiple meetings and helping to organize my ideas. I would like to thank my mother Vita and father Mykolai for being endless sources of inspiration and life models. I would like to thank Multicert for the support. Thanks to everyone who gave me encouraging words, and never stopped believing in me. And thanks to the good people in the XRPL discord, who always have time for their community.

Abstract

Small scale is characteristic to most complementary currencies (CCs) and the reason for their success and failure simultaneously. While it isolates communities from external economic conditions in periods of high inflation or recessions, it contributes to the short life of the currency and leads to marginal economic impact. In turn, it becomes unviable to prove their efficiency, which hampers the economic and interdisciplinary research. Therefore, scale is a fundamental problem of complementary currencies such as mutual credit and private money that emerges by design and is not being addressed. Instead of segregating the economy members, we propose to onboard the maximum amount of users when designing complementary currencies by employing the most relevant and versatile use cases that comprise monetary transactions. Inspired by the fidelity points of large companies, which are commonly not thought of as complementary currencies, and have a longer life, we design and develop a credit network based on blockchain where each individual or organization can issue their own money tailored to specific use cases such as salary payments, debt registering, fundraising, donations, gift cards and fidelity points, creating a market of interoperable currencies and leveraging trust connections in a community. By encompassing a significant variety of IOU use cases, more opportunities for users arise in the credit network, increasing the scale of the complementary currencies' network, potentially leading to significant economic impact.

Keywords

Complementary Currencies, Cryptocurrency, Blockchain, Credit Network, Debt Clearing, Mutual Credit

Resumo

A pequena escala é característica da maioria das moedas complementares (CCs) e, simultaneamente, a razão do seu sucesso e fracasso. Embora seja o que isola as comunidades das condições económicas externas em períodos de alta inflação ou recessões, contribui para a curta vida da moeda e leva a um impacto económico insignificante. Desta forma, torna-se inviável comprovar a sua eficiência, dificultando a pesquisa interdisciplinar e na área de economia. Portanto, a escala é o problema fundamental de moedas complementares, como crédito mútuo e dinheiro privado, que surgem por natureza e não estão a ser abordados. Em vez de segregar os membros da economia, propomos incorporar a quantidade máxima de utilizadores ao projetar moedas complementares, empregando os casos de uso mais relevantes e versáteis que compreendem transações monetárias. Tirando inspiração nos pontos de fidelidade das grandes empresas, que comummente não são vistos como moedas complementares, e com vida útil mais longa, projetamos e desenvolvemos uma rede de crédito baseada em blockchain onde cada indivíduo ou organização pode emitir o seu próprio dinheiro, para casos de uso específicos como pagamento de salários, registo de dívidas, angariação de fundos, doações, cartões-presente e pontos de fidelidade, criando um mercado de moedas interoperáveis e estimulando conexões de confiança numa comunidade. Ao abranger uma variedade significativa de casos de uso de dívida, surgem mais oportunidades para os utilizadores na rede de crédito, aumentando a escala da rede de moedas complementares, levando, potencialmente, a um impacto económico mais significativo.

Palavras Chave

Moedas Complementares, Criptomoedas, Blockchain, Redes de Crédito, Compensação de Dívida, Crédito Mútuo

Contents

List of Figures

List of Tables

Listings

Acronyms

AMM	Automated Market Maker
BFS	Breadth First Search
BFT	Byzantine Fault Tolerance
BoLT	Building On Local Trust
CAP	Consistency, Availability, Partition Tolerance
CC	Complementary Currency
CLi	Command Line Interface
CN	Credit Network
CPU	Central Processing Unit
CRDT	Conflict-free Replicated Data Type
CS	Computer Science
CSE	Computer Science and Engineering
DAO	Decentralized Autonomous Organization
dApp	Decentralized Application
DEX	Decentralized Exchange
DCN	Decentralized Credit Networks
DHKE	Diffie-Hellman Key Exchange
DLT	Distributed Ledger Technology
EdDSA	Edwards-Curve Digital Signature Algorithm
FBA	Federated Byzantine Agreement
ICO	Initial Coin Offering
Intel SGX	Intel Software Guard Extensions
IOU	I Owe You

IPFS	InterPlanetary File System
LETS	Local Exchange Trading Systems
MC	Mutual Credit
NFT	Non-Fungible Token
ORAM	Oblivious RAM
P2P	Peer-to-Peer
PBT	Path-Based Fund Transfer
PCN	Payment Channel Network
PGP	Pretty Good Privacy
PoW	Proof of Work
RPC	Remote Procedure Call
SDK	Software Development Kit
SLA	Service Level Agreement
SLR	Systematic Literature Review
SME	Small or Medium Enterprise
SMT	Sparse Merkle Tree
SPV	Simplified Payment Verification
SCP	Stellar Consensus Protocol
TAD	Topological Anomaly Detection
TDA	Topological Data Analysis
TEE	Trused Execution Environment
TPS	Transactions per Second
UNL	Unique Node List
URE	Universal Re-Encryption
WIR	Wirtschaftsring-Genossenschaft
XRPL	XRP Ledger

1

Introduction

Contents

1.1 Motivation

Complementary Currency (CC)s have been used to solve liquidity problems during economic downturns. Their main purpose was to serve as a means of exchange in periods of high inflation, in which the supply of fiat money in a community is insufficient, but the need for goods and services as well as their availability prevails. The failure of fiat currencies may be a result of assigning multiple incompatible functions to its role of medium of exchange, as is further discussed in this study. When the role of exchange medium was not being fulfilled, fictional money filled the gap. Thus, the economy did not have to stop as trades could proceed with an alternative currency that circulated in parallel to fiat currency, until a supply of had fiat money was re-established. In some cases (e.g. WIR), CCs are believed to be the reason for the nation's economic stability, whereas in other cases, they end up falling into disuse and disappear shortly after the recession. Typically, CCs that emerged during economic downturns and fixed the medium of exchange problem, were used by SMEs, who, despite being considered key elements for economic growth, are the least likely to get financial support from banks, mainly due to the opaque nature of their projects and finances (information asymmetry). Thus, without a wide range of funding options, SMEs are the most vulnerable to economic downturns. Since SMEs represent the vast majority of most economies worldwide, the economy spirals during recessions, taking more time to recover and decreasing the population's welfare. The CCs are a fair starting point for increasing the liquidity in a community, including SMEs.

1.2 Addressed Problems

Since most complementary currencies usually isolate groups to protect them from external shocks, their impact on the economy is marginal, as discovered in 2. It means that by design, complementary currencies are small-scale hence their impact on economic development cannot be confirmed, leading to less interest from economists, less experimentation, less innovation, which in turn, leaves the state of the art in complementary currencies as is, making the field stagnant. This issue is currently not being addressed in economic or computer science literatures.

We address the problem of complementary currency scalability in the following way: instead of protecting the most vulnerable users by creating a smaller economy within the economy, we try to onboard the maximum amount of users in the complementary currency network by enabling several use cases with fictional money, issued by any user. To increase the potential for economic impact, we chose use cases as main incentives for users to join the network. Users may be individuals, big, small and medium enterprises, charity organizations, communities, etc. We want to cause the fewest possible restrictions in regard to the use cases in the network of interoperable personal complementary currencies. However, some constrains must exist to guarantee user's economic and technological safety.

On the other hand, cryptocurrencies are being analysed for the suitability of complementary currency roles and emerging as open, shared, decentralized, digital currencies. However, due to the characteristic volatility, cybersecurity attacks, price manipulation, cryptocurrencies have been deemed unsuitable for a reliable complementary currency. However, mutual credit-like system started emerging with blockchain. This means that not all cryptocurrencies are subject to price manipulation, especially if the supply is elastic. We explore these unusual blockchains, compare and choose one to help us to develop our solution.

1.3 Objectives

The goal of this project is to advance the state of the art in the field of complementary currencies. In order to arrive to a robust solution, the following objectives must be met:

1. Understand the main concepts, and state of the art of CCs in interdisciplinary research
2. Understand the state of the art of CCs development in CSE literature
3. Understand if the main problems of item 1 are being addressed in 2.
4. Design a solution to address the most urgent and important issue found in the literature
5. Implement the requirements of the solution
6. Develop tests and a simulation of the solution

1.4 Document Organization

This remainder of this dissertation is organized as follows. Chapter 2 presents the Systematic Literature Review (SLR) of complementary currencies and cryptocurrencies for economic impact, including the purpose, methodology, research protocol, results, findings, discussions and indicates future research directions. In this chapter, key issues emerge to be addressed in the next chapters, and are decided in the conclusion based on the importance, urgency and current state of research on the same issue. Chapter 3 presents an overview of the solution to the issue chosen in the previous chapter: the use cases are exemplified, as well as the benefits and system's functional and non-functional requirements. Chapter 4 starts by giving a general context of blockchain, to then contrast it with blockchains and other Distributed Ledger Technology (DLT) that were built specifically for complementary currencies rather than cryptocurrencies. The chapter proceeds to compare the different technologies and choose one to develop the designed solution. In chapter 5, the testing of the solution is explained, and a simulation is described with the results. Chapter 6 summarized the main findings and the trajectory of this study, enumerating contributions and suggests future work directions.

2

Systematic Literature Review

Contents

In this section, the process and results of searching and reviewing the existing literature on complementary currencies and economic growth are reported, as well as the reason for researching this topic. Furthermore, the main steps of the chosen methods and frameworks for conducting and reporting the review are summarized, and their suitability justified for this study in particular.

2.1 Introduction

Purpose. Since CCs constitute an old practice, the conducted research aimed at performing an inspection of the successes and failures of complementary currencies, differentiation of their types, identification of main innovations, and an assessment of the role cryptocurrencies and blockchain currently play, or their potential, in supporting the creation of private money and CCs. The study spreads across several multidisciplinary fields, however, the interdisciplinary research on CCs and blockchain is limited, which can be explained by the recent emergence of the technology. Interestingly, the research of CCs in economics is also limited, but for a specific reason found in literature and further discussed. Despite this, a general level of understanding of the complementary currencies' field is necessary before inspecting present day innovations, and especially gaps of CCs and blockchain. To better equip ourselves and the reader to understand how CCs stand in the real world and research state-of-the-art on technology, the study is divided in two parts: the **context** of CCs in the real world and the research of CCs and **blockchain** or **DLTs**. The former allows for a broad understanding of the main concepts, types, features, experiences, and mechanisms of CCs, coming mainly from economic literature, while the latter allows to focus on a particular research direction from the CSE literature to solve a key aspected that emerged during the exploratory research of CC's context. In the context, a niche from the real world worth pursuing is discovered and used to produce the research questions to explore the state of the art in CSE of that niche — its projects, challenges, and innovations. From this point, it becomes possible to start building a solution to contribute and advance the state of the art. Not all problems can nor should be solved at once. Hence, the most impactful, beneficial and critical issues should be chosen. And this can only be achieved with context — the exploratory search in other disciplines. Without the context, there would be no reliable bridge between real-world CCs' shortcomings and the technological solutions, as research is limited. Thus, no confidence that the problems being solved are the most priority, urgent and relevant would exist. In the domain of CCs and blockchain, research cannot be local to CSE fields, nor it should be in any area that causes such magnitude of impact. A strategy was employed to achieve the research goals in a reasonable amount of time despite the necessary search in multiple fields' literature, discussed in methodology.

SLR. Other types of literature reviews exist (*e.g.* scoping reviews, "state-of-the-art" reviews, *etc.*), but this study applies the SLR methodology. A "systematic review is essentially a tool; hence, one needs to ask whether it is right for a given job" [1]. The difference between a SLR and other types of literature reviews revolve around rigour and the amount of effort necessary to accomplish it: one “practical consideration is whether one can justify the amount of time, energy, and financial cost required” [1]; “certainly not easy to undertake, the commitment to complete a standalone review provides the academic community a valuable service: such reviews can, and have in the past, been true “paradigm shifters”” [1]. In other words, “most scholars conduct literature reviews primarily for their own learning and benefit, a published review primarily benefits the scholarly community” [1]. A SLR shouldn’t be expected in any academic paper, but it is highly valuable when published standalone: “its best form, it becomes a much cited piece of work that researchers seek out as a first clear outline of the literature when undertaking a new investigation” [1]. Moreover, “a SLR is quite appropriate for the literature review chapter of a graduate thesis” [1]. The learning benefits collected from a comprehensive and rigorous examination and the potential to impact the research stream of complementary currencies constitute the main drivers for this study. But, since “science is not ”value free”” [2], it is important to note that contributing with knowledge of technology for CCs to foster economic growth impacts and can potentially better over a million lives across the European Union as well as increase businesses’ and countries’ development.

Previous SLRs. To the best of our knowledge, no systematic literature reviews were performed on complementary currencies for economic growth with a quantitative analysis of cryptocurrencies and special attention on innovations (i.e., blockchain, cryptocurrencies), which makes this report a relevant contribution — one more motivation to invest time and effort on a systematic literature review. The most similar study ([3]) found is from 2015. [3] review studies until 2013 and is not related to blockchain nor cryptocurrencies.

Outcomes. With this study, we were able to plan the next steps for employing blockchain to solve a key issue that CCs face, develop new mechanisms that can be enabled by this technology, and pave the way for future research. Although social currencies and time currencies are fundamental for the community development and reduction of inequalities, the focus is on businesses as those are the main drivers for economic outcomes, such as economic growth and stability, *i.e.*, our subjects of interest and ultimate goal of this project. This report is not a compilation of different complementary currency systems that exist or have existed, nor it is a comparative analysis of CCs, even though examples of currencies whose functioning, implementation choices, challenges, innovations, or outcomes are relevant findings are mentioned.

Structure. After introducing (2.1) the study topic, its purpose and goals, the methodology is explained (2.2), search protocols of both parts (context and technological research on **CCs!**) are exposed (A), followed by the results of the search (A.2) where the reasons for rejections are clarified. The findings (2.3) present the lessons extracted from the literature, which are discussed in discussion (2.4). Finally, limitations are identified (2.5), and future research directions proposed (2.6). The conclusion (2.7) summarized the trajectory of the carried study and the most relevant points discovered for this dissertation.

2.2 Methodology

This report applies *A Guide to Conducting a Standalone Systematic Literature Review*, [1], which advises that “a systematic review is not very valuable early on when limited studies might be available because they might not represent the best knowledge that more time might give” [1]. Since research focusing on the application of CCs using blockchain in the field of Computer Science (CS) is scarce, other disciplines were also searched, which divides the structure of this report in two: the CC’s context research and technology research, both follow the SLR methodology.

A Guide to Conducting a Standalone Systematic Literature Review, was compiled to address the need for the “rigorous, standardized methodology for the systematic literature review” [1] similar to the ones in health sciences, it is “particularly tailored [but not limited to] for the diverse needs of information systems research”. This guide is for “literature reviews that set the theoretical background for a work of primary research or for a graduate student thesis” [1], which makes it suitable for this report. It comprises an eight-step guide to perform a rigorous SLR - “a systematic, explicit, [comprehensive,] and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners” [1]. *Systematic* implies “following a methodological approach” [1], *explicit* means “explaining the procedures by which it was conducted” [1], and *comprehensive* relates to the scope of the review and “including all relevant material” [1]. These attributes help to achieve the *reproducibility* of the review by other researchers, which contributes to the credibility, thus increasing the probability of being reused in other research. The more comprehensive and explicit the review is, the more reproducible it may be, and the systematicness is a means to reach this goal. The eight step taken are as follows. (1) Identification of the purpose (2.1), (2) drafting of the protocol, (3) searching with inclusion and exclusion criteria, (4) performing the screening, (5) extracting the main points, (6) appraising quality, (7) synthesizing studies, and (8) writing the review (8).

To reduce the considerable amount of time a review in economics of CCs would take in search of a niche to then research the solutions to it in CSE fields, a clever technique is employed. *A Guide to Conducting a Standalone Systematic Literature Review* ([1]) advises searching for previous systematic reviews on the same topic when starting a systematic review as they “consider the current evolutionary state of the research field” [1] and to not repeat work, *i.e.,* search that was already performed. Searching for previous literature reviews on a topic drastically reduces the amount of yielded papers and such studies contain an overview of the most important aspects, such as challenges, typologies, and innovations of CCs. Therefore, to have a reliable bridge between multiple disciplines and save time, comprehensive reviews of CCs were searched using the SLR methodology employed on reviews. More details on the protocol of the searches are present in Appendix A.

2.3 Findings

2.3.1 Part One – Complementary Currencies' Context

2.3.1.A Complementary Currencies in the Real World

Definition. Although there “is no universal” [4], “clear-cut, generally-accepted definition of CCs” [5] and “their economic meaning has still to be discussed” [6], there is consensus that a CC is “a standardized unit or medium of exchange that circulates in parallel to conventional, general-purpose money [...] such as the euro or the dollar” [4], thus being called *complementary* or *parallel*. They are “new systems of exchange which operate alongside conventional money, facilitating the exchange of goods and services in a parallel market, where alternative rules and resources prevail” [7], being their acceptance voluntary [7]. CCs can take many forms : “notes and coins, smartcards, or through telephone conversations and slips of paper” [7]. “CCs have been geographically confined parallel systems of exchange developed by civil society groups and non-governmental organisations” [4], not to “replace official money but circulate alongside it for specific purposes” [6]. Alternative designations include “social, local and alternative currencies” [6]. CCs “allow communities to trade resources and skills among their members” [5] and “respond to the peculiar needs of a given community” [6]. Typically, “circulate only within the boundaries of a given geographic community” [5], a “a delimitated territory” [6]; thereby being “geographically rooted” [6]. Some sources suggest that “they can work at a local, regional or national level through different issuance model” [4], and “at the moment they are largely fields for endogenous (insider-driven) service development” [4]. And “[w]hile they are still small in circulation and impact, they deserve attention as potential models of alternative ways forward for sustainable economies and societies” [8].

Context. Most CCs emerge “during periods of economic instability” [5] (*e.g.* 2007 crisis [6]). “The development of several contemporary CCs since the 1980s has indeed been linked to periods of monetary crisis or financial shock” [5]. “[E]fforts to reform, replace and redesign money have a long and rich history around the world as a tool to support local economies in times of recession (when conventional money is worthless or in short supply)” [8]. [5] analyses that earlier CCs “were developed in the 1930s in in Germany, Austria, France, USA” in the context of “rising Capitalism and macroeconomic depression, which eventually led some activists to explore other ways to revitalize the economy”, “while contemporary (from the 1980s onwards) were developed for fostering human development, social cohesion and protection”, and “contemporary CCs have proved rather more durable than earlier systems emerging in response to crises (with the latter soon vanishing once the local economy began to recover)”. Another reason for CCs development is to fix problems of current monetary systems: “a shortage of money – supposedly the measuring stick of the economy – results in the paradox of having people with skills and labour to offer, plus work that needs to be done, but without the money to bring them together, the result is unmet needs and unemployed workers” [8], which happens not only during crises, but regularly as "'capital flight' away from peripheral economic areas and towards centres, so draining regions and communities of the means of exchange" [8] - meaning "the mobility of money is not necessarily a good thing for local economies" [8]. A solution to fix this problem, "would be to split the functions and have separate currencies for each purpose, so ensuring a ready supply of money for trade regardless of stores of value" [8], a gap CCs can fill as "they provide a medium of exchange which circulates alongside scarce national currency to provide new opportunities for economic activity; they are place-specific, retaining roots in local communities, and they are not mobile, which means they circulate within a given area and do not drain away" [8]. Nowadays, there are "over 5,000 communities around the world to address a variety of economic and social issues including the credit crunch, education, care for the elderly and unemployment" [6]. From which "[b]etween 3,500 to 4,500 CCs have been recorded (since the 1980s) in around 50 countries" [5]. Both reasons for CCs emergence presented (crises and problems with money) can be caused by the monetary system, which is unsustainable ([3] [7]) " because of the constant drain of financial resources going from poor to rich segments of the population, and the obsession for economic growth as main economic philosophy" [3]; "contributes to high levels of global economic inequality" [5], enabling "the concentration of capital resources, power and control of exchange relationships in the hands of a small number of elites, often multinational corporations" [4]; "it values some types of labour and not others, values scarcity (encouraging exploitation of abundant goods such as ecosystem services), promotes competition, and externalises certain costs" [7]. It leads to "the amplification of economic disparities and the decline of local economies [...] and even frequently the depletion of natural resources" [3], thus "a few 'new economic' approaches argue that we need to revise priorities away from the principal objective of economic growth and more oriented towards the well-being of society and community-level sustainable development" [3]. And "community-based (as opposed to commercial) CCs are specifically designed to overcome these problems and incentivise sustainable development" [7]. In sum, CCs have been emerging during crises to tackle economic instability, but nowadays, they appear in multiple forms to promote local and social development with more expansive, forward-looking and sustainable goals.

Functions of General Purpose Money vs CCs. "According to mainstream economic theory, money is a politically and socially neutral technology, with four core functions: as a medium of exchange, a unit of account, a store of value, and a standard of deferred payment" [8]. Critics to this theory argue "the functions of money – particularly medium of exchange and store of value – contradict each other. The fact that money is both a symbol (used for exchange) and a commodity itself (an item to be stored) encourages people to hoard money, removing it from circulation and thus reducing the amount available for transactions" [8]. "CCs can perform only some of the functions of formal currencies" [3]; they "tend to fulfil one or other of money's functions to the exclusion of others (for instance offering a medium of exchange which is incentivised to encourage circulation)" [7]. Moreover, "CCs both abhor interest as harmful and spurn the traditional function of money as a store of value" [5], and ""they cannot act as a standard of deferred payment (which involves charging interest)”” [5]. In a study “comparing the interest paid and received by German households, [it was] found that the mechanism of interest only benefited a small minority of rich people, while the majority (80%) paid almost twice as much as they receive” [3].

Goals. Generally, currencies were “intended as a tool for ease of exchange” [5]. However, the global economic system is not meeting people’s needs sustainably [5]. This is where CCs come “to fix some of the shortcomings of the state-managed currencies and the global capitalist economy” [4], “ remedying some of the negative effects of the mainstream, State-sponsored currencies dominating today’s global system of economic exchange” [5] and respond “to the failings of mainstream money – the conventional system of exchange – to promote sustainable consumption” [8]. By “design, many CCs attempt to serve the overall (economic, social, and environmental) wellbeing of the population” [6]; “the rationale for using them is often to contribute to the economic, social, and environmental sustainability of that community” [5]; “[t]hey therefore meet certain social needs by providing the purchasing power needed to engage in productive activities, create employment and buy goods and services” [6], “reduce the number of bankruptcies connected with the use of mainstream methods to stabilise the monetary systems” [6], “exercis[e] greater local control and development of markets” [5]. “Many recent community currencies are now emerging more and more deliberately as grassroots innovations with the aim of promoting sustainable development” [3]. “[Social sustainability] implies the maintenance of social capital, the promotion of cooperation, trust, and cohesion within the community for the benefit of all” [3]. But CCs “do not seek to replace the dominant money nor to eliminate public regulation of money completely ” [4]; “instead of undermining the roles played by traditional public and private banking institutions, they may well complement them” [5]. In sum, their goal is to serve individual and collective needs sustainably and promote sustainable production and consumption, sustainable development, and social sustainability, which general purpose money cannot do.

Typology. “Contemporary CCs are not homogeneous because they have not replicated any specific model, but instead have simply spread and diversified” [5], thus making their classification difficult, in addition “there is some overlap among CC types due to their complexity” [5]. Their typology across different studies diverges slightly, most authors divide CC types in three to four groups, not always the same. [5] separates four types: “LETS Models (or “Mutual Exchange” systems); Time Currencies (“Time Banks”); Local Currencies; Complex Schemes (or “Mobile Money”)”, while [3] uses a classification that encompasses “Service Credits; Mutual Exchange; Local Currencies; and Barter Markets”. *Service Credits* from [3] corresponds to *Time Currencies* from [5], and *Barter Markets* are fundamentally different from *Mobile Money* (explained later). *Mobile Money* from [5] is the same as in [9]. [6] presents a study that categorizes CCs according to their objectives: social, economic and digital money — an example of social objective can be *Time Currencies* (or *Service Credits*) that “seek to strengthen underlying relations within a community, increase the sense of self-esteem, offer a perspective and development reciprocity within a community", economic objectives comprise LETS, barter networks and regional currencies (*i.e.,* Mutual Exchanges, Local Currencies and Barter Markets) that "seek to stimulate the local economy, strengthen the position of medium-sized firms with respect to large multinationals, support local regions in absorbing global or national shocks, diminish leakage from poorer to richer by creating extra liquidity in underprivileged regions and increase economic diversity", and digital money comprises "mobile money systems—online payment platforms—peer-to-peer money systems) have their own logic and focus primarily on economic goals" [6].

Starting with **Mutual Exchanges**, these "systems "lie on a continuum between economic and social objectives"" [3]. Local Exchange Trading Systems (LETS) "use "deposit money". That is, the buyer pays the seller (for goods/services provided) using a cheque-like trading slip which records the amount of goods/services as a "credit" to the seller, and as a "debit" to the buyer" [5]; meaning "one account is credited and the other is debited of the same amount. The sum of all accounts is always zero and the value of the currency is preserved by the trust the participants have in each other to meet their respective obligations" [3]. "Members of a LETS list their 'wants' and 'offers' in a local directory then contact each other and arrange their trades, recording credits and debits with the system accountant" [8]. "No interest is charged or paid, so there is no incentive to hoard credits, and exchange becomes the primary objective" [8]; "they aim to provide access to additional liquidity and interest-free credit, and to encourage import substitution" [3]. "Their value can either be linked to a national currency, be time-based or even a mix of the two" [3], but "the units are not convertible to the official currency of the country" [5]. LETS are "designed to strengthen local economic linkages, to offer a greater degree of resilience against economic shocks, and support local exchange in times of economic downturn" [7] (*i.e.,* local economic development), they "grow in times of recession, providing an alternative labour market, opportunities for informal employment and cash-free access to goods and services" [7]. "LETS deliver small, but significant, economic benefits to members, providing new opportunities for informal employment and gaining skills, and enabling economic activity to take place that would not otherwise have occurred. But their social impact is much greater, as they build social networks, generate friendships and build personal confidence" [8]. "Mutual Exchange currencies such as LETS comprise 41.3% of total projects" in one reviewed sample [3].

"**Time banks** aim to overcome the limitations of LETS by being based in mainstream institutions (health centres, schools, libraries), paying coordinators for development and support work, and most importantly, for brokering transactions between participants" [8]. A Time bank "is essentially a volunteering exchange" [7], it "operates like a reciprocal volunteering scheme, with a central broker to coordinate members activities" [8]. "In Time Currencies (or Time Banks), participants exchange services in terms of their time" [5], "[e]veryone's time is worth the same – one time credit per hour – regardless of the service provided" [7]. "Members receive a time credit for each hour they provide a service to someone else and they can use this credit to benefit a service from another member" [3]. Time currencies "are not backed by the national currency and are thus wholly non-convertible to the latter" [5]. [5] suggest that "the system seeks to encourage local employment", however, it seems to have a more significant effect. "[T]ime banks address [...] that certain types of labour are valued and others neglected, producing perverse incentives which undermine social cohesion" [8], it allows to value work as "raising children, caring for elders, community volunteering, helping neighbours – in order to strengthen communities' capacities to support and care for themselves through the development of social capital (ties of reciprocity and trust)" [8] and "invigorate active citizenship" [8]. "[T]ime banking is being used to promote more sustainable consumption and environmental governance through 'ecological citizenly' action in a variety of ways" [8]. In the reviewed study, time banks or *Service Credits* were the majority of CCs in the sample (50.2%) [3]. Which is coherent with [5]: "an estimated 90% of CCs worldwide have been either Mutual Exchange schemes or Time Banks; local currencies account for about 7% of CCs)" (7.1% according to [3]).

Local Currencies are "convertible to the national currency" [5] thus "covered by equivalent reserves in the national currency" [5] used for "ordinary purchases at participating shops and enterprises" [5]. [3] mentions that "[t]hey are paper-based currencies sometimes convertible to national currencies and circulate within a geographically confined region".

Mobile Money "typically use an electronic form of currency" [5] and it "lies outside the formal banking system" [5], which allows users to "make basic financial transactions (such as transfers, deposits, and withdrawals of digital money) without a formal bank account" [5]. It relies on "the use of mobile phones to replace banks and ATMs in regions where access to these institutions is limited" [9]. "[C]onsumers would deposit cash (legal tender) in their mobile money accounts by visiting a participating agent" [5] ("small retailers, such as grocery stores and petrol stations" [5]), by "depositing official money, consumers purchase an equivalent value in the electronic currency (E-money) which is held in their mobile wallets" [5] enabling transactions with other holders of such accounts [5]. It is important to note that "there is a ceiling on E-money transactions (e.g., a maximum of $1,000 in Kenya and Uganda) to minimize the use of mobile money for money laundering" [5]. These systems started in Africa — *e.g.,* "Côte d'Ivoire, Egypt, Ghana, Uganda, Nigeria, Kenya, Zimbabwe" [9]), where money is scarce, started to trade airtime minutes "on their phones as proxies for money" [9]. "[P]re-paid mobile phone minutes could be transferred between users, meaning they could be used in bartering" [9]. Leading to the establishment of *M-Pesa*, which enabled "mobile phone users can deposit money into an account accessed through their phone, send money through text messages, and withdraw cash at the phone dealers" [9]. "[T]he banking branch and the banker are represented here by the neighborhood shop owner who serves as the mobile phone company's agent. As a known social figure in the neighborhood, the financial system builds on a trust network that's already in place" [9].

Examples. "The Swiss Wirtschaftsring, **WIR** (founded in 1934), and the Sardinian currency Sardex are examples of centralized mutual credit systems with no circulating (paper) currency. They aim at supporting trade in their specific area by increasing demand and financing working capital of business" [4]. "WIR credits do not pay interest but earn it. The fact of not having to borrow money from outside is sufficient to allow the bank to offer mortgage loans at very low interest rates and independent of the credit conditions in international markets" [6].

(from [6]) **Sardex**, as a mutual exchange system inspired by WIR, "offers liquidity of the means of payment by offering a basket of goods and services that is larger than the monetary basis". "One SRD is equivalent to one unit of the official currency", WIR is also pegged to their national currency. "The online portal allows all subscribers to create profiles providing all the information on their activities and products, to contact other firms and arrange and complete transactions". The portal was developed to have multiple functions, including e-commerce, yet "most relevant contacts appear, however, to be made offline". "Firms join, thus accepting payments in SRD on a voluntary basis, by signing a two-party agreement on the percentage of the compensation to be covered in SRD. For transactions of up to €1,000, members agree always to accept the full amount in SRD. The level of overdraft facilities is determined on the basis of an assessment of the member's creditworthiness and opportunities to buy and sell within the circuit". "Every firm is assigned a broker that gives advice and manages transactions", "and finds potential business opportunities by comparing data on supply and demand" - "firms enjoy access to these competent advisers". Use cases for Sardex include partial payment of wages and bonuses with SRD ("employees who need an advance on wages to cover unexpected expenditure", thus "avoid using their own savings or applying to some credit company and paying high rates of interest"), fidelity points ("[s]pending on the part of consumers within the circuit is rewarded with credits to be spent in the same sphere, something like the system of fidelity points at a grocery store, which offers a concrete incentive to remain inside the circuit" which "could replace the mechanism of discounts and generate a multiplier effect on consumption at the same time"), donations to charities and non-profit organizations of unspent balances. "The real 'spendability' of credits must be guaranteed, which makes it necessary to increase the number and variety of firms participating in the circuit". This system, guarantees that means of exchange is always available (as it is created in the transaction), that it "circulates more quickly than the official currency because the party holding it always has an incentive to spend it", and solves the paradox "in which unsold goods and unused labour capacity coexist with needs that are not satisfied", crucial in crises or peripheries.

JAK Medlemsbank, a Swedish bank, is "concerned with the negative social impacts of interest that wished to promote interest-free financing" [9], as "interest is a root source of social inequity" [9], provides interest-free savings and loans for over 38,000 members. [9]. The system uses *savings points* that determine members' borrowing amounts. "In this way people can borrow and save approximately the same amount over the course of their lifetimes, as if they were borrowing interest-free from their future selves" [9], and members also "collectively vote on the bank's activities" [9].

Grameen Bank, started in Bangladesh, a bank that brings "credit to the poor, who are otherwise excluded from traditional banking" [9]. Debt repayment relies on social pressure as members form small groups to whom credit is given. Sometimes they help others pay their parts, as the group will not benefit from more credit if a member defaults, thus being called *solidarity lending* [9]. "The bank itself is owned by its borrowers, with a small percentage of ownership held by the government" [9].

Gift economies are based on the principle of reciprocity — "gifts are exchanges that create social relationships" [9]. Contemporary gift economies include open-source software, peer-to-peer file sharing networks (*e.g.* Napster), where "individuals are valued by how much they give, and reciprocity is considered essential to the health of the system" [9].

The **NU card** is "a 'green loyalty point' currency which" [8] from the Netherlands. "Points are earned when residents separate their waste for recycling, use public transport, or shop locally. Extra points can be earned by purchasing 'green' or 'ethical' produce (such as organic food, fairly traded goods, recycled products, rental, repairs etc) at a range of participating local stores. The points can then be redeemed for more sustainable consumer goods, public transport passes, or cinema tickets (in other words, spare capacity in existing provision which incurs no additional costs), or donated to charity" [8] - "in other words, promoting sustainable consumption using carrots rather than sticks" [8]. "Like time banking, it rewards actions which are seen as positive, building on psychological responses and self-esteem to grow sustainability, rather than guilt, exhortations to action, and punitive measures" [8].

"In addition to these 'social' currencies, a range of virtual currencies is now in use across the globe which are rarely thought of as alternative exchange systems, but which nevertheless function as mediums of exchange, units of account and stores of value: air miles and supermarket loyalty points are two common examples which demonstrate the plurality of money in everyday use" [8].

2.3.1.B Complementary Currencies' Economic Impact and Challenges

Benefits. CCs build up communities' self-reliance [8] [5], "[insulate] local economies from larger exogenous shocks" [5], "[build] social capital and [strengthen] social cohesion" [5], "reduce people's dependence on unsustainable labour and consumption practices [...] and facilitate the workings of commons-based sharing platforms and organisations" [4]. Mutual exchanges and other CCs based on the principle of credit clearing "improve the stability of production and consumption" [6] and have "the effect of stabilising the profits of firms while attenuating the impact of the credit crunch at same time" [6]. "CCs can contribute to sustainability first of all because they can promote localization or foster local economic activity by preventing global outflows of wealth and increase the circulation of money in the community[...]. When the usage of the currency remains local, it is safe to assume that the money will circulate faster and in larger proportion, thereby stimulating the local economic multiplier and increasing local incomes" [3].

They “[allow] people to incorporate social and environmental factors into their valuations and purchasing decision” [8], “valuing and rewarding the development of social capital and active citizenship” [8]. “CCs promote social participation, allowing fringe groups, (for instance, the poor and the elderly) to participate in economic relations from which they might otherwise be excluded, and therefore create/maintain bonds of reciprocity between people within a community” [5]. Make the exchanges happen: “a large proportion of the time exchanged would not have happened without the time bank” [8]. Regarding time banks, the “valuing all labour (or time) equally seeks to explicitly recognise and value the unpaid time that people spend maintaining their neighbourhoods and caring for others. Thus voluntary work is rewarded in credits, and so incentivised, rather than squeezed out by the conventional economic system which accords it no value” [8]. In “the mobile currency system have a larger set of people in their network to rely upon whenever there is an economic shock. Put another way, it is easier for participating households to receive a remittance quickly from friends or family, making them less vulnerable to shock” [5].

Experimentation and Innovation. “CC innovation patterns and found that new CC models are most often created by experiment-led forking in previous models” [4]. It does not work to copy and paste successful schemes of CCs to solve local problems: community banks from Brazil that “copied from models used in other countries, have performed incredibly poorly in comparison to these community banks, who have developed their own local methods of operation” [9]. For instance, “Sardex’s trial and error development has been firmly attached to the island’s existing social networks with the blessing of the local officials” [4]. However, “[c]urrency innovation has suffered from the inflexibilities of political ideologies that hinder radical sustainable innovation from taking place” [4]. While general purpose money “disregard[s] the need for trading partners to establish and solidify particular social ties and trust relationships” [4], “CCs represent new forms of valuation systems that allow re-connecting money to the social realm” [4], as “[t]he very idea of distinguishing between the social and the economic aims and features of money is, however, questionable” [6]. “[R]esearchers stressed the importance of ‘the emergence of new information and communication technologies’ to promote local projects that use ‘open source money’ or ‘collaborative money’ ” [6]. “Some of these digital currencies are specifically created to promote sharing and cooperation among community members, yet their deployment is still in its infancy” [4]. “We are currently moving to a new era of currency innovation that utilises digital networks and new technologies (for instance distributed ledger technologies, also known as blockchains) to produce, numerate and distribute value [...] modern CCs include cryptocurrencies and digital tokens to support person-to-person collaboration” [4]

Economic Impact. The general conclusion to the economic impact of complementary currencies is that their impact is marginal: “although there is some evidence that CCs promote localization and support local businesses, the results of the analysis demonstrate that CCs’ impact on the overall economic activity remains marginal” [3]; “the economic activity of CCs is too low and not significant in macro-economic terms" [3]; "the beneficial impacts of CCs are endogenous/marginal to the local mainstream economies" [5]; "CCs have at best resulted in modest economic benefits for their local societies, and that these benefits fall short of the anticipated economic gains" [5]. Other reviews claim that CCs have a positive impact: "it is effective in building economic sustainability, as some CCs improve employability and promote local economic activity; most CCs seem to have a positive impact in terms of social sustainability and in the achievement of social goal" [5]; "CCs may ease negative aspects of traditional financial exchange by serving those on the fringes of and/or excluded from formal economies, and without necessarily competing with public or private traditional banking institutions" [5]. Local currencies "were regarded as 'small and marginal' by the Seyfang research group, who stated that 'little is known about the processes and contexts necessary for mainstreaming them" [6]. [4] regards that "[l]ocal and community currencies have thrived especially during economic downturns and played a stabilising role when official money is hard to come by". "[T]he implementation of the Red de Trueque had an added value to Argentina's GDP of just 0.6% while this system is considered as one of the most successful" [3], and "their impact seems greater in period of instability as was the case in Argentina with the RT, Switzerland with the WIR or El Salvador with Punto Transacciones" [3]. "Local currency Bristol Pound (a local currency in the UK), Marshall and O'Neill (2018) find that the system has very little economic impact even within the local economy and that as a result, it has done little to foster either local production and or regional economic development" [5]. "LETS in Australia, British LETS, and the French SOL revealed that the levels of trading were too low to have a meaningful impact on the local economy" [3]. "In the case of the Swiss WIR system, Stodder (2009) finds a positive (stabilizing) relationship between the WIR and the country's economy" [5]. With " Sardex, bank deposits tend to decrease while consumption and firm profits show an increase. In this case, the decrease in deposits, being related to the increase in consumption and ultimately to the capacity of firms to pay their debts, tends to improve the solidity of bank balances by reducing the volume of bad debt. The result is an attenuation of the credit crunch for local firms belonging to the Sardex circuit" [6]. "[T]he most positive contribution of CCs is their social benefits, and that the economic benefits are somewhat diminished by the small scale of these systems and the lack of awareness on their scope, making it difficult for them to have a significant impact on the local economy" [3]. "CCs thus appear to have a greater social dimension of sustainability than on the economic and environmental ones" [3]. Other benefits were present, such as "recognizing informal work and valuating skills usually not valued by the formal labour market" [3]; "promot[ion of] local economic activity" [3], "stimulat[ion of] local consumption and increas[e of] the economic multiplier" [3], "access to goods and services otherwise not affordable" [3], "act[ing] as cushions against external economic shocks during economic recessions" [3]. "Regarding Mutual Exchanges (MEs), a majority of [...] studies [...] indicate no significant impact" [3]. The limitations to these findings include "the limited number of studies evaluating CC's impact" [3], "a wide range of different frameworks, methodologies to collect and analyze data, and performance indicators to assess CCs' outcomes" complicate the comparison of the data [3].

Challenges. The main challenge with CCs is that "the positive social and economic impacts [...] tend to be small-scale" [5]; "scale is an issue, particularly for LETS" [5]. "While the scale of these examples is presently small, they have demonstrated that they do achieve their objectives and have the potential to achieve much more if scaled up and mainstreamed" [8]; "CCs would be better able to achieve their social goals if they could attract more users, and if more goods and service providers were to accept them for payment purposes" [5]. "One reason generally outlined in the literature and confirmed during the data extraction process regards the small scale of CC systems, and the low number of transactions per member. With such small scales, CCs are thus creating relatively small local economic circuits of exchange, and only a small proportion of wealth remains local" [3]; "one reason for the low participation rate is the lack of awareness on CCs. In fact, either people don't know that CCs exist or what they are, either they are not fully conscious of their potential. One study in particular revealed that improved mindfulness leads to increased participation, which in turn provides greater benefits" [3]. "[T]he impact of some CCs (for example, in boosting the local economy and benefiting users) is hindered by their small size, or by restrictions on the range of good and services exchanged" [5], and "government regulations are a significant obstacle. Current social security rules deter benefit-recipients from participating in local exchange systems like LETS, by counting LETS earnings as equivalent to cash income" [8]. In time banks, "the unemployed are officially encouraged to participate, for social and community reasons, but may only exchange their credits for services, not goods" [8] and "those in receipt of incapacity benefits are deemed to be capable of working if they take part in time banks, and so risk losing their benefit payments. This is a short-sighted and misguided policy, as much time banking work is carefully targeted towards the abilities of participants, so for example a housebound person might earn credits for making telephone calls to others, but still be incapable of conventional employment" [8]. Other obstacles for time banks include "Limited range of services available in exchange for credits; difficulty becoming established, as projects take a long time to develop yet they are reliant upon short term funding; and reciprocity is slow to materialise due to a cultural shift needed to alter the reluctance of participants to ask for help" [8]. Many currencies are "short-lived" [4], which can affect trust and long-term goals; "projects dependent on funding often struggle for survival" [7]; "many time banks have also ceased operating due to lack of funds" [7]. [5] indicates that "CCs would need institutional recognition from public authorities and banks, which could either come in the form of financial support, or as official validation by governmental authorities", since "[i]n the past, many CC initiatives have been challenged or depleted by regulatory action" [4], "[s]upport from the public authorities has been seen as vital for the impact, legitimacy and viability of the CC projects" [4]. Although "CCs are frequently designed as a means of exchange rather than a store of value, hoarding is still a problem which contributes to system stagnation" [7] which happens due to the " reluctance to ask for help, inability to find goods and services to purchase, and a desire to save for a rainy day in some cases, this is 'irrational' behaviour" [7]. Transaction costs of CCs tend to be higher than using conventional methods of payment [7], and "it is reasonable to assume that these costs and unfamiliar mechanisms deter some participants" [7]. "[P]revious experience with LETS and time banks demonstrate that it is not sufficient to simply introduce new systems of exchange and expect people's behaviour to adapt to the new infrastructure. Barriers include the high levels of social skills and personal confidence required to initiate a transaction" [7], *i.e.,* the new systems should be familiar and people should be skilled in performing the actions the new system require them to perform. Since Mutual Exchanges "do not appear to achieve their economic objectives" (*i.e.*, "Provide additional liquidity; ease access to interest-free credit; encourage import-substitution" [3]) [3].

2.3.1.C Cryptocurrency's Economic Impact and Suitability for CCs

Bitcoin in the economics and finance literature: a survey [10], published in 2021, presents a review of Bitcoin in multiple domains: "price and volatility dynamics; economics and efficiency of the system; and financial aspects and regulation" [10]. The most relevant for this study domains are efficiency and economics, and bitcoin as currency vs asset, as it briefly portrays what is missing for bitcoin to work as an alternative currency. [10] starts by contextualizing the invention of Bitcoin as an attempt "to create a transaction system free from intervention by any central or monetary authority, be based on a mathematical algorithm instead of "third-party trust", [where] payments can be done electronically in a protected, verifiable and incontrovertible way" [10]. Despite presenting several characteristics in regard to Bitcoin — the public access to the information, the anonymity; and an overview of how Bitcoin works technically — mining, blocks, Proof-of-Work, consensus, the main focus of the review is to study the economic and financial perspectives of Bitcoin.

Benefits of Bitcoin. Bitcoin is powered by the blockchain technology which, in turn, provides safety, verifiability and quasi-anonymity. Bitcoin accounts for more benefits as "tie savings, business flexibility, cost minimisation, avoids third-party commissions, does not generate inflation; anonymity of traders, and escapes central intervention" [10], moreover, it "overcome the difficulty of transport and storage compared to standard currency" [10]. It is, thus, "an inexpensive fund transfer system" due to the low transaction costs which "helps improve access to financial services" [10].

Disadvantages. However, it also faces issues of "extreme volatility of price, uncontrolled transaction, large speculative attacks that can cause negative effects, limited confidence[...], and increased vulnerability of cyber theft" [10]. Its transactions are considered secure as long as "no party controls more than 50% of the network's computing power" [10], which leads o significant electricity consumption "to carry out high computational problem" [10], "leav[ing] behind a carbon footprint" [10]. There are expectations that with time, technology evolves and the mining process decreases its difficulty, "making the entire process more efficient" [10]. Other means to improve efficiency include "implementing transaction fee and limited block size in mining" [10].

Price Fluctuations/Volatility. For now, "it lacks liquidity and yet to achieve a widespread user base" [10] and it "is not, yet a very widely accepted payment system" [10]. The considerable fluctuations in price of Bitcoin further hinder its adoption as a means of exchange. "There is extensive literature trying to examine whether it is an efficient means of payment" [10]. Although normally basic economic indicators (*e.g,* "utility, supply, demand, and scarcity" [10]) are used to adjust the prices of commodities, the price of Bitcoin is influenced by many more factors than regular currencies, some of "which might be very absurd to be considered for any other fiat currency" [10]. For example, the "transaction volume [...] proves to be a significant demand driving ingredient implying that the transactional needs of users drive up the prices" [10], but the "supply-side variables, on the other hand, prove to be insignificant in driving the prices of this unregulated contemporary currency" [10]. It is so because Bitcoin is of fixed supply (determined/governed by a mathematical algorithm) thus "any expected future change is already reflected in the current prices" [10]. Some reviewed authors believe that the fixed supply of Bitcoin "will lead to deflation which will, in turn, lead to high welfare destroying volatility" [10], to deal with this issue, it has been proposed "to have an adjustable growth rate of currency supply" [10] or implement "a decentralized voting mechanism" [10]. On the other hand, there are authors that do not agree that Bitcoin's fixed supply will lead to deflation, but that it "will negatively impact the profitability of mining activity" [10]. The fluctuation in Bitcoin prices is due to associated market expectations, however, "Bitcoin price reflects much more than just standard supply/demand and fundamental news. Bitcoin being a digital currency **needs to be analyzed from a further perspective than just as an ordinary currency**", [10] concludes.

Alternative Currency. It is recommended "to create a mass demand for Bitcoin to have a parallel economy and later serve the instability and deflationary pressure issues" [10]. However, when "[t]esting against standard definitions of money", a reviewed study "**does not pass Bitcoin to be an alternative currency** and asserts that **it cannot function as a store value of money**" [10]. Similarly, other studies "declare Bitcoin as **unfit to be used as currency since the high volatility feature** adversely affects its store of the value property" [10] as they find it "to be thirty times more volatile than other currencies (US dollars, Euro and Yen)" [10]. Other comparable study "hails Bitcoin as a digital Ponzi scheme down the road if it fails to prove itself as cheap, efficient, ingenious, democratic, and a stable payment system" [10]. In contrast, other authors suggest that Bitcoin is "highly effective for transactions and can be used in conjunction with fiat currencies i.e., it is not a substitute but a compliment" [10].

Price Manipulation. Since Bitcoin is generally unregulated, "makes it highly vulnerable to manipulations" [10], which have "substantial distortive effects on Bitcoin" [10]. News impact it's price, specifically, "bad or negative news has a greater effect on the volatility of Bitcoin prices than good or positive news and is highly driven by presumptions of the market participants" [10]. Similarly, "word of mouth and expanding Bitcoin user base are significant influent on the existence of a pricing bubble" [10]. The cycle starts with "media reports a price increase which further triggers search activities among investors" [10], lifting investors' interest in buying Bitcoin, which, in turn, increases the demand, ultimately uprising its price and "attract[ing] new investors thus increasing the user base" [10]. Interestingly, "the number of searches declines as the bubble nears its end" [10].

Stabilization. Some studies defend that "the acclaimed volatility of Bitcoin in the literature is because it ignores the trading volume. The Bitcoin has relatively lower trading volume due to which the Bitcoin exchange rate faces unavoidable shocks and hence, so does its price" [10]. Even though "Bitcoin prices to be more volatile than EUR-USD exchange" [10] and "experience a higher number of bubbles and crashes" [10], "the volatility is getting reduced and stabilized over time" [10]. In other words, even if Bitcoin "appears as highly volatile in the short-run, it will stabilize over a longer period of time" [10]. Most of the reviewed literature, as [10] claims, defend that it is so because Bitcoin is in its infancy - "the Bitcoin market is volatile due to the fact it is in its nascent stage. In the longer run, the price stabilizes, volatilities dampen and the existence of bubble diminishes" [10].

Speculation. New investors tend to use Bitcoin for investment purposes rather than buying goods or services, and their sentiments affect its volatility [10]. Its "value at any point in time reflects its expectations about the future value and a change in this expectation can change the value further" [10]. Since Bitcoin is "characterized by high price fluctuations, users may use it only as a speculative instrument" [10], which earns high returns due to high volatility to compensate the risk. This is the main reason that "Bitcoin **cannot compete with standard currencies due to its speculative nature**" [10]. The "Bitcoin market is user-driven" - "it can be said to be driven by future expectations of the Bitcoin holders and future investors" [10]. In other words, it "has a value till the users think it has some worth or can be converted to currency at a higher return" [10]. A "piece of false or fake news can blow out easily and thereby causing unrest in the [...] market" of Bitcoin [10]. Additionally, not only the internet searches influence prices, but also the prices influence the number of searches. Other study found the "number of tweets to be a significant driver of Bitcoin's trading volume and realized volatility" [10] but its "supply and demand are independent of macroeconomic factors [unlike] standard currencies" [10]. However, multiple studies concluded that Bitcoin is not a strong safe-haven instrument during market turbulence [10] (conclusions around Bitcoin's safe-haven capabilities are conflicting). Although "the returns are independent of external economic factors", it "is the market participants that internally drive the market returns which make it a front runner as a speculative instrument". Since "Bitcoin is weakly correlated with other assets" (*i.e.,* traditional assets), the "inclusion of Bitcoin in the portfolio makes it well diversified" [10] and can be a good tool for hedging - "Bitcoin's hedging effectiveness against global equities and global bonds becomes prominent if we consider the level of global economic policy uncertainty" [10]. A study assesses Bitcoin against energy commodities "since electricity is a key input in Bitcoin transactions and can be expected to have different results from non-energy commodities such as gold" [10].

Economic Impact. Although our interests lay in understanding the economic impact of cryptocurrencies as complementary currencies, there is not enough work done in this topic — the "application of Bitcoin (or cryptocurrency) for the upliftment of economies and financial inclusion needs more exploration" [10]. However, the symmetric assessment (the impact of economic factors on Bitcoin) has been investigated. There is work that "exhibits that real interest rates, tax burden, and investment freedom across different countries is significant in determining Bitcoin prices. In contrast, inflation rates and monetary freedom across boundaries have no impact on Bitcoin prices" [10], partially, conflicting with the idea that Bitcoin is independent of macroeconomic factors.

User Trust. Bitcoin "is not backed by any regulatory authority nor does it have any asset backing" [10], "no central backing or point of trust" [10]. "Its feature of being decentralized attracts individuals who want a "freely traded currency" and stay away from any intermediators such as the bank, or the government" [10], which has linked Bitcoin to "evasions in terms of legality" [10], "illegal activities and money laundering" [10], mostly by cause of its anonymity feature. Bitcoin is not fully anonymous, as it "is possible to unveil up to 40% of Bitcoin user profiles" [10]. Most reviewed studies propose "to enhance the transaction-related regulations to curb money laundering and criminal activities" [10] and "recommend not to put a complete ban on Bitcoin as that could hinder the technological advancement" [10]. But "[r]esearch focusing on regulatory and legality aspects fails to suggest suitable solutions to make Bitcoin a safer and widely acceptable cryptocurrency to avoid illegal activities" [10]. Since Bitcoin is "decentralized, there is absolutely **no guarantee of any help or resort in case of a failure** and is thereby difficult to safeguard it from various types of risk" [10], which constitutes a considerable drawback "that limit people from using it as a hardcore currency" [10]. "[S]tandard financial regulations can have a quite significant impact on the Bitcoin market" [10]. As the government "has the power to prevent an ancillary currency in countries' economy if it enforces severe penalties" [10], it could also play a role "in reducing the speculation behavior of Bitcoin (and other cryptocurrencies) to stabilize the market". Ultimately, Bitcoin is evolving, but it is still a new technology, in order for it to be used as an alternative currency, it should be robust and "be able to prevent any fraudulent exploitation".

2.3.2 Part Two – Complementary Currencies and DLTs

In this part of the study, "credit network" was added to the keywords of complementary currencies, as the economic benefits are alike. However, there exist considerably more results in Computer Science about credit networks and decentralized credit networks than about complementary currencies.

2.3.2.A Credit Networks and Decentralized Credit Networks Background

Credit Network (CN) (or Decentralized Credit Networks (DCN)) model the social ties and trust [11] [12] "among users in a peer-to-peer system as a directed, weighted graph and the capacity of an edge (link) indicates the level of trust that a user is willing to extend to another" [11]. They "are essentially peer-to-peer lending networks, where users extend credit, borrow money and commodities from each other directly, while minimizing the role of banks, clearing-houses, or bourses" [12], but "with much lower transaction fees" [12]. Moreover, CNs have the "capability of performing same and cross-currency settlement transactions between fiat currencies, cryptocurrencies and even user-defined currencies at a very low cost in few seconds" [13]. Since CNs are systems based upon the trust of the users, their functionality is inherently different from Blockchain, a trustless system. A CN "provides the basic infrastructure for building distributed payment networks" [12], just as Blockchain. However, while in a Blockchain any user (Alice) can transact directly with another (Bob), in a CN "Alice and Bob can trade credits directly with each other, if there exists a direct trust relationship between them, or via a path between them through network peers, built on peer-wise credit relationships" [12]. This means that Alice and Bob can trade directly if they trust each other (thus having a link (edge) representing this trust in the graph of the CN) or they can trade if there is a path of trust in the graph that links the two (*i.e.,* if some of their neighbours or their neighbours' neighbours trust each other). "For broad-based acceptance and use, any credit network has to handle the following three major challenges:" [12]

1. **Concurrency** - transactions, running in parallel and potentially using the same links, ensure integrity and atomicity ("either all credit links on the path get decremented, or none at all" [12]). "This guarantees that the right receiver gets the payment, and prevents double-spending of credits" [12].
2. **Efficient Routing** - "Routing of a credit payment, requires finding of a path between a sender and receiver that has sufficient credit, in an efficient way" [12].
3. **Privacy** - "at a minimum, a well-designed DCN needs to guarantee sender and receiver privacy (does not reveal their identities), as well as privacy of the amount transacted between them" [12], the privacy of the users in the path must also be guaranteed as well as the network topology and ensure the "un-linkability of transactions" [12] (*i.e.,* deanonymization).

The concurrency guarantee can be ensured with the use of blockchain, which (presumably) is the case of a widely deployed CN, Ripple ([14]). The other two challenges, privacy and efficiency of routing, are being researched in academia and the results of which are reviewed in this SLR. "The credit network is a promising paradigm, but it is still in an early stage and has some unresolved issues" [11], which are detailed in 2.3.2.B, the solutions and innovations for these problems are shown in 2.3.2.F and in 2.3.2.G we enumerate the challenges found in those solutions. Other studies, such as [11], also include in their system goals or requirements security (confidentiality, integrity, authentication) and scalability, while not enforcing concurrency.

2.3.2.B RQ1. What are the main issues that the studies try to address in credit networks and complementary currencies?

Privacy has been the most prevalent issue being solved in CNs, as in "making payments in credit networks, both merchants and customers are trying to protect the privacy of their credit links and transaction patterns from outsiders like competitors, authorities, and service providers" [11]. "However, in current credit networks, the network topology as well as the available credit value of the links are public to all users" [11]. "Designing a distributed credit network, that maintains user and transaction privacy, while supporting concurrency is a challenge" [12]. There is a tradeoff between concurrency (since the system is decentralized and distributed) and privacy in DCN [12]. "[C]redit networks have different structure and privacy needs as compared to cryptocurrencies, which do not require credit links or IOU paths, secure path-finding, etc." [12]. "The simple pseudonym mechanism employed in Ripple cannot provide any meaningful privacy protection" [11] as it is "vulnerable to deanonymization attacks" [11], or "linkability of transactions" [12]. Therefore, different solutions have emerged to protect users' privacy, most of the time, deeming this quality as a requisite/guarantee and focus of a CN (*e.g.,* in [11], or a DCN [12]). Payment Channel Network (PCN) have also been an innovation for blockchains, "which combines blockchain with the credit network in economics" [15]. "A well-connected channel network can enable off-chain transactions for most payments, drastically improving the efficiency and scalability of blockchain" [15]; in other words, "are designed to improve the scalability of blockchain" [16] as it allows peers to transfer funds without frequently updating the blockchain [16, 17] and "[a] payment network over offline channels allows path based fund transfer among peers who do not have mutual channel" [16]. Similar to CNs, "[a] crucial challenge in PCN is routing, i.e., to find a set of paths that fulfill a payment request" [15]: "while the payment itself is privacy-preserving through existing protocols, the probing process can leak sensitive information including the location of the sender or the recipient" [15]. Although PCNs focus on the infrastructure and communication protocols, the main challenge remains routing, but the paths and the recipient are unknown to the intermediary nodes [15]. PCNs are thus scalability solutions [17] for the blockchain which leave privacy issues to be addressed, as study [15] and [16] (which uses an alternative name for PCNs — "Blockchain offline channels") do.

Channel Imbalance. "Unlike traditional communication channels, credit channels can become imbalanced" [17], which hinders the transaction throughput of the network [17]. When a credit link becomes exhausted, no new credit flow can be routed through it, preventing the node (or user) to receive fees from that channel [18], and possibly preventing users trusted by that node to make payments or transfer IOUs, if the exhausted edge is the only link. Moreover, "imbalancing creates a complex dependency between a network's throughput and its topology" [17], which can cause deadlocks in the network [17]. Rebalancing of the links is the operation that enables a user to create more links if they had run out of credit [18]. However, another study on channel imbalance and deadlocks are against current methods of channel rebalancing and propose a different approach related to network topology and transaction patterns [17, 19].

Graph Topology. "In a general credit network, autonomous agents can issue their own notes, and other agents can choose whether to accept these notes as payment, i.e. they can decide whether to trust any other agent [i.e., that they will atisfy the obligation], and for how much" [20]. "More recently, credit networks are in use to improve cryptocurrency transaction rate and latency" [20]. However, if there are agents who trust each other, "they could transact without putting any information on a blockchain. Instead, they could privately track the net balance of their transactions and settle this balance only as necessary" [20]. The set of contains that is imposed to the agents has relevant results in network topology [20]. Blockchain crimes, such as money laundering and blackmailing, can be detected by tracking the shape of a network [21]. Such crime usually involve currency exchange however, no previous work has been done in detecting anomaly patterns on multi layered networks (cross-cryptocurrency) [21]. Graph analysis to detect illegal activities involving cryptocurrencies is known as taint analysis, which can be passed to Machine Learning methods to detect analysis or not [21].

IOUs. Lending markets have not been able to provide the needed liquidity for the SMEs due to asymmetric information, imperfect competition and systemic biases which decrease SMEs chances of obtaining loans [22]. CC, and commodity money "have proved to be useful instruments to facilitate economic regeneration" [23]. They are "useful for facilitating exchange among selfish peers" [23]. "They can be valued and exchanged in relationship to national currencies but also function [...] their own" [23]. Although towns and SMEs issue their own scrip (a kind of SME CC) and sell coupons with future-redeemable goods on a discount to increase their liquidity, they "face significant challenges including information hiding, liquidity, fraud, problems with valuation, and acceptance" [22]. Service Level Agreement (SLA)s are "efficacious tools for managing resources" [23]. It "provides a contract between a service provider and one or more users" [23] in which "contains guarantee terms that need to be satisfied by a provider, and a payment that needs to be made by a user when such guarantees have been met" [23]. "The relationship of such a currency to a "service" is particularly interesting" [23] and is explored in [23]. Issuing a new personalized kind of IOUs "currently resides only in the hands of technologists" [24]. There are efforts, such as [24] to put the power of issuing IOUs in communities by and for their own members in a "single app, rather than different ones for different associations and retailers" [24]. "It provides commons and associations with instruments to help finance themselves with tokens representing prepaid cards, crowdfunding, complementary currencies, to share tools and infrastructures with tokens representing access rights" [24]. The impact of the financial inclusion initiatives is still marginal, but blockchain can be a suitable infrastructure for CCs especially due to its ability to tokenize assets [24]. [22] also uses a DLT to create a system where "businesses can raise money by selling claims to their future goods and services at a discount" [22], which can also work as a medium of exchange as the claims are tradeable [22].

2.3.2.C RQ2.1 Solutions and Innovations: CN's Routing Privacy

Multiple solutions were presented to ensure privacy in credit networks' routing, which include: path mixing ([13]), use of the Trused Execution Environment (TEE) on a centralized payment path provider ([11]), or by designating a subset of users who serve as routing helpers ([12]) (landmark-based routing), probing ([15]), edge-colouring routing ([16]) all of which present their algorithms.

PEAR is "a centralized routing architecture for credit networks, which preserves the privacy of routing with high performance" [11]. Along with privacy, PEAR focuses on scalability and efficiency of routing, as previously proposed routing schemes (*e.g.* SpeedyMurmurs and SilentWhispers) lacked those qualities [11]. Other related work focused in using a "centralized privacy-preserving scheme for credit networks with the help of trusted hardware and oblivious computation mechanism" left unresolved issues regarding the entity who is in charge of possessing the trusted hardware, the reason for that trusted hardware being trusted by other users, and the interaction of the (assumed) malicious (but rational, meaning it does malicious activity when there is benefit to it) service provider and the trusted hardware without leaking sensible information [11]. Intel Software Guard Extensions (Intel SGX) "allows the applications running in it to initiate trusted execution environments called enclaves, and lets the enclave process run in a secluded manner where other processes, even with high privileges, cannot read or modify its memory pages" [11], thus providing data and code integrity and confidentiality [11]. PEAR's routing algorithm is executed on an enclave, which receives the users' (payer and payee) identifiers and signatures and the amount of credit to transfer, and returns the payment path in an onion routing (as Tor does) to preserve privacy of the payment path as well [11]. The integrity of the execution of the correct code in the enclave is sustained via remote attestation, in which the user is provided with a cryptographic proof of the state of the remote system [11]. The routing algorithm uses an "Oblivious RAM scheme, to protect the access pattern of the enclave and prevent sensitive information from leaking during path computation" [11], particularly to prevent the side-channel attack vulnerability discovered in Intel SGX [11], thus ensuring confidentiality. Oblivious RAM (ORAM) assumes the memory is not trusted. It "read[s] a set of encrypted data blocks during every data access, then shuffle and re-encrypt them before storing the data back, making it difficult for the attacker to determine which data block is really being accessed" [11] (in subsequent accesses). Particularly, the used algorithm (Path ORAM) uses a full binary tree, where each node can contain blocks of valid data or *dummy blocks*, undistinguishable to the attacker as they are all encrypted [11]. After securely retrieving the data, a modified Dijkstra algorithm is used to find a payment path [11]. The authors regard the performance results as practical for real credit networks, despite exceeding 1 second, with low memory and communication overhead (since it is centralized, one request is sufficient) [11].

BlAnC (Blockchain-based Anonymous and Decentralized Credit Networks) addresses the same issue of privacy as [11], but for a DCN. They "propose an alternative to proposed landmarks-based routing and DCN maintenance techniques [...], by having a subset of users facilitating transactions, termed routing helpers (RHs)" [12], which are a group of volunteering nodes (incentives and mining fees are out of scope) that can change over time and collude (penalizations are out of scope) [12]. Most previous works either don't take into account user and transaction privacy (*e.g.,* the routing algorithm Flare of the Lightning Network) or are centralized [12]. "[S]ince there is no central server to manage the network/users, find paths, and route payments, operation and maintenance of such distributed credit networks is more challenging" [12]. In peer-to-peer networks, the nodes only know their immediate neighbours, "but the [network] design offers better privacy guarantees and is intuitively more resilient against failures" [12]. As a relevant example, SilentWhispers uses landmark-routing, each landmark joins the paths of two BFS that in runs on regular time steps, one rooted at the sender and the other in the receiver, both targeting the landmark, forming a payment path [12]. This scheme is not concurrent nor scalable, but vulnerable to deadlocks, and has constraints of users joining the network at particular times [12]. Blanc solves the above problems of the two most relevant related works, and it ensures transaction privacy, accountability (transactions are published in the blockchain, and it is possible to identify malicious agents); transaction splitting among multiple paths (hampering transaction linkability); transferring dynamic amounts; concurrency and efficient on-demand routing (no pre-computed routes) [12]. When a node wants to join the network, it "needs to find at least one network node that is willing to extend credit to, and/or receive credit from it" [12], share their public key and agree on (by double-signing) a credit amount (link weight) [12]."All nodes, in BlAnC are part of a Blockchain" [12], "thus high mining complexity (proof-of-work) is not essential in BlAnC" [12]. When they figure out a path, they add it to their message pool and broadcast it to write it on the ledger. It is assumed the existence of routing helpers who don't know the identities of the sender, receiver, and intermediary nodes and "help set up checkpoints, which minimize the number of rollbacks, shorten the length of a path segment along which a failed transaction (or path set-up) needs to be re-tried, and provide resilience" [12] (rollbacks are necessary when "a transaction does not go through successfully (after multiple retries)" [12]). BlAnC is divided in three phases: Find Route, Hold and Pay. In the Find Route phase, the sender and receiver agree on the credit amount, number of paths and two routing helpers to segment the routes [12]. In the Hold phase, all nodes in the selected paths sign hold contracts with their neighbours "specif[ying] their current and future link weights" [12]. Finally, in the Pay phase all nodes receiving the pay message without the exceeding timeout, sign the pay contracts as it means the hold phase succeeded in all the nodes of the path [12], and it is safe to commit the transaction. Being n the number of transactions for a given amount, and k the number of nodes in the transaction, the Find Route phase is $O(n)$, Pay and Hold phases are each $O(k.n)$.

PathShuffle is a transaction anonymization protocol that uses Path Join for the atomicity of the transaction and DiceMix for path mixing [13]. It's the first attempt at addressing the absence of privacy preserving protocols on DCNs, more precisely, on the Ripple network, just as an example, extensible to any credit network that uses a distributed ledger [13]. Ripple supports the transaction of fiat currencies, cryptocurrencies, and user-defined currencies [13, 25]. Previous works comprise centralized protocols for path mixing, and "theft-resistant mixing protocols for cryptocurrencies" [13] that are incompatible with the nature of IOU transactions in CNs such as Ripple [13]. The heuristics for the deanonymization attacks are ("this technique can be used to link wallets belonging to the same user by examining the correlation between transactions and the credit network topology" [13]): (1) when exchanging bitcoin for I Owe You (IOU)s from the ripple network, "The sender wallet in the Bitcoin transaction and the receiver wallet in the Ripple transaction belong to the same user, and the remaining two wallets belong to the online exchange" [13]; (2) when analysing the hot-cold wallet mechanism, "a cold wallet can be identified by examining the network topology as it only has outgoing links" [13], as it "only sends IOU to hot wallets" [13]. While in cryptocurrency networks, it's possible to gain anonymization by grouping several transactions into one and executing them atomically (*e.g.,* CoinJoin), as the transaction can have multiple inputs and outputs, credit networks don't have the same functionality (*i.e.,* multi-input-multioutput transactions) [13]. Therefore, anonymous transaction in CNs such as Ripple "can be achieved by mixing the paths used in a set of transactions" [13]. The key idea is that IOU paths can be mixed if they share a common node [13]. Assuming each user has an input and output wallet and all wallets have links to a gateway in the Ripple network and everyone agreed on transferring x IOUs from the input to the output wallets, then the pair of wallets belonging to the same user can't be known if the transactions happen atomically (either all are performed or none) [13]. The issue is that the gateway, in this process, must be trusted not to revel the input and output wallets of a user and not to steal the credit transferred to it, but to create credit links [13]. Therefore, [13] propose a decentralized path mixing (PathJoin) approach which do not require any trusted third party such as the mentioned gateway, by using shared wallets, which "only when all users agree, a transaction involving the shared wallet is performed" [13]. PathJoin ensures atomicity with the use of two shred wallets and the mixing is performed with DiceMix, a P2P mixing protocol [13].

P4PCN(Privacy for Payment Channel Networks) is a proposed lightweight, anonymous and scalable protocol that preserves privacy in probing-based routing algorithms by using path probing [15]. "At its core, PCN relies on routing to find payment paths with sufficient fund balances, and employs a multi-hop payment contract to secure indirect payments via the network" [15]. "To improve routing success, many algorithms employ probing, which actively gathers up-to-date network information before making routing decisions" [15]. While the transparency of blockchain transaction makes it difficult to provide unlinkability (anonymous blockchain provide only pseudonymity), "PCN has a natural advantage for privacy, as most transactions happen within channels without being published" [15], making it possible to hide "information such as user identity or location, and the transaction value, can be hidden from external adversaries and curious intermediate nodes" [15]. Contrary to onion routing (also used for anonymous communication), in path probing (*i.e.,* "information gathering process" [15]) routing "the sender may not know the path(s) that the probe will traverse in advance" [15], therefore doesn't know the public keys of the nodes on the path. P4PCN proposed that nodes in the path derive the symmetric key with the sender, a modified "Universal Re-encryption [URE] protocol is used to re-encrypt the probe at each hop" [15]. URE "enables mix nodes to re-encrypt an encrypted message without knowing the public key used for encryption" [15]. P4PCN uses URE to carry out Diffie-Hellman Key Exchange (DHKE) with each node as each intermediate node has to add data, which must be kept secret from the remaining nodes but not from the recipient, who should be able to decrypt it [15]. The URE "modified to additionally use the symmetric keys to encrypt and re-encrypt the data each node attaches to the probe" [15]. The data is serialized in "a reversed onion: each node wraps a layer of encryption over the received payload plus the newly attached DH-value and data" [15]. "In path probing, the sender sends out probing messages to gather information from network nodes. Each node attaches the queried information onto the probe, and then forwards the probe to one or multiple next hops, until each probe reaches the intended recipient" [15]. To know if a node is the ultimate recipient of a request, each time a node receives a request, it decrypts it and tries to decrypt the interior message [15]. To protect against linkability in the case two colluding nodes receive the same request from the same node, P4PCN generates a random pair of secret keys for each node a node forwards the probe [15]. It also protects from a node estimating its location in a path based on the length of the message by using padding, which makes all requests of the same length [15]. But P4PCN uses the padding to allow the sender to pre-define the maximum number of hops, as "[i]f a path is too long, both the risk of a failed payment is high, and it may incur a high transaction fee at the sender" [15]. "Comparing [this] protocol with another possible protocol derived from hybrid universal mixing, [this] protocol has constant probe creation and processing overheads, lower (although linear) probe decryption overhead, and smaller communication overhead" [15].The authors mention that this protocol may find application "to find a trust path in a trust-based social network" [15].

Edge colouring-based routing protocol for Path-Based Fund Transfer (PBT) solves issues underlying landmark-based routing on offline channel networks, such as privacy (when landmarks collude to infer the recipient and sender) and DoS attacks on landmarks [16]. Landmarks are "nodes with high degree and willing to facilitate PBT execution [which] may be in exchange for transfer fees" [16]. PBT consists of routing (find path), probing (test path), create a sequence of contracts on probing, use onion routing to execute them sequentially [16]. "In a landmark-based routing, each landmark maintains two rooted trees with itself as the root, one tree with incoming edges and another tree with outgoing edges" [16], a path from the sender to the landmark and another from the landmark to the receiver are found and combined to form the PBT path [16]. If the identity of the receiver is known by the landmark, the path will be known as well as it is unique in trees, which "can lead to censoring the PBT execution or altering PBT transfer fees as the PBT execution path can be anticipated" [16]. In [16]'s edge colouring-based routing protocol, "each peer finds and maintains a few small subgraphs of the channel network with a particular topology" [16]. The protocol uses a special form of edge colouring, road-colouring, where a "graph can be coloured in such a way that certain nodes can be assigned a unique sequence (synchronising word) of edge colors" [16]. A synchronising word (*i.e.*, an edge colouring sequence) may be repeated several times to follow coloured edges until eventually reaching the correct node, "[hence] it creates ambiguity about the start location" [16], hiding the identity of the sender and receiver [16]. Then, isomorphic graphs satisfying topological road-colourable graph constraints are created for each offline channel so that multiple nodes can be reached by following a synchronising word (reachability) [16]. Multiple graphs are created since "the constraints on the structural properties(aperiodic, even out-degree, strongly connected) makes it difficult to convert any arbitrary graph into a roadcolourable graph" [16]. Finally, the protocol attempts at finding a path from the receiver to the sender using the synchronizing word of the receiver [16]. In this protocol, "[e]ach peer will create at least one road-colorable subgraph and broadcast this graph information to all peers" [16]. "[F]inding road colarable is an NP-hard problem" [16], however, the authors claim it "efficiently generates a road-coloarable graph with 8 nodes" [16]. Moreover, the evaluation (which used Bitcoin Lightning network data) showed that this protocol performed better than landmark-based routing in terms of the disconnected groups of nodes when increasing the number of failed nodes (difference is significant), as well as an increase in the success rate of fund transfers and the average number of attempts, meaning there are more paths for PBT with the edge (or road) colouring based algorithm [16].

2.3.2.D RQ2.2 Solutions and Innovations: CN Channel Imbalance and Payment Throughpout

The reports [18], or its full version [26], included as a backward citation for being referenced in [18] and including results and algorithm details, "propose a two-step rebalancing process wherein a node whose link weights are low or close to zero, can create fresh incoming links in a process called balance transfer, and then create fresh outgoing links in a process called as bailout" [18]. *Balance transfer* consists in creating weighted incoming links directed from existing users, and *bailout* of creating outgoing links directed to new users, both of which operations are part of the proposed rebalancing mechanism [18]. Previous works in credit networks focused on privacy and security, however, "not much work has been done in the area of rebalancing link weights of a user that has run out of credit" [18] which blocks the flow or new routing thorough the exhausted link [18]. Rebalancing thus help a node become [26]. "[O]ne way for it to rebalance its links would be to extend credit to, and borrow from new users" [18]. "[A]ny user can disconnect from an existing lender and transfer credit links to a new lender node offering a lower rate of interest" [18]. In *balance transfer*, a routing algorithm is performed using prefix embedding to find the shortest path, which creates a spanning tree (children IDs have the prefixes of their parents IDs) where the hop distance is reflected by depth of the tree, and Chord, “a routing algorithm built using distributed hash tables for peer-to-peer networks” [18]. In *bailout*, “a trusted, highly connected party such as a bank, [called a landmark], or a credit union temporarily lends credit to a node [in exchange for a fee], say, D, so that D can establish outgoing connections” [18], it “will use the fact that is is highly connected, and temporarily connect D with several other nodes in the network with whom [it] has a direct connection” [18], if none accept the lending offer, the landmark will connect D to new nodes [18]. Experiments using routing with Chord in balance transfer take roughly half a minute, while using the prefix embedding algorithm take less than a second [26].

Unlike [18], [17] mentions that “[r]ebalancing usually comes at a substantial cost (high transaction fees, confirmation delay) and should be avoided to the extent possible”, therefore, the study is focused on “study[ing] the throughput of a credit network in the absence of external rebalancing” [17]. We searched for forward citations of this work on Google Scholar, which didn’t yield citations of interest to our study, but it linked to a summarized version of this paper [19], which we included in our research as the full version is highly technical and extremely detailed, and a higher level perspective helped to understand better. This study proposes a peeling algorithm, “inspired by decoding algorithms for erasure codes [...] that can be used to bound the number of deadlocked channels in the network” [17]. “[A] central performance metric in credit and debit networks is throughput: the total number of transactions a credit network can process per unit time” [17]. However, “because channels impose upper limits on credit (respectively debit) in either direction, transactions cannot flow indefinitely in one direction over a channel” [17], hindering the network’s throughput [17]. Imbalanced channels “depend on topology, user transaction patterns, and transaction routes” [17] and can lead to deadlocks [17]. According to [17], the existing systems that try balancing channels in CNs “currently lack an understanding of how network topology and channel imbalance impacts the throughput in credit networks”, which is the gap [17] is filling. “[D]etermining whether an arbitrary topology is deadlock-free is NP-hard” [17], but “it is possible to identify subsets of edges that are provably deadlock-free in polynomial time” [26]. Thus, this study designs “a “peeling algorithm” that bounds the number of deadlock-free edges in a credit network” [17]. Intuitively, the peeling consists “iteratively identifi[ying] channels that cannot be deadlocked in a particular direction, owing to flows that traverse them in that direction and are not blocked elsewhere” [19]. LT codes have each encoded symbol correspond to an input symbol node (, or multiple, and vice-versa) forming a bipartite graph which is used in the peeling algorithm with modifications [17]: while the LT codes algorithm removes encoded symbols that have degree of 1 in the bipartite graph, in the peeling algorithm “flow is removed only after it reaches degree 0 when every channel that it uses is covered in the color opposite to the direction of use” [17]. The “peeling algorithm takes as input a credit network topology and a set of flows (paths) in use” [19]. The bipartite graph in the peeling algorithm has “flow and channel partitions [and e]dges connect each channel to the flows that use it” [19]. “The connecting edge is colored red if the flow uses the channel from left to right and blue otherwise. The peeling process colors each channel node red or blue [...] and determines if either color results in a deadlock" [19]. "[E]very flow traversing a single channel (called flows of length 1 [i.e., nodes from the flow partition with degree 1]) constrains the channel's possible deadlocked state to one color" [19]. The algorithm "look[s] for such channels with flows of length 1, assign their remaining possible deadlock color, and "peel" [i.e., remove] those channels from the flows using them in the un-deadlocked color's direction" [19] which generates new flows of length 1. The process is repeated until no edge is found to be deadlocked "or the procedure gets stuck providing a lower bound for the number of deadlock-free channels" [19]. [19] finds that "scale-free graphs have fewer deadlocks and achieve better worst-case throughput than random regular and Erdos-Renyi graphs when the network contains fewer demand pairs, but achieve lower throughput when the network is heavily utilized" [17].

2.3.2.E RQ2.3 Solutions and Innovations: CN Graph Topology Lessons

Graph Analysis of Ripple. By analysing the data from the Ripple network from January 2013 to August 2017, [25] conduct a study on the health of the Ripple blockchain. Their "work motivates the Ripple community to enhance the health of the network by educating users on improving their connectivity and setting the upper limits of their credit links well below the default value" [25]. Their findings include that "[t]he ratio between wallets and credit links has however remained constant and hence the network density is decreasing"; the gateway nodes are the key players of the network, the "wallets are dynamically grouped into geographically demarcated communities, where each community is defined by (on average) two gateway wa llets" [25], Ripple's "path-based IOweYou (IOU) settlements across different (crypto)currencies conceptually distinguishes the Ripple blockchain from cryptocurrencies (such as Bitcoin and altcoins)" [25]. "[T]he Ripple network essentially is a weighted, directed graph where nodes represent wallets and edges represent credit links between wallets" [25]. The credits upper bound can be customized by the wallet owner, and "each wallet is associated with a non-negative amount of XRP" [25] (the Ripple's blockchain cryptocurrency) "initially conceived perhaps for users to pay a small fee per transaction towards curbing denial of service attacks and unbounded wallet creation (or Sybil attacks)" [25]. Ripple wallets are "governed by a pair of signing and verification keys" [25] and "[a]n encoded version of the hash of the verification key identifies the wallet" [25]. To be valid, operations (transactions, updates of credit links, exchange offers) must be signed with the signing key of the wallet, and the resulting signatures are verified with the verification key [25]. "Ripple allows two types of transactions: direct XRP payments and path-based settlement transactions" [25]. "A gateway is a well-known business wallet established to bootstrap credit links to new wallets in an authenticated manner" [25]. They "are the Ripple counterparts of user-facing banks and loan agencies in the physical world" [25] and "maintain high connectivity" [25]. "A market maker is a wallet that receives a certain currency on one of its credit links and exchanges it for another currency on another credit link, charging a small fee" [25], these wallets are known by publishing exchange offers [25]. "In the Ripple community, rippling denotes the redistribution of credit on the links for each intermediate wallet as a consequence of a transaction" [25]. In this Ripple's lifetime analysis, a "trend showing that wallets and credit links grow at a similar rate and new wallets enter the Ripple network by connecting to a few existing wallets" [25] was found. Regarding the Ripple's graph properties, they discovered that "the Ripple network is a sparse graph" [25], "the core of the Ripple network has higher connectivity than the periphery" [25] and "most graph properties remain stable over the Ripple network lifetime except density, which has continuously decreased" [25]. The exchange offers are used in a considerable part of transactions; most transactions require intermediate wallets [25] and "the Ripple network has gateways as key players" [25]. This study "extracted 77 communities of sizes ranging from 3 to 23869 wallets", "discarding 61 communities that are not associated with a known gateway. The discarded communities are the smallest communities [...] found, with sizes ranging from 3 to 999 wallets", most of the analysed communities are from Europe, China, Japan, Israel, Australia, and Korea [25]. "[T]he core of the Ripple network provides high liquidity and the bottleneck for transactions are the credit links from the users. In terms of liquidity, the Ripple network is similar to the current banking system, where the major banks hold more credit than their customers" [25]. Rippling "can induce a redistribution of credit from a more valuable to a less valuable issuer without the specific consent of the involved wallet's owner" [25] and "actual market value and stability of the credit depends on the issuer of such credit" [25]. "[A] wallet is prone to rippling if it has at least two credit links with no_ripple = false (i.e., they allow rippling) and they hold credit in the same currency" [25], the no_ripple flag was added and by default its value is set to true, but there is still a significant value in links prone to rippling resulting from the lack of users' education [25]. "[A]ctive users can [...] opt for dynamically adjust the amount of credit prone to rippling and add a rippling fee to it", whereas less active users should avoid it [25]. "[T]he Ripple network still has a few wallets that are "too big to fail"" [25], "it is necessary for many users to increase their connectivity and split their credit among different credit links to avoid losses due to the failure of a handful of wallets" [25], *i.e.,* add credit links to prevent losing a considerable amount of credit due to a faulty gateway, and market makers should "periodically update their offers according to the real-world exchange rates, as they otherwise risk several hundreds of thousands of dollars" [25].

Graph Topology Effect on Liquidity Theorems. The study [20] formally introduces a set of theorems related to graph properties under node constraints (e.g., "every node is disallowed from borrowing more than some quantity in aggregate from its neighbors" [20]). The study proves the following theorems. (1) If a network constraints agents to issue less than aggregate limit (c_v) minus the initial score k_v notes (*i.e.,* $c_v - k_v$) then properties of the networks such as route independence, cycle equivalence, transaction equivalence (defined in [20]) and symmetric transaction distribution are maintained. The score vector of a valid configuration C of a node v is the weighted outdegree of v in C, or $S_v(C) = \sum_n w(v, u)$, where $w(v, u)$ is the weight of the link vu [20]. "for a given credit network, a score vector uniquely captures a cycle equivalence class" [20], as "[w]hen the payment is along a cycle, then, the score vector is invariant" [20]. "This theorem shows that independent restrictions on node behavior preserve most useful properties of credit networks" [20]. (2) Any predicate that is well-defined in terms of cycle-equivalence (definition: "Two configurations are cycle-equivalent if and only if one is reachable from the other by routing payments along cycles" [20]) will preserve the properties mentioned in the previous theorem. "[T]he total amount that a group of nodes has borrowed from other nodes is invariant within a cycle-equivalent class. Hence, restrictions on group aggregate borrowing [...] are well-formed predicates" [20] such as constraining "that agent v_1 can pay agent v_2 but only if it owes less than a certain amount to v_3" [20]. (3) The liquidity of the network can be calculated in polynomial time if the graph's topology is a tree [20]. (4) The probability of failure between any two vertices i,j, in a star graph with centre vertex u, whose score is lower than $\sum_i c_i/2$ (capacities of edges to u's neighbours), is at most $4/(c_i + c_j)$, and "constraining the star has not significantly reduced liquidity" [20]. (5) Constraining every node's score to a specific bound based on weighted degree of each node and a positive integer lower than the edge expansion (integer) makes the graph equivalent to the star graph [20]. (6)(Conjecture) The addition of an edge to a graph decreases liquidity at most for a factor of $1 - 2/h_G$, where h_G (integer) is the expansion of the graph G [20]. The *Braess's Paradox* ("the paradox is the observation that adding roads in a road network can reduce the overall throughput of the network, when drivers choose routes selfishly" [20]) can happen in credit networks. "[A] star-like design where every agent has a global lending limit achieves the optimal tradeoff between liquidity and total escrow costs" [20]. However, these conclusions lay on the assumption "that a unique stationary distribution exists; [which] happens if there are not two sets of agents that never transact with each other" [20].

Graph Topology for Crime Detection. To track financial crimes on blockchain, such as money laundering, [21] proposes Topological Data Analysis (TDA) by "identify[ing] anomalous patterns in higher order graph connectivity" [21], "one of the most robust tools for blockchain data analytics" [21]. This study's postulate is that "anomalous higher order patterns can be detected using geometric and topological inference on graphs" [21], resorting to "clique persistent homology" [21]. Persistent homology "provides systematic mathematical means to extract the intrinsic shape properties of the observed data" [21]. Clique persistent homology tracks cliques "over the filtration and quantifying lifespan of topological features/shapes such as loops, holes, and voids that appear and disappear at various thresholds" [21]. TDA focuses on the topological features that present higher lifespan after the clique filtration [21]."TAD method is designed to associate anomalies in the sequence of multilayer networks to anomalies identified from the time series of their topological summaries" [21]. "Dynamic networks such as Blockchain transaction graphs tend to be sparse" [21] because it is inexpensive to create an address without providing identity, and some communities encourage the creation of one time use addresses (for each transaction) [21] to preserve privacy. Since it is sparse, the weighted adjacency matrix is replaced with the geodesic distance matrix, as this representation "reconnects node pairs that have a commmon path" [21]. The algorithm for TAD consists of two steps, first, transforming the data and performing the filtration using persistent homology, second, employing a "change point detection algorithm for univariate time series" [21] to detect the anomalies. Experiments with Ethereum and Ripple show high accuracy in detecting anomalies comparing to single layer algorithms.

2.3.2.F RQ2.4 Solutions and Innovations: IOUs

[23] propose using SLAs as a CC, in terms of performing a role of medium of exchange to "encourage resource sharing between peers" [23]. Previous work include the iWAT, the internet version of the peer-to-peer WAT, "a debt-oriented system using WAT tickets [issued by the participants] as mediums of exchange" [23] whose value is dependent on the participants' expectation of the future value of the good that it represents [23]. CCs usually have a devaluing mechanism to prevent hoarding and foster exchange [23], which is also the case with iWAT, as "reduction in the value of tickets accelerates spending [...], as buyers are able to purchase at a lower perceived cost" [23]. The Ripple Protocol (version of 2004, did not use blockchain) is also present in the related work, it "enables trustworthy 'IOU' exchanges defining particular trusted connections for each currency" [23]. The welfare in these systems is correlated with bankruptcy rates and whitewashers (users who leave and join the network with a new identity to their advantage) [23]. An SLA "refers to a service that is to be provided in the future" [23]. "Penalties and rewards are also parts of the SLA template" [23]. If a better offered is presented to the holder of the SLA, they can forward this SLA to another node, and can be redeemed (during the redeeming period, its values cannot be changed) or expire [23]. In the presented protocol, it is possible to issue (by asking a node the list of their services or delegated services — both are SLAs in the list), forward (provide a delegated SLA to another node) or redeem a SLA and it contains the ID of the issuer, context (expiration date, agreement metadata), service terms and guarantee terms (conditions for the agreement to be valid, penalty terms) [23]. The assumptions made for this protocol are that the "service provider does not care about the identity of the client" [23], that a client will prefer to purchase SLA indirectly as they are cheaper (when no longer need a service, the node that is selling the SLA will sell it cheaper than the provider of that service), and the SLA is eventually converted to a physical currency (provider is paid in the SLA issuing phase) [23]. In short, the system from [23] functions as follows. A service (or product) provider issue a SLA which they sell at a certain price, other nodes in the network buy the SLA, either because they need the service contained in the SLA or they speculate the value of it will increase in the future, and pay for it with *real* money. If the person does not need the SLA any more (found another with a better price, or simply do not want it) or want the profits from their investment, they can sell it again

(*i.e.,* forward it) to other peers, with a discount comparing to the market value, either recovering part of the money they had spent initially or making a profit. The simulations use a framework for simulations of peer to peer algorithms using a Poisson distribution, and [23] discovers that the high level of circulation of SLAs and the scalability of the network improves overall benefit, as well as having different types of SLAs (a variety of services or products) [23].

[24] construct an Ethereum Decentralized Application (dApp) that gives the "general public the ability to create new cryptographic tokens for their own purposes" [24], economic and social [24]. These tokens can be used to represent discount coupons, prepaid cards, access rights to establishments and shared resources, tickets, *etc.* [24], "or can be purpose-driven tokens that incentivize individual behaviours towards common goals" [24]. Previous work using blockchain include financial services for the unbanked, microcredit initiatives, charitable donations, complementary currencies, *etc.*. Blockchain tokens can be native (or protocol level), when the token has its own blockchain and the value of the token is linked to its mechanism, or application level, which are created on top of other blockchains and tokens and the transaction fees are paid in native tokens [24]. "A smart contract in the context of blockchain technology is [...] "executable code that runs on top of the blockchain to facilitate, execute, and enforce an agreement between untrusted parties, without the involvement of a trusted third party"" [24]. CommonHoods supports issuing coins ("prepaid cards, cashback initiatives, and complementary currencies" [24], can serve to pay for crowdsales), coupons (after being sent to the issuer cannot be put into circulation again unlike coins, usually are the object of crowdsales), *crowdsales* (a type of crowdfunding, which after the purchase sends the purchased coupon tokens to each member from the crowdfunding) [24]. CommonsHoods has two types of users, the individuals, and institutions, commons, associations, *etc.*, which is mapped to a social network *FirtLife* to be found by users [24]. The architecture of the dApp includes a webApp, wallet (transaction authorization), OAuth2 authentication, connection to the civic social network FirstLife, a proxy to call smart contracts, access to the API of the storage for binary assets such as images and documents (using IPFS network) [24]. The blockchain is a consortium with Proof-of-Authority for the consensus, meaning that "anyone can connect to the network with a simple node, but sealers are pre-authorized and well known to the network" [24], "sealer nodes [...] decide the next block that can be attached to the blockchain" [24]). The authors resorted to OpenZeppelin Contracts for the development of three smart contracts (two ERC20 for tokens and crowdsale, and one DAO for crowdsale management) [24].

Building On Local Trust (BoLT) is a system that allows businesses issuing coupons with a discount redeemable in the future to raise funds [22]. Thus, the community is the main investor in their local businesses [22]. Moreover, these coupons can be used to exchange good at different stores, which may accept other business's tokens as payment for their own goods and services [22]. "BoLT combines ideas from past implementations of local currencies and discounted gift cards with modern cryptographic primitives and cryptocurrencies" [22]. Previous work on simulations of P2P networks where agents offer services to each other show that welfare increases as scrip is added to the system [22]. BoLT uses *trustlines* (credit lines) "to guarantee that they will accept another user's BoLT up to a certain amount no matter the state of the world" [22]. This solvency guarantee that creates a bound to the loss of a defaulting agent "might not help with liquidity crises and even exacerbate them" [22] as the reason for the defaulting agent may be that their bolts (the IOUs of BoLT) weren't easily tradeable [22] *i.e.,* not widely accepted. A bolt is issued by a business, corresponds to a good or service from that business worth a certain dollar amount [22]. A bolt that can be redeemed in the present is called a *certificate* and before the maturity date it is a *commitment* [22]. BoLT uses a public ledger and a wallet to register changes in the ledger, all the transactions are made public "allowing users to determine for themselves which bolts are useful" [22]. Bolts can have options, such as to be redeemed for fiat currency and to have an interest rate to incentivize their purchase [22]. This enables users to help their local businesses and buy an asset, as the bolt will be worth more than its original amount [22]. To create bolts, the BoLT API is called to first create the bolt specification (creates a new kind of bolt), then users who issued that bolt can mint it to create several instances of that bolt [22]. The bolts can be transferred, exchanged with other bolts by proposing an exchange offer or destroyed [22]. Other businesses can mint and accept others' (businesses to whom they extended their trust) bolts [22]. It is also possible to buy back issued bolts to reduce the interest burden [22]. After a purchase in the store, bolts are presented on the customer's wallet app to the point of sale (POS) terminal of the business [22]. Wallets process the web of trust from the truslines and enforce that the seller accepts their own bolts and the bolts from their trustlines [22]. Clients can negotiate for the business to accept other bolts [22]. However, if none of the bolts from the client's wallet is accepted, the seller can issue (mint) their bolts on the spot and sell to the client, or the client can see the exchange offers of bolts from other users [22]. Since the graph of trustlines can be sparse, resulting in difficulty to have exchange bolts at all times, BoLT introduces bridge bolts to serve as a common medium of exchange, which can be general bolts (such as Ripple and XRP) or a representation of a fiat currency, the latter issued by a trusted entity that mints one representation for every fiat unit deposited [22]. The "failure to honour a bolt in the real world" [22] is reflected in users' interest on the bolt [22] in exchange offers, working as an intrinsic reputation mechanism. "Previous approaches for enforcing the rules of ledger-based cryptocurrency systems have been to assess a penalty, recorded on the ledger, against the non-cooperating party such that they lose more value than the party they hurt" [22].

By measuring the shortest path between an issuer of a bolt and the trading circle of a user, or the maximum flow of bolts between the trading circle of the user and other bolts issuers, or the bolts' velocity (the amount of bolts in circulation), it is possible to evaluate the acceptability of a bolt based on the trustlines and bolts in the network making informed decisions to accept bolts [22].

Simulations of BoLT led to the following conclusions: if traders only accept bolts 1 hop away, the utility is worse than fiat currency, but improves as users extend trust [22]. “This simulation is in some sense a worst case for BoLT since claims have no interest, there are no trustlines, and no one can create or mint new claims” [22]. Operations in BoLT have polynomial complexity (quadratic at most), but the overhead with the implementation in Ethereum is too high so the authors propose implementing BoLT on a custom ledger [22].

2.3.2.G RQ3. What are the main technological challenges or future work of the solutions?

Privacy. The PEAR private routing scheme was described “with a single payment path provider, which cannot provide high service availability” [11], “a system with multiple providers to achieve higher robustness” [11] is a proposed future work. The future work of BlAnC is to be implemented “in a real-world testbed like Hyperledger” [12] and the “impact of real-world network dynamics on the protocols’ stability and scalability” [12] to be tested. PathShuffle, the credit mixing protocol, mitigates heuristics that allow linking accounts on a public credit network (such as ripple), and the future work comprises studying the effectiveness of the protocol empirically on the network [13]. It is important to experiment it given that “Ripple applies reserve requirements to each new wallet in order to prevent spam or malicious usage” [13], which is why creating new wallets for path mixing can be a burden, as it is not what wallets are for by design. Additionally, “[e]very wallet in a path might charge some fee as a reward for allowing a transaction” [13], therefore the cost of the privacy should also be assessed along with transaction success rate. Regarding Ripple, there are operations “such as rippling and exchange offers pose important security challenges” [25]. P4PCN, the privacy protocol for payment channel networks, lets the communication method used to forward the request to the discretion of each node, but they note that if broadcasts are used, it’s possible to overwhelm the network with requests until the probe finally reaches the recipient [15]. The future work of P4PCN encompasses “[t]wo promising solutions [which] are probabilistic forwarding and coordinate-based routing. The former naturally preserves privacy, while the latter can be implemented using a privacy-preserving coordinate system to avoid breaking user anonymity” [15]. Edge colouring routing (from [16]) use a NP-hard algorithm with for constructing 8 node subgraphs that hold the road-colouring graph properties. More tests need to be done to verify the impact on routing time in networks with more nodes and fewer edges, and to determine heuristics about how many nodes should be used to construct the road-colouring graph. Verifying the routing time is essential for the applicability of this protocol in a real life credit network.

Channel Imbalance and Throughput. The study [26] tested their solution on a simulator, and future work includes “to implement the idea on a real world credit network such as Ripple” [26]. The study [17] future work includes “synthesizing graphs that are: (a) easy to peel, (b) exhibit high throughput, and (c) limit the maximum degree of any node” [17]. “Another interesting direction is to analyze the peeling algorithm given the correlations induced (in the bipartite graph) by an arbitrary topology and demand pattern" [17] and "designing suitable incentive/recommendation mechanisms to achieve a desired topology in a decentralized manner" [17].

Graph Topology Lessons. Future work of [20] includes "experimental analysis of realworld Lightning networks, particularly with regard to the tradeoff between subgraph expansion, escrow savings, and implementation concerns" [20], and also "an analysis of the constrained credit network using forests" [20]. Testing how different distributions affect the results and "[u]nderstanding the incentives at play could improve designs of credit network-like systems" [20] as "[c]onstraints allow for many interesting scenarios in which to study the behavior of rational agents" [20]. To see any advances on these topics, we searched for forward citations of this paper on Google Scholar, for the relevant results, [22] was already included in our study and the rest are not relevant. The study [21] plans to advance on TAD to detect anomalies in more complex networks where each node has more information (attributed networks), and in doing analyses of the evolving communities.

IOUs. The study of using SLAs as CCs [23] suggests future work as to study the behaviours and strategies of the selfish peers. CommonsHood from [24] propose to develop their wallet app on a mobile platform and support NFTs. The most significant challenges in BoLT are: how to start the web of trust in an empty ledger, the intuitive design of the wallet since the functionality of BoLT is more complex than regular means of payment, formulae for risk profiles, and more general challenges such as insurance for handling bankruptcy, privacy vs reputation tradeoff, prevention of Sybil attacks, throughput, latency, miners incentives and transaction costs [22].

2.4 Discussion

Most studies on privacy do not include protection mechanisms from denial of service attacks, usually by mentioning in their threat model that the adversary is interested in reading private information (*e.g.,* "goal of the adversary is to undermine user privacy instead of launching denial-of-service attacks" [15], "the denial-of-service attack is out of scope for this paper" [11]). In blockchain, this lack of study can make sense as, for example, [13] mention that XRP "is used to organize transactions fees for non-XRP transactions and other fees used to prevent DoS attacks in the Ripple network". But since PCNs are offline payment methods, it should be a bigger concern (PCNs are optimizations for the infrastructure of Blockchains to allow faster payments). It is also common to leave out of scope the incentives of agents when adding them to a payment solution that encompasses privacy (further exemplified). However, it can push end users from using such systems.

PEAR [11] uses a centralized TEE with remote attestation solving the confidentiality and thus privacy, however, the study does not present a discussion on the fact that the solution is centralized, and that it is easier to achieve high efficiency and scalability in centralized systems than in decentralized networks. The study compares its centralized solution to a protocol using distributed BFS algorithms, which is an unfair comparison. Moreover, the entity controlling the trusted hardware will be a central point of failure (service availability) and the cost of using such service will be determined unilaterally, which is more difficult to happen in decentralized networks. Since credit networks are widely used for micropayments, a high cost is not expected nor tolerated by most users that have cheaper alternatives.

BlAnC [12], which uses decentralized credit networks, mention that Ford-Fulkerson or push-relabel algorithms can be used in the credit network as it is a flow network, to make a path payment, but, their time complexities ($O(VE^2)$, $O(V^3)$) are not scalable for large networks. However, payments that are of the size of the network are not common, and have a high probability to fail since the network is dynamic. Using these algorithms is only problematic due to the privacy restrictions imposed in the project, of no node knowing the destination unless it is the destination. The solution is efficient, however, the incentives for the routing helpers are out of scope, which can mean a higher price for end users, who will be distanced of using privacy solutions due to their cost.

The edge-colouring graph solution [16] uses an NP algorithm to construct the edge colouring subgraph, which was tested with data of the Lightning network. However, ¡5000 nodes and ¡6000 edges (2019 data) may not be the case of real world networks, as the lightning network may still not be very used, or not represent a real life credit network. Moreover, it is not taken into account that nodes can lie about their subgraphs. The adversary model is not presented, nor are the execution times, although it is falsely claimed to be in the abstract. Forward citations were applied on this study in Google Scholar, however, no references were yielded.

Two studies analysing the network topology of credit network claim divergent characteristics for the same data set: while study [18] mentions that "[c]redit networks are usually dense networks, e.g., Ripple [...] with several incoming and outgoing links from the nodes", another study [25]'s analysis of the graph properties of Ripple consider it to be a sparse graph. Ripple is a very popular network for studying credit networks, even the oldest paper we included (2012) mentions it ([23]).

Trading mobile minutes, as found in the context, is similar to SLA as a CC in [23]. The idea of [23] is to sell third-party services as SLAs to recover part of the initial price, or making an investment. However, the assumption that the service provider does not care about the identity of the client is not applicable in many services from the real world (hence the rise of KYCs, etc.).

BoLT ([22]), states that "[b]y allowing anyone to create, trade, subdivide, and exchange bolts, [it] eliminates monopolistic or oligopolistic tendencies that have arisen from banking mergers and reduced competition of mainstream lenders". However, since BoLT uses trust lines, and a trust line increases the probability of IOU acceptance, the more trust line a business has, the more trust lines it is prone to have, at least intuitively, in a rich-get-richer effect. The study did not present the simulation of the statement. A question that also emerged but was not answered is of the reason that BoLT does not build on Ripple, since the concept is similar. Multiple reasons may exist, such as not wanting to depend on the value of

XRP, or be associated with the XRP community (as it is not fair for the community, and BoLT may risk the reputation), but no reason was provided.

2.5 Limitations

The main limitation of this study is the absence of a team, especially on a complex and multidisciplinary topic of complementary currencies and blockchain. To compensate for the lack of academic background in economics, a SLR was conducted on economic literature to ensure that the conclusions in the part two have solid foundations and to aid the reader to follow and understand the path taken during the study. The pat one of the SLR was also purposefully included to make up for the lack of a stable bridge between economic and CSE literature. Second, research on blockchain and cryptocurrencies is still in its early phase, which can affect the quality of the studies, meaning that if the field was older, some articles would be known to be relevant, with more citations, thus accreditation.

Throughout the examination, we tried to keep a healthy level of scepticism, especially to avoid the confirmation bias that complementary currencies help the economy. Thus, studies that review the efficacy of monetary plurality in practice and conclude that CCs have no significant impact on the economy are of particular interest. Any bias or other limitation of this study unknown to us is expected to be revealed to the reader by the transparent reporting of the protocol draft, keyword search, number of papers excluded by the inclusion and exclusion criteria and explicit mentioning of the accepted papers. "A published review should even be somewhat "vulnerable" by publishing its procedures because such vulnerable transparency helps advance scholarly knowledge by admitting possible limitations in the procedure that could affect the review's result" [1]. In other words, the transparency of the process may reveal limitations.

2.6 Future Research

A study analysing the Ripple network [25] uncovers that the currency interoperability, as anyone can be an exchange (or market maker) and place exchange offers can reveal being dangerously insecure. There is a problem with the gateways: since they are "key players" and there are some too big to fail as they would leave a considerable amount of wallets disconnected (not mentioning the amount of money lost). The study explains how users can protect themselves from these exploitations: "[a] market maker can update a previously offered exchange rate at any time" [25] and monitor the prices for spikes or other abrupt changes and adapt their exchange offer to that. It can be interesting to research design ways to keep interoperability but have security by default (aside from the default no_ripple flag).

Studies including payment channel networks leave a discussion to ponder. In PCN, participants use a channel to make payments without committing the transactions to blockchain, to reduce costs, enhance throughput, *etc.* However, as explained in [20], the participants put an amount of money as escrow which they can freely transact between each other, and if anything happens, the transaction can be committed to the blockchain and the balance is settled. It may be interesting to design a mechanism that does not lock the money, as it is unproductive, but that maintains the security guarantees.

Although the study [20] only applies to graphs where each two nodes have a path between them, it showed that constraining agents maintains the liquidity, which is an extremely relevant result for the credit throughput of the network, for example. Constraining rational agents to understand the evolution of the network in time is also recommended for future research.

BoLT proposes "making all transactions visible to all users the ledger serves as a distributed Irish Publican; allowing users to determine for themselves which bolts are useful" [22]. However, there might be competition between local businesses and secrecy may be needed. A research direction would be to find a mechanism, such as zero knowledge proofs, that would guarantee privacy but still allow users to make the most informed decisions possible.

2.7 Conclusion

In the part one of the SLR, the definition, context, goals, typologies, and examples of CCs were presented. Moreover, the CCs comparison with fiat money was provided, as well as the benefits, economic impact, and challenges. Further, cryptocurrencies were investigated for the role of complementary currencies. Despite only one currency being investigated in the review, the results can be extended if the cryptocurrency hold the same properties, such as price volatility.

We could not find answers to economic impact of cryptocurrencies as there is not enough research yet, but it became clear the field's experts' positions regarding the acceptance of Bitcoin as a complementary currency. As it is functioning now, Bitcoin cannot be used as a complementary currency because it is not being as a means of payment in the first place, it is used as an investment, with high volatility due to the speculation caused by investor's opinions, searches, comments, tweets, and also the media, and fake news. The considerable price fluctuations also prevent Bitcoin to function as a store of value, thus further hindering its role as alternative money. Another reason to not be accepted as a complementary currency is that the technology is recent and new cyberattacks are being uncovered, multiple due to malfunctions, which could lead to devastating losses and there would be no authority to help and solve those issues, which impacts the user trust.

There is little research trying to use blockchain to leverage complementary cryptocurrencies. Ripple, as cited in multiple studies, allow for the coexistence of both, cryptocurrencies and user-issued IOUs. The areas with most focus using credit networks such as Ripple are payment privacy, agent behaviour, graph topology implications on liquidity, *etc.*. However, the most important problem of CCs found in the first part, in the context of CCs, is not being addressed.

The main obstacle for complementary currencies success has been their small size, this, in turn, leads to marginal economic impact and makes CCs a less interesting topic for economists. Moreover, it may discourage the emergence of new systems of this type as they can be deemed ineffective, which in turn, doesn't generate more research on the impact of these systems, forming a vicious cycle (see Figure 2.1). But it can also be viewed as an invitation to research and find new ways of increasing the scale of this system by providing a scalable technological network coupled with incentives to join, stay and transact frequently in the network, fostering participation. This problem is especially interesting to solve for Mutual credit, as it the only type of CC that doesn't fulfil its economic objectives, however, there are mutual credit systems that do succeed, as in WIR case. Solving this problem can increase research thus paving the way for more innovation and gather interest from economists (from a long-term perspective) and foster network robustness, which is crucial for those involved in it: they have a bigger basket of goods to trade, and more support to rely on in economic recessions. As [5] suggests, "[u]ser confidence and trust in agents and the technology used is a must, as this positively correlates with transaction volume", moreover, "an effective, supportive regulatory framework for the mobile currency seems to be a key success factor" [5], however, it is out of scope of this project. These types of system are more than economic instruments as the social component plays a substantial role for the thriving of the community. Therefore, the goal of this system should not be economic growth, but rather economic, social and (preferably) environmental sustainability, as focusing on economic growth has been linked to decreased welfare, unsustainable consumption and production patterns and devaluation of important but (typically) unpaid work (*e.g., volunteering*).

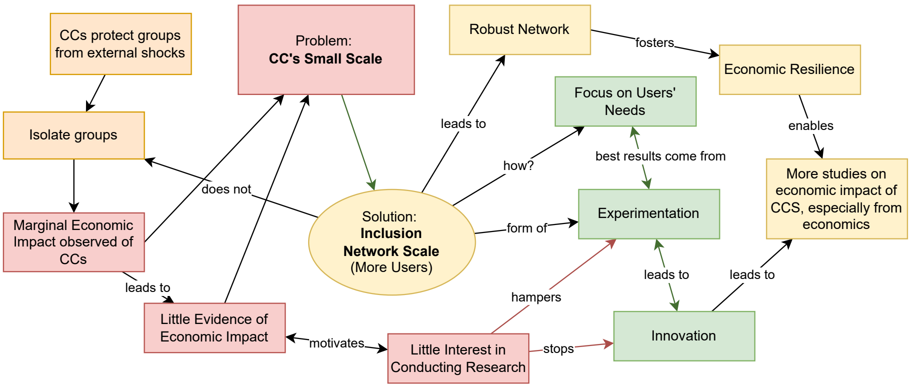
CCs protect groups from external shocks
Problem: CC's Small Scale
Robust Network
fosters
Economic Resilience
Focus on Users' Needs
Isolate groups
leads to
enables
how?
best results come from
does not
More studies on economic impact of CCS, especially from economics
Solution: Inclusion Network Scale (More Users)
Experimentation
Marginal Economic Impact observed of CCs
form of
leads to
leads to
leads to
hampers
Little Evidence of Economic Impact
motivates
Little Interest in Conducting Research
stops
Innovation

Figure 2.1: Diagram of the main problem and solution suggested based on complementary currencies research

3

Designing an Inclusive Credit Network

Contents

3.1 Rationale

From the literature review in Chapter 2, the most urgent problem that remains unattended is the **marginal impact of complementary currencies in the economy**. The potential of these systems remains in most part unexplored, as its impact is negligible in the large scale, leaving a gap in the economic literature. Which, in turn, creates a loop, leading to less experimentation, less innovation, less progress in the technological field, thus maintaining the low level of impact. A conclusion that researchers have reached is that there is a need for experimentation, rather than imitation, as it most likely leads to undesirable results. Experimentation with complementary currency systems are healthier alternatives for the community and research in this field.

Thus, our goal is to make complementary currencies large in scale. A scalable system needs a scalable technology, however, **there is no use for scalable technologies without a large amount of users**. Technological scalability can be a requirement, but it should be justified by the number of users interested in it. Complementary currency systems sought to isolate an economic or social group to protect it from the outside economy. This strategy can be the reason for their success and failure at the same time. Our approach to create a scalable system is to not isolate individuals or groups, but to **include the most significant amount of use cases** possible and build a credit network that supports them. The economy is not restricted to a small group, it is for everyone — every element should contribute and receive the benefits from being part of the system, potentially resulting in a more significant economic impact. The next sections elaborate on the solution, its use cases and requirements.

3.2 Solution Overview

In economic recessions, the economy slows down. There can be inflation, people might become more cautious on spending money when making purchases, more likely to save money than spend, slowing down the circulation of money. Small businesses are among the first entities to suffer liquidity shortages, and eventually the economy is in a state where services and products are needed, meaning there is a demand, and offer, but no medium of to settle the exchange, as there is no liquidity. This issue of fiat money, which combines the clashing functions of medium of exchange and store of value, can lead to wasted products and unmet needs, a market failure.

To overcome difficult situations such as crises, but also to help with liquidity problems for any reason, it is possible to leverage peoples' and businesses' connections and more specifically their trust. The principle is similar when people informally lend money to their friends, as they trust their friends will be able to pay back. The maximum amount lent is proportional to the confidence of the lender in getting their money back from the borrower, or in other words, the lender's trust in the borrower. Hence, trust can be quantified by one of the functions of fiat money that has been working, unit of account. This is how trust can be exchanged for currency, typically fiat currency. But it may not work when both parties need liquidity, or more generally, when most parties in an economy need liquidity. *How can we use trust as a currency without having to exchange it for fiat currency?*

Our solution builds on concepts of:

- **CC**, a medium of exchange that circulates along the fiat currency, not intended as a substitute to it but to close gaps and solve issues created by fiat currency.
- **Mutual Credit (MC)**, allowing anyone creating money according to their necessity, making the supply elastic. Typically, MC consists of ledger entries that map an entity to a balance which can be negative if they had received more products or services from others than given, or positive otherwise. Positive balances can be thought of as a claim or debt of any participant of the MC system to that party, and negative balances are the debt of that party to any other party of the system. All balances in the ledger sum to zero. The most common problem with mutual credit is acceptability, as found out from Chapter 2, that it can be difficult to redeem the positive balance when no service or product offered is desirable, which happens when the amount or diversification of businesses is small. No other party will want to exchange their negative balance for fiat money, as they would prefer to offer their service instead. Unfortunately, this is a disincentive to participate in the MC system for entities that are most wanted for this system.
- **IOUs** are claims to redeem goods or services in the future. IOUs can solve the acceptability problem from MC systems as there is accountability — owning an IOU is similar to a positive balance in MC but it is not general, it is with an entity that explicitly gave the claim, which mitigates the acceptability problem. IOUs can also be traded for profit and sold to recover invested money.
- **CN and web of trust**, allowing anyone to register and leverage their connections, and their connections' connections, to increase their credit potential proportionally to their trust relationships.
- **Credit clearing**, which consists of registering the debts of everyone, summing them up, some debts will clear others out and settling the remaining debts, saving liquidity.
- **Blockchain**, an immutable distributed and decentralized ledger to keep track of transactions and balances of cryptocurrencies.
- **Cryptocurrency**, which uses cryptography to secure the currency transactions on the blockchain.

Combining the mentioned concepts, we define a credit network, which can be represented as a **weighted and directed graph** $C_N(U,T)$, with nodes U representing the **users** of the network and edges T represent the **trust relationships** between users. Each edge $(u_1, u_2, \alpha, I_IOU)$ (see Figure 3.2) can represent the maximum amount of debt α issued by I_IOU that u_2 trusts (or is comfortable lending to) u_1. The system is dynamic, and these α in each edge can change over time. The flow in the network represents the amount of actual debt that exist in the system. It could be represented with positive and negative balances as in mutual credit, the edge maximum capacity would create a bound to the

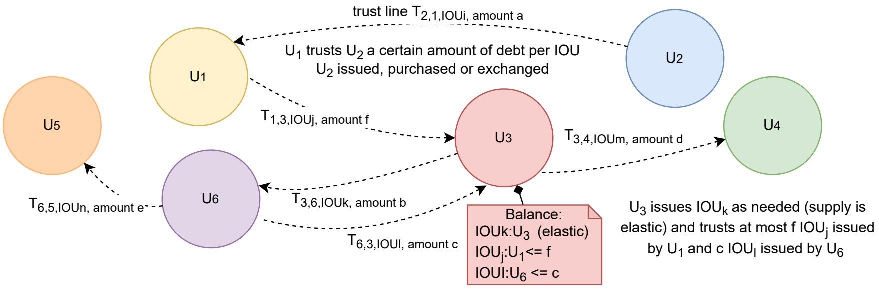
trust line $T_{2,1,IOUi}$, amount a
U_1 trusts U_2 a certain amount of debt per IOU
U_2 issued, purchased or exchanged
U1
U2
U5
$T_{1,3,IOUj}$, amount f
U3
$T_{3,4,IOUm}$, amount d
U4
$T_{6,5,IOUn}$, amount e
U6
$T_{3,6,IOUk}$, amount b
$T_{6,3,IOUl}$, amount c
Balance:
IOUk:U_3 (elastic)
IOU_j:U_1<= f
IOUl:U_6 <= c
U_3 issues IOU_k as needed (supply is
elastic) and trusts at most f IOU_j issued
by U_1 and c IOU_l issued by U_6

Figure 3.1: Overview of the credit network and trustlines

problem with acceptability. However, it is more expressive to represent the balances as IOUs, as the balance is assigned to the source of the debt, leading to more accountability, **further mitigating the acceptability problem**. Moreover, IOUs make bigger markets, as it **encompasses more use cases**, capturing the interest of more users who can employ different market strategies, which is our goal. It enables people to make payments with currencies (IOUs/debt) they trust or exchange those they do not trust with other connections. This is how **trust becomes a (scalable) currency**.

3.3 Use Cases and Incentives

To invite the maximum amount of users to the network, there should be support for a vast number of use cases that comprise users' most frequent economic activities. "A key characteristic of resilience and adaptability is diversity" [8]. The inclusion of different use cases could also help the complementary currency system to exist and be used when there is no economic crises. The incentive to join would be the size of the network, resulting from the broad use of the credit network. A list was compiled of supported use cases of credit networks and IOUs:

1. **Purchases** (supermarket, grocery stores, cinema or concert tickets, restaurant, bookshop, online shopping, *etc.*) — users can purchase products or services by exchanging IOUs.
2. **Fidelity points scheme** — stores can easily employ a fidelity point scheme.
3. **Discount coupons** — stores can easily employ a marketing scheme comprising selling discounted store points.
4. Keep **track of debt** among friends, family, colleagues, businesses, organizations, *etc.*.
5. Help (local or not) businesses — buy IOUs to redeem in the future (pre-buy).
6. **Invest** in (local or not) businesses — buy IOUs to sell at a higher price in the future.
7. Invest in **future businesses** (ICOs) — buy IOUs to redeem in the future form a business that does not exist yet.
8. Sell IOUs that are not wanted/needed any more, recovering the spent money.
9. Trade coupons (IOUs) from other businesses — even if they have the same value, some people may

value certain coupons more than others.

10. **Trade or exchange fidelity points** — fidelity points can be viewed as IOUs and can be traded or exchanged.
11. **Gig economy** — independent contractors such as Uber and Uber eats drivers can issue their IOUs when paying for products or services as the services in this emerging type of economy can are widely used and can easily be traded, and redeemed with these contractors (*e.g.,* someone who needs a ride can redeem the IOUs).
12. **Gift economy** — *e.g.,* schools can gift its students with IOUs, for good behaviour or grades, good deeds, or simply gift and have agreements with bookshops or zoos so that students can redeem. The main principle of gift economies is *the more you give, the more you will have* (from the literature review Chapter 2 - *e.g.,* Napster). In the example of the school, the behaviours that are rewarded are incentivized by giving IOUs.
13. Tipping — it is possible to tip at restaurant or for good service using IOUs, which is particularly useful when there is a recession, when money is (even more) scarce, and people are more hesitant in spending money on tips, and where it is obligatory to tip, they may consider not going thus not spending any money. With IOUs, the tips can be redeemed later with fiat currency or other IOUs.
14. Wage payment IOUs — when a business does not have enough liquidity, it can pay (or partially pay) its workers in IOUs, which can then be used to make payments.
15. Wage advancement — "employees who need an advance on wages to cover unexpected expenditure can draw on this account and avoid using their own savings or applying to some credit company and paying high rates of interest. The benefit is twofold. On the one hand, the workers do not have to spend their savings and pay interest; on the other, employers who advance wages in SRD form will save money in the following periods as their wage bill is reduced by the amount advanced" [6].
16. Unemployment IOUs / state benefits — pay with personal IOU in the supermarket and buy it back later, or future employer or state can buy it from the holder
17. Change shortage — when a customer pays for something and there is not enough change, instead of spending more than wanted, losing money or not getting the intended product, the store can issue an IOU to be redeemed later.
18. **Forgive debt** — buy debt issued by a certain entity and burn or send it back to the entity (such as the healthcare debt from literature review), certain entities holding others debt may exchange them on a discounted price to incentivize the issuer of the IOU or others buying that debt.
19. **Charity** or donations (for organizations, businesses, or individuals, not just charities) — can be done by buying or exchanging directly from the entity or from other source entity's IOUs and burning them or sending them back to the entity (forgiving debt); or simply sending fiat money or reputed and relevant for the entity IOUs to the entity's wallet, potentially making donations more transparent, or

buying a zero note worthless/symbolic currency.

20. **Time banking for community service / community currency** — organization or community can issue IOUs that are accepted in local stores, helping value informal jobs (*e.g.,* reward for finding a lost animal, helping someone with their garden — 1h of human work equals to the medium salary in that region).

Except for community currencies, other activities from the list above involve businesses activities, and it is possible this system being subjected to tax, however it is out of scope of this project.

Use cases regarding coupons or fidelity points trading could sparkle hesitance for large companies who already have fidelity schemes implemented, such as Pingo Doce and Continente (supermarkets) in Portugal. Fidelity points and coupons are strategies that draw customers to purchase items in the stores when a specific discount is available. "Spending on the part of consumers within the circuit is rewarded with credits to be spent in the same sphere [...] which offers a concrete incentive to remain inside the circuit" [6]. If the coupon or fidelity points are not spent, they are wasted, and the customer feels a sense of lost opportunity, nudging them to purchase in the store. Giving customers the possibility to exchange their fidelity points and coupons with other people (for a small profit), removes the sense of loss of opportunity and may lead to more coupons and fidelity points being redeemed than usually. While it is true that the statistics of big producers would need to be adjusted as more offers (coupons, discount) would be taken, which may result in less profit than expected. On the other hand, these offers would do their job: bring more customers, increase sales. Although strategies in the coupons or fidelity points would need to be slightly adjusted, to issue less or different offers, these adjustments are more than common even with centralized fidelity points/coupon systems, and present opportunities to reach a wider market and a bigger potential to reach sales goals. From the technological perspective, the centralized fidelity points apps can resort to the public ledger as an external database or use the microservice that exposes an API, the architecture of the solution is detailed in Chapter 4.3 and was elaborated based on the use cases.

This system enables **a trust-based marketplace of debt intended to make the economy move** when it usually slows down or stagnates. The network incentivizes to create new trust connections (and to do so, good participations are rewarded with more connections) to increase the credit potential and the acceptability of tokens, thus creating cohesion in the economy, along with resilience to external shocks.

3.4 Benefits

Bounding Loss. By giving the possibility of limiting trust, *i.e.,* the debt amount, in each connection, and by assigning the debt to IOUs, the loss in case of default (when a participant refuses to pay their debt or goes bankrupt) becomes **localized and bound**, whereas in mutual credit (MC), the entire network suffers, including users who have never interacted with the defaulting party.

Scalability and Impact. MC systems are not scalable by design, as trust in these systems is a relationship from each party to every other party, which does not correspond to the reality. At best, such relationships exist in small groups. But smaller economic groups, especially those who are most likely to participate in MC systems, do not have the potential to impact the economy as large groups do. By using CNs, large groups can emerge in a form of less connected graph than the graph of MC systems, but it more closely resembles real trust relationships. Trust in mutual credit is not scalable ([27]), while trust in CNs is.

Currency Interoperability. Zooming out on a CN, the network will look sparse, but connected. The trust relationships will enable users to trade their own produced currency, *i.e.,* IOUs, but also to trade valuable IOUs from other trusted owners of the claims, enabling currency interoperability. This benefit is vital for a decentralized monetary system, as there is no authority enforcing the acceptability of the claims. Thus, each node can issue their tokens, but it is a decision of other nodes to trust the tokens and exchange them for other tokens, making the owner of the debt the authority in a decentralized network.

Accountability and Acceptability. CNs specify the trust relationships, and IOUs work as the flow in those connectors, a special kind of flow that is assigned to the owner of the debt. This allows the holders of the claims that represent the debt to keep track of where their *positive* balance come from, which creates accountability and increases the acceptability of the claim. The root cause of acceptability is that there is an unmet expectancy between having a positive balance and being able to redeem it. CNs with IOUs remove that false expectancy, as they are more specific regarding the amount of debt that can be accepted, by whom and for whom, leading to more realistic expectations regarding acceptability. Comparing to nowadays cryptocurrencies, each node works as a bridge to other types of currencies when they exchange a certain currency for other, both of which they trust.

Free Network. No one should be obliged to accept offers they otherwise wouldn't just to be part of the network to collect benefits. A participant A might want to not allow another participant B to redeem their high positive balance, as A might never need that amount of positive balance in the network. In a sense, this is a more general scenario of double coincidence of wants (someone wants to redeem a big value the other party is, coincidentally, willing to take as they also trade that amounts), which is the reason bartering does not work. In the proposed solution, everyone is free to accept or not the IOUs, or debt, and their corresponding amount of others as they please, following their trust relationships. Every participant has more control (thus, freedom) over their relationships and trust amount.

Transparency / Reduced Information Asymmetry. SMEs rarely get credit from formal banking due to lack of transparency. Moreover, when lending in a setting with high information asymmetry, one can unknowingly/naively trust and lend funds to a party that is already very indebted, further increasing the risk of default of that party. In this credit network, because the debts are visible to all the participants, when accepting IOUs (which is a form of lending), participants are taking more informed decisions as there is less information asymmetry, decreasing the risk of default.

Increased Welfare and Social Justice. There is an incentive to provide better services and products and not behave maliciously in the network, as then no trust connections will be extended to the misbehaving party. Fewer connections mean less potential credit, therefore less liquidity. Social justice emerges, increasing the welfare in the network.

Disincentive to Hoarding. The problem with hoarding is that "any number of hoarders in a population will eventually lead to a crunch. This is because hoarders store-up increasing amounts of credit and eventually deprive all other peers of credit" [28]. Hoarding positive balances is less common in MC systems than with fiat currency, however, human psychology can trick rational agents into *saving for the rainy day*, or saving to redeem something bigger and more important if the balance is higher, even if the system has no intrinsic value, as found out in Chapter 2. *Demurrage* was invented to devalue positive balances to incentivize expenditure. In the IOU setting, there is no incentive to hoard other's IOUs unless it is an investment, which does not qualify as hoarding (irrational practice), but as a rational strategy. Each participant can diversify their IOUs to manage risk. Due to the expressive nature of the IOUs, each claim can have a specific purpose (*e.g.*, IOU 3 kg of apples) which makes hoarding less appealing as it does not give the owner of the IOUs endless possibilities (or at least the vague notion of it). The service or product the claim represent is more valuable than the claim itself, and when not, it is because there is an expectancy of increase of value (investment). Essentially, the problems of MC come from positive balances, IOUs subtly remove vague positive balances with others' (specified and quantified) negative balances.

Circular Economy. By exchanging IOUs for other IOUs, *i.e.*,, making them circulate, the claims that belong to the owner return have a higher probability to their hands, creating a circular economy, and employing the principle of credit clearing as the owner will not need to redeem (or pay) that debt. In other words, cycles in credit networks make the IOUs return to the claim issuer, the equivalent of cancelling debt in cycles.

Inclusivity. IOUs are versatile to represent any product or service, quantify its value and exchange it. This enables an exchange of any trusted object for others. The use cases are endless and are enumerated in section 3.3.

3.5 Paradoxes and Game Dynamics

Combining trust relationships and scalability can lead to paradoxes:

Paradox of Scalable Trust. Our goal is to create a scale credit network, however, the study [27] notes that, "the more players get added to the social graph, the more likely one-time games become between players". "Game theoretically speaking, trust can only exist between players that play "repeated games" (i.e. that interact more than once with one another). Trustworthiness therefore decays the larger the network size of players becomes" [27]. In short, the bigger the size of the network, the more likely are participants to take advantage of the system and behave selfishly. The paradox is the following. "For a party X to be able to spend another party's (Y) debt with party Z, Z has to believe that Y is trustworthy and that their debt will eventually be repaid" [27], however, with more players and more one-time games, the more difficult it becomes to trust players - "[t]rust erodes with network size" [27]. This is particularly inconvenient for a system built based on trust relationships and that aims to scale. However, by closely analysing our modelling of the credit network, this paradox can be resolved. Using the same scenario as given in the example, if Z does not know or trust Y, party X can issue their own currency and pay party Z, that trusts Y. The credit network should not be a place for one-time games, but rather a representation of existing real world trust relationships, where different kinds of debt, claims, and money can flow respecting participants' (quantified) trust relationships. The different IOUs can serve as bridges between multiple small communities, as they are interoperable money. Scaling trust can be done without incurring in this paradox, and without recurring to centrally issued money.

Braess's Paradox. This "paradox is the observation that adding roads in a road network can reduce the overall throughput of the network, when drivers choose routes selfishly" [20]. In credit networks with IOUs, this paradox can be viewed as by adding trust relationships in the network, the resulting credit potential of the network decreases. This is a counterintuitive phenomenon which depends on (1) the routing algorithms for payments and (2) the user IOUs exchanges in the network. While (1) can be analysed depending on the heuristics, strategies and algorithms for finding the best payment path, (2) has to be analysed in a simulation of the system. This paradox is left for future work as it encompasses a detailed analysis of the path finding algorithm of rippled servers.

Payment Dilemma. Exchanging *invented* money, such as IOUs when there is not enough liquidity of fiat money, does not create any dilemma as there is no other choice such as in crises. However, when agents are presented with a choice between receiving a payment with IOUs or receiving a payment with fiat money, the rational choice would be to choose the latter. While from the position of the payee, the rational choice is to choose the former. This can be the reason for the short life of most complementary currencies, which stop being used after the economy recovered from the recession, except for notable examples such as WIR. In short, when given a choice, rational agents will prefer to pay with *invented* money (IOUs) and receive payments in fiat money, as having fiat money opens more possibilities (leading to hoarding). This creates a dilemma because both wants cannot be met at the same time for a payer and a payee. To assess the behaviour of agents with this dilemma, the network is simulated and evaluated in an economic simulation in Chapter 5.

3.6 System Requirements

3.6.1 Functional Requirements

The functional requirements are written in the format of a user story (a user is the end user) following the Agile practices. The format of sentences enables software developers and other stakeholders to focus on the user and understand the purpose of each requirement.

1. As a user, I want to **set and update the trust amount in my connections**, so that I only receive an amount of IOUs/debt that I trust will be repaid or can be exchanged.
2. As a user, I want to **leverage my connections' connections to make and receive payments** from outside my trading circle, so that I can make and receive payments where I am not trusted, or I don't trust, with the similar confidence as with fiat money.
3. As a user, I want to **issue custom IOUs**, so I can use them for transactions.
4. As a user, I want to **make payments**, so that I can pay for products and services.
5. As a user, I want to **exchange/trade (buy and sell) IOUs**, so I can get more favourable deals.
6. As a user, I want to **visualize my balance** of currencies, so I can make payments.
7. As a user, I want to **start a marketing campaign**, so I can improve sales from my business.
8. As a user, I want to **finish the marketing campaign**, so I do not lose money.
9. As a user, I want to **send fidelity points to my costumers** as a thank-you for visiting the store so that they return.
10. As a user, I want to **sell discounted points** that can be spent in my business to increase sales.
11. As a user, I want to **buy discounted points** from the store I go to, so I can get discounts.
12. As a user, I want to **sell gift cards to anyone** in the credit network, to increase sales.
13. As a user, I want to **buy gift cards from anyone** to be able to redeem the gift.
14. As a user, I want to **pay the salary** of my employees from my accredited business so that they can use the money when the business does not have enough liquidity to pay salaries.
15. As a user, I want to **specify the amount of salary** I am comfortable receiving from my employer.
16. As a user, I want to **pay using my salary**, so I can continue living decently while in crisis.
17. As a user, I want to **trust another user's salary**, so they can make payments with salary.
18. As a user, I want to give a **promise to pay with my salary**, so I can buy now, pay later.
19. As a user, I want to **promise to pay the salary** to my employee, as soon as my business receives a pending payment.
20. As a user, I want to **register my debt to other people** so that I can keep track of my debt.
21. As a user, I want to **accept the debt from another member** of the network, to track their debt.
22. As a user, I want to **confirm the debt has been paid** so the borrower is free from the debt.
23. As a user, I want to **donate any asset I own** so that others can benefit from it.

24. As a user, I want to **send donations** on the behalf of the accredited institution so that the receiver of the donation can redeem it somewhere.
25. As a user, I want to **start a fundraising** for a specified amount, so I can get funds.

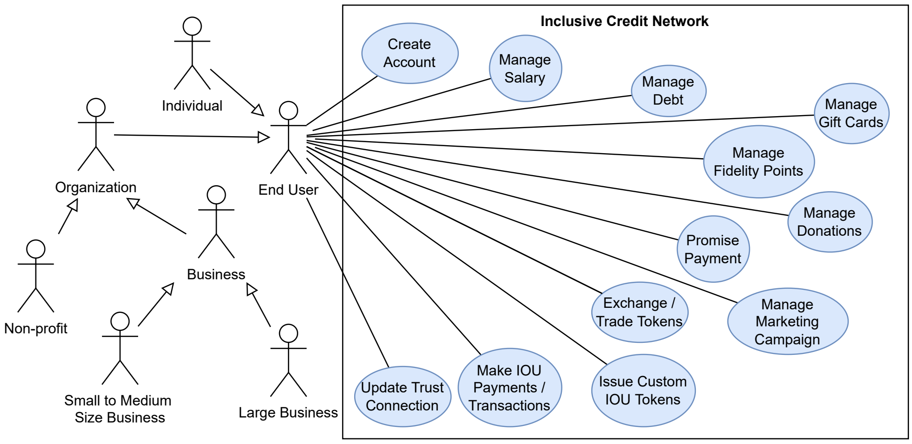

Figure 3.2: UML modelling of the actors and operations in the system

Figure 3.6.1 illustrates the functional requirements and different classes of actors participating in the network and their operations in the network. End users are the participants of the credit network, which can be single individuals or organizations. Actors that are organizations, can be for profit (businesses), or non-profit. In turn, businesses can be small, medium or large size. Businesses can be grocery stores, supermarkets, coffee shops, restaurants, hotels, hospitals, banks, beauty salons, *etc.*. Non-profits can be charity organizations, NGOs, sport clubs, communities, *etc.*. For the functioning of the credit network, there is no differentiation between any of these roles. The modelling of these actors in the UML diagram is to convey explicitly the classes of actors that are end users. End users can create accounts which creates their wallets, issue tokens, trade and transact, update their trust to connections, promise redeemable in the future payments, manage (pay, pay with, promise) salary, manage (sell, buy, redeem) fidelity points, manage (donate, pay with) donations, manage (register, accept, confirm payment) debt, manage (buy, sell, redeem) gift cards, manage (start, finish) marketing campaign. The use cases encompass a variety of use cases from section 3.3. The use case regarding a marketing campaign is a new marketing strategy designed in our credit network in addition to issuing regular fidelity points and IOUs. The details and implementations of the use cases are further elaborated in Chapter 4).

3.6.2 Non-Functional Requirements

The non-functioning requirements are presented as validation criteria and user stories.

1. **Blockchain.** Write transactions in a public permissionless distributed ledger.

   1.1 **Scalability.** The blockchain has high **throughput** (>= 1000 TPS)

1.2 **Efficiency.** The blockchain has low **validation time** (=< 30 seconds)

1.3 **Ecology.** The blockchain is **energy efficient** (*e.g.,* does not use PoW)

1.4 **Cost.** The blockchain **transactions cost less than €0.1** (ten cents).

2. **Security. Non-repudiation** property for all transactions.
3. **Security.** Trust amount, token, and party originating the transaction will respect the trust configured by the user. (As a user, I will not receive more tokens than the amount I specified for token and transaction source.)
4. **Safety.** No spoofing or tampering of the issuer of tokens. (As a user, no one can issue tokens/IOUs on my behalf).
5. **Safety.** No misleading issued tokens. (As a user, I will not be misled or tricked to receive tokens that I do not want).

Although payment privacy is an important requirement, as businesses may want to not disclose their suppliers, it is out of scope of this project as it has been sufficiently explored in the literature of credit networks payments routing, whereas our goal is different.

4

Inclusive Credit Network Implementation

Contents

4.1 Blockchain Fundamentals

Context. Before the emergence of blockchain in 2008 with the Bitcoin whitepaper ([29]), there was a research stream of decentralized P2P complementary currency system using cryptography (chained digital signatures, asymmetric cryptography, Pretty Good Privacy (PGP) encryption) and incentives, such as [30], [31], [32], to build collaboration and relationships on the internet. But the author's focus was then shifted to the novel distributed P2P trustless monetary system, Bitcoin and its underlying technology, blockchain. Ripple already existed as a decentralized currency system [30], and started using blockchain afterwards.

Double Spending Problem. When paying over the Internet, there is no physical token being transferred, so a proof is needed that the balance of the account is not double spending their tokens. A proof would remove the trust that is often deposited in centralized systems to the entity/authority that runs the system. However, in a decentralized payment system, there needs to be an alternative to trust.

Blockchain. As described [29] and explained in [33], *blockchain* refers to the public append-only distributed ledger replicated among several peers (nodes) in a network. The nodes can dynamically join or leave the network at any time without compromising the liveness (*i.e.,* progress) of the system. The data on the ledger consists of signed transactions involving digital money, it is grouped in sequentially ordered blocks using timestamping, forming a chain. Each block has a reference to the previous block, which is its hash.

Proof-of-Work. Each node receives transactions from inside (broadcasted by other peers) or outside (clients) of the network, and adds them to its transaction pool. A set of transactions is selected, each transaction is verified and added to a block, filling the maximum amount of transactions in a block data structure. A special transaction is added that indicates the issuance of new coins and transfer to the peer's address. The block is then processed to solve a cryptographic challenge, which "involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits" [29]. The solution (called a *proof-of-work*) is obtained by brute forcing the that value starting with a number of zero bits, which requires exponential time to execute but can be easily verified (by executing a hash of the block with that value). While performing computations for a new block (*i.e.,* mining), each peer is also *listening* for a block mined by a peer that has arrived to the solution, broadcasted by any node that has accepted the block. In which case, the receiving node verifies the block, and if it's valid, it stops the mining process for the proof-of-work, writes the received block on its copy of the ledger, and broadcasts the block to its connections.

Incentives. Since the block contained a special transaction that issued and transferred digital money to the peer's address is written in the ledger, the miner is rewarded as it won the competition for that block, incentivizing the participation on the system, as those are the coins exchanged in the payment system. The amount in the special transaction (the reward) is not set arbitrarily, and nodes will validate if the value is correct, rejecting the block in case it is not, wasting the effort of the node, which will not get any reward and has to start computing the proof-of-work again with the block that contains the correct reward amount. However, it is more likely that another node will win that round. Therefore, there is also an incentive to be honest and not tamper with the reward amount.

Drawbacks. The node removes the transactions that were present in the received block from its pool of transactions, and starts the process of mining for the next block. In short, all nodes are trying to compute the next block, but only one block will be accepted, meaning only one miner will receive the reward, wasting considerable computation time, hardware resources, and power/energy.

Longest Chain. Since the network is prone to partitioning, there may emerge different valid chains which do not in different partitions at the moment they are reconnected. The longest chain will be accepted as each block that is appended to the ledger can be viewed as a vote for the previous block, therefore, the longer the chain, the more CPUs have voted for those blocks.

51% Attack. Although unlikely, it can happen that malicious nodes fabricate the longest chain faster, and it becomes the accepted chain by the rest of the network. If the adversary controls the majority of the CPU power of the network, the underlying mechanisms of blockchain do not guarantee a resistance to the double spending problem. However, [29] theorized that, the amount of bitcoins (the digital cash) that would have been mined would have surpassed the value gained in the attack, which is impractical to carry out. In short, the benefits of behaving honestly surpass the amount gained by attacking the system.

Smart Contracts. Nowadays, different kinds of blockchains have been emerging, with different mechanisms both for the functionality of block validation and incentives, with Bitcoin ecosystem being the starting point. However, the most significant advancement since are *smart contracts*, introduced with the Ethereum protocol [34]. Smart contracts make the blockchain programmable by deploying scripts (pieces of executable code) to add behaviour to the transactions to the otherwise "close-ended, single purpose" [34] blockchain. This functionality enabled the decentralized autonomous organizations, lending, insurance, escrow, gambling in the blockchain, leading to a widespread development of decentralized applications using the new, open-ended blockchain as its infrastructure.

4.2 DLTs for Mutual Credit

There are multiple popular blockchains and DLTs, such as Bitcoin, Ethereum, and Hyperledger. However, blockchains or DLTs for mutual credit, complementary currencies and credit networks are not as widely discussed. Since in mutual credit and IOU based systems the money is not a scarce commodity, and it is not what attributes value to the token, the technologies functioning is inherently different from the presented traditional blockchains. DLTs, P2P frameworks and protocols tailored for mutual credit or other complementary currencies or credit networks are presented in detail in Appendix B.

4.2.1 Comparison and Discussion

The XRP network (Ripple), built on XRPL was the most referenced and studied blockchain in the literature review (Chapter 2), the Stellar network was occasionally referenced along but never a target of an analysis. To understand all the technologies build specifically with community currencies as a use case, including mutual credit, we browsed the first two pages of Google search engine for 'mutual credit' or 'community currency' and blockchain, which yielded projects such as Holochain, Hypersyn and the ReSource protocol.

Our investigations concluded that Hypersyn is still being developed and is deployed yet, ReSource protocol could allow the execution of our project, however, since it is a layer 2 (application) protocol, it would add a considerable overhead to our application. These two projects were excluded from further consideration, but their functionalities were investigated as certain features could be useful in the future. Holochain is not a blockchain, but it can be programmed to work as one. Although the presented solutions are very different, Holochain and Hypersyn defend that MC does not need to be represented with tokens therefore not needing consensus as the credit is not double-spendable, which makes blockchain an unsuitable infrastructure for it. Instead. Hypersyn uses conflict free replicated data types to maintain the balances, and Holochain uses peer witnessing to maintain the integrity of the balances. Both systems agree that MC should be a tokenless system, represented by positive and negative balances that add up to zero. However, as explained in Chapter 3, MC has inherent scalability and acceptability problems, due to the nature of real-life trust relationship and positive balances in MC networks. To work over these problems, IOUs are similar to mutual credit but are more debt explicit (issuer, owner, amount), which localizes the loss in the network leading to higher accountability, traceability and more informed decisions (the benefits of our systems are presented in 3.4). A system which uses tokens would be more appropriate to our solution, as it comprises a wider set of use cases (presented in section 3.3) than mutual credit and more closely resembles IOUs.

XRPL and Stellar were the remaining solutions to be considered for our projects. The projects are very similar (features and system), as Stellar founder worked in XRPL but branched due to divergence of opinions. Both consensus mechanisms are similar if not equal, there are no incentives to run validators other than for the ledger's health. XRPL and Stellar prioritize Consistency and Partition Tolerance over Availability (CAP Theorem). It is not clear from the Stellar documentation if the payment channels and two-step payments support non-XLM tokens (XLM are Stellar native tokens) tokens as in XRPL, payment channels and escrows only work with XRP. There is a deeper focus on providing bridges with real world assets and currency compatibility (such as integrations with Moneygram) in Stellar, while XRPL focuses on community currencies and independent stable coin issuers (gateways), the latter being more similar to our goals. XRPL development recently brought smart contract features (hooks) to the ledger, which is the main reason for our decision of developing the solution on XRPL, since the transaction fees,

	XRPL	**Stellar**	**Holochain**	**ReSource Protocol**	**Hypersyn**
Developed	✓	✓	✓	✓	✗
Layer Solution	L1	L1	L1	L2 (Cello Network)	-
Type	permissionless	permissionless	permissionless	-	-
Integrity	BFT	FBA	Peer Witnessing	-	CRDTs
Throughput	1500 TPS	3000 TPS	-	-	-
Validation Time	<10s	<10s	-	-	-
Transaction Fees	0.00001XRP (€0.00000466)	0.00001XLM (€0.000001137)	No Fees	-	-
Programmability (Smart Contracts)	Hooks - alpha testing	✗	-	-	-
Requirements Alignment	✓	✓	✗	✗	✗
Related Work Reference	✓	✓	✗	✗	✗

Table 4.1: Comparison of different DLTs for community currencies

validation time and throughput are similar (data from [35], [36], and approximate currency conversion from investing.com). Table 4.1 illustrates the comparison.

A frequent concern about XRPL is if the network is centralized due to the UNL. XRPL is permissionless and decentralized as anyone can run a validator node (rippled) and every node can choose their UNL. The consensus is based that UNLs overlap, so if the majority of the network nodes and a node's UNL do not overlap, there is a higher probability of creating partitions for that node. "As of September 2022, Ripple runs 3 of the 35 validators in the default UNL" [37], therefore, if some nodes start acting maliciously, other nodes can update their UNLs to disregard them from consensus. "The transaction cost is generally very small in real-world value, so it should not harm users unless they are sending large quantities of transactions" [35], which prevents the network from spamming from existing accounts. To prevent creating multiple accounts, there is a special process to open an account which involves locking reserve of 10XRP (€4.5). When deleting an account, the reserve can be returned, but this transaction costs 2XRP (€0.9). Aside from the habitual transactions fees, users pay higher fees to store objects in the ledger, paid once, to prevent irresponsibly storing objects.

4.3 Solution Architecture

Having a solution defined and the underlying blockchain infrastructure chosen, we construct a Command Line Interface (CLi) to prove that the inclusive credit network concept is elegantly achievable with XRPL. In the proof of concept, the functionalities to be included allow the use cases (section 3.3) and follow the requirements (section 3.6). To achieve those goals, the XRPL native capabilities, and support for the intended use cases are exhaustively explored for the development of the proof of concept.

4.3.1 Proof of Concept CLi

To limit the scope of the project, the proof of concept consists of a CLi that receives commands and arguments to execute operations that are familiar to users, such as issuing IOUs, sending fidelity points, redeeming gift card, making payments, register debt, *etc.*. These high-level operations are composed in the CLi service of different transactions, techniques, and processes tied to the functioning of the ledger and are seamless to the end user, but complex underneath. The architecture is presented in Figure 4.1. All the features were designed to offer the maximum benefit with the lowest possible risk, economic and security-related.

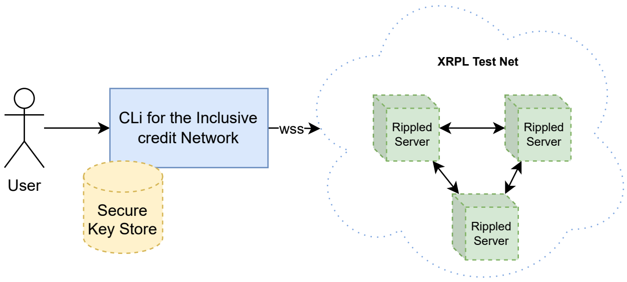

Figure 4.1: CLi system architecture

A CLi is not destined to be the final application a user would use, nor it is production ready. Instead, a suitable architecture of the system that would use the service CLi is presented in section 4.3.2, and the development of such system including the scalability (*e.g.,* load balancing of the microservice), secret storage security (represented by a local key store in the CLi) and the configuration of the sidechain rippled network is future work. Since our goals are focused in XRPL and support for our use cases and features to serve the user model, external services such as a key store are assumed to be implemented. With the CLi we are capable of testing the functionalities of the XRPL service without the need to solve networking and interface design which are two research streams by themselves in distributed computing and web3 systems. A CLi provides us with a reliable prototype of our inclusive credit network service concept in real life and draws the limits of what is possible to achieve with XRPL and its limitations.

4.3.2 Production Scenario

A CLi is sufficient for experimentation purposes, but after researching about production use of rippled servers and side-chains (section B.5.0.A), a real-world scalable architecture is proposed in Figure 4.2. Dotted non-blue lines mean that the element is not directly part of our system, but our system interacts with it.

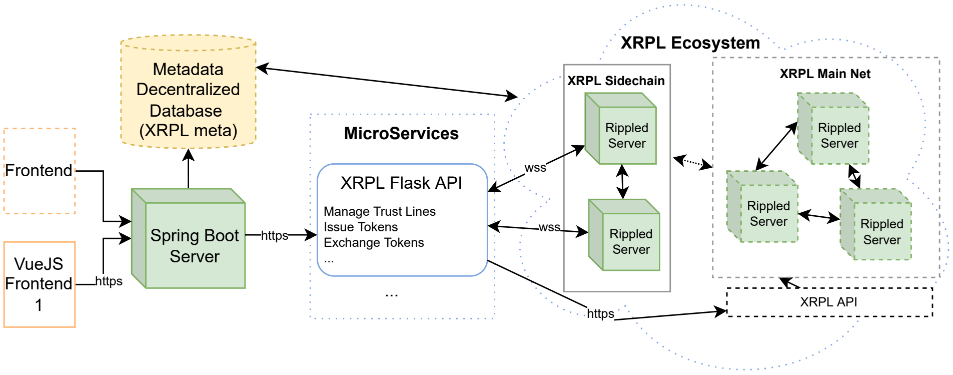

Figure 4.2: Real-world scalable architecture of the system

Wrapping the CLi in a stateless microservice within a Flask server and exposing its API is a good solution with maintainability and low coupling benefits, but higher overhead of communications, a common issue in microservice architectures. Decoupling the Spring Boot Server from the microservices allow better organization when are multiple ledgers connected and easier migrations to other services. It also allows for external systems to use the microservice. The Spring Boot Server, (multiple redundant servers) would be mainly a decorator, it could contain metadata of coupons, which would help users with choosing offers, and personalize accounts to help users find and interact with each other online. The key store can be another microservice used by the server or a library imported by the Spring Boot server. Multiple frontends are possible, including those programmed by external apps. The metadata database is a representation of a storage system as XRPL Meta. Storing the metadata related to tokens and accounts. In this proof of concept, its usage is dispensable.

The benefits of configuring and running a sidechain are considerable: not to flood the main net with our *writes*, which, since the system is scalable, is can be an issue, and to have more control over the network — it can be near permissionless or permissionless, permissioned, etc. It is possible to change the logic of the validating servers in side chains (including consensus), and maintain the interoperability with XRPL main net. It is also possible to remove fees from transactions in our sidechain and solve the spam problem differently. Before constructing this architecture, the Hooks amendment should be merged into the source code of rippled servers, after it passed quality assurance and is at least in beta testing. At the moment of writing, Hooks are in alpha testing, which is the reason the project (CLi) uses the hooks test net to connect to the ledger.

Since this project aims for a proof of concept of the inclusive credit network (and its simulation), we implement the core of this architecture, *i.e.,* the microservice's functionality as a CLi as explained in section 4.3.1.

4.4 Project Organization

The project was developed using python3.9, and makes use of the xrpl-py library to interact with the XRPL. The source code is in the `inclusiveCryptoEconomyProject\inclusiveCryptoEconomy` directory, which contains python files of `account`, `wallet`, `offer`, `iou_manager`, `commands`, `use_case_commands` (which are decorated commands), `xrpl_interactions`, `utils`, `errors`, `main` as well as the `keystore` directory that stores json files of cryptographic keys[1].

The Appendix C (C.1) presents the commands accepted by the CLi. In order to accept such amount of commands (>40), a hierarchical structure of `ArgumentParser` (argparse library) was used, so that multiple commands could reuse the same arguments.

4.4.1 Data Model & Execution Flow

The data model of the system is presented in the class diagram of Figure D.1, in the Appendix D. To attend to the requirements, several in-built structures of XRPL were employed (`IssuedCurrency`, for IOU issuing, `Offer`, for trading tokens in the decentralized exchange, `Check`, for making redeemable payments, `Payment` to transfer tokens). The information flow through the classes is the following. When a command is typed, argparser parses the command, which is saved along with the flags and arguments in the corresponding `Command` in the `main`. The `Command` is then passed to the `CommandDispatcher` class to execute the command. Multiple commands exist, that must extend the abstract class `Command` and implement the `execute_command` method. If relevant, the specific command can also override the `verify_arguments` method. Strategy and Command design patterns are used to delegate different commands. A command typically invokes the `KeyStoreUtils` which loads the `Account` from the `KeyStore` directory, which contains a `json` file for each username using the CLi. An `Account` is composed by two `wallets`: one for transactions, the other for IOU issuing (for security reasons). To load the account using the name of the user, the `KeyStoreUtils` class invoke the `AccountEncoderDecoder` class to transform the `json` input to `Account` object. Since `Account` is composed, the `AccountEncoderDecoder` calls the `WalletEncoderDecoder` for each `wallet` of the account. After loading the user's account, the command performs its logic. Most commands (aside from the commands that display information of accounts, wallets, and exchanges) need to send a transaction to the ledger. The requests to the XRPL

[1] A repository with the source code of the developed project was made public on https://github.com/NikolettaMatsur/Thesis-Project. It also contains the testing folder and the simulation.

are performed in the class `XRPLInteractionsManager`. Since the transactions need to be signed, the account that was loaded by the command in the beginning is invoked to perform the signing. The account, however, does not sign. It is an abstraction in our system, to make the system secure by default. Therefore, the `Account` knows which wallet should sign the transaction, delegating the signing. The correct `Wallet` requests the transaction to the `XRPLInteractionsManager`, which is prepared by the interactions manager specifically to have a higher probability of succeeding by requesting the last ledger sequence number. The wallet then signs it, and invokes the `XRPLInteractionsManager` to send the transaction to the ledger. The `XRPLInteractionsManager` waits and then parses the ledger's response codes, displaying a user-friendly message depending on the error code. We distinguish between three types of command. There are fundamental commands: IssueIOUCommand, CreateAccountCommand, GenerateAccountCommand, ShowAccountDetailsCommand, SetTrustCommand, PaymentCommand, ExchangeOfferCommand, ShowAccountOffersCommand, ShowOrderBookOffersCommand, CancelOfferCommand, SendCheckCommand, RedeemCheckCommand. Fundamental commands' options (flags and command line arguments) allow for generic and versatile transactions. However, to enable specific use-cases, there are special `IOUTypes`, which are different currencies codes such as "FID" for fidelity points, "DON" for charity and donations, "GFT" for gift cards, "SLY" for salary, "DBT" for debt, and "OOO" for the zero note. All currencies have the conventional value that a unit is pegged to the Euro. However, it is still possible to sell and buy IOUs for more than this value on exchange, the community decides as it is their market. The commands that enable the use-cases which use the mentioned currencies are **decorators** for some fundamental commands. For example, BuyGiftCardCommand is a decorator of the general and fundamental command of ExchangeOfferCommand that automatically fills certain fields tailored to the use case, including the currency code "GFT". Another type of command (GenericIssueExchangeCommand and GenericIssuePaymentCheckCommand) are internal commands that always perform the actions as in their name by composing two or more fundamental commands, *i.e.*, issue IOU and make an exchange offer or, issue IOU, try making payment, if it fails, send a check. These commands are internal utilities that also have decorators, such as SendFidelityPointsCommand, that tries to deliver bonus fidelity points, which have to be issued first, then attempted to send, and if there is not enough trust in the trust line, a check is given, which the receiver can accept or not, complying with the requirements. The offer class displays offers and decides which type of offer the selected options correspond in the ledger.

4.5 Implemented Features

The implemented system is a minimum viable inclusive credit network. The system comprises the core features of a credit network: IOU issuing, transactions with IOUs, updating trust, debt clearing (rippling), account creation, tracking their debt (one can see how much is their debt and to whom by seeing their circulating issuing balance), burning IOUs (by returning them to the issuer). The innovation contributions of this system and the underlying mechanisms are the following.

1. **Secure Account Creation and IOU Issuing.** Because the system is a proof of concept for its deployment in the real world, where users are innocent and oblivious to security risk, account creation and IOU issuing are designed with best practices that enhance the security of the user, without requiring security knowledge. Achieved by, with a single user command, creating two wallets, one that only issues tokens, the other which only receives the issued tokens to minimize the risk of compromising the issuing wallet.
2. **Use cases.** Enabling different use cases for end users (such as **debt registering**, **payments** with own and others' **debt**, fidelity points **exchanging**, **gift** cards, donations, fundraising, and salary payments) which paves the way for an inclusive economy, unlike most complementary currencies that restrict users, hampering the economic impact of the system. This is achieved by leveraging functionalities of the XRPL such as payments, checks, and different types of mechanism from the decentralized exchange.
3. **Fidelity Point Campaign.** Enabling SMEs, who usually do not have a fidelity points campaign, set it up easily. Any enterprise can benefit from this fidelity point scheme. Achieved by designing DEX offers and IOU exchange process.

4.5.1 Create Account Process

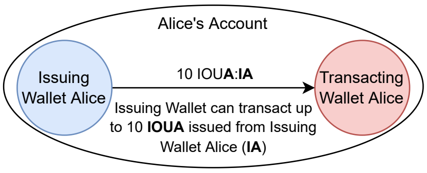
Alice's Account
Issuing Wallet Alice
10 IOUA:IA
Transacting Wallet Alice
Issuing Wallet can transact up to 10 IOUA issued from Issuing Wallet Alice (IA)

Figure 4.3: Representation of an account in our system following the issuing best practices

The XRPL does not provide an explicit endpoint to create accounts. Instead, creating accounts on the ledger involves a process. An account, in our system, is composed by two wallets (see Figure 4.3). One is used for IOU issuing and the other for transactions, to disallow rippling in the transactions and ripe the benefits of rippling in the issuing account. Moreover, since the issuing account will be used less than the transacting account, the risk of exposing the secret is reduced. To open an account in XRPL, a valid address needs to receive funding from an existing wallet that covers at leat the account reserve. In the Inclusive Credit Network, the user (named username) requesting an account inserts in the CLi "`create-account` -u username". The application will generate two wallets using, save them in the key store and display the addresses of the wallets that need funding. The user should then request to a member of the XRPL network to send to their wallet a sufficient amount of XRP to cover the reserve (currently 10XRP). A suggestion is to have a responsible entity in the early stages of the network to board users who are not expected to be tech-savvy. After the wallets are funded, the user should type "`configure-account` -u username" so that the default rippling is enabled in the issuing wallet and an authorization to hold issued tokens is enforced on the transacting. Rippling allows other users to pay with your IOUs, but your transacting account (which holds other people's tokens) will be protected, mitigating the faulty gateway attack. Enabling authorization on transacting account is a safety measure against issuing and sending money from the wrong wallet, which could lead to security risk and render the wallet separation pointless. For development purposes, a wallet generation command ("`generate-account` -u username") was created that uses faucet wallets, and configures them immediately since the wallets come funded from the test net.

4.5.2 Issuing Custom Tokens or *FID*, *SLY*, *DBT*, *OOO*, *DON*, *GFT*

Issuing tokens is the central feature of the credit network as it enables transactions, credit clearing, and multiple use cases. Assuming a user has created an account successfully, it was funded, and the user ran the configuration command on the wallet, they can now issue any amount of token desired. Tokens are defined by their currency code (3 capital letters – standard) and the issuer wallet address. Tokens always exist in trust lines, *i.e.*, bidirectional relationships between wallets, where each side has a maximum amount of trust and a balance (positive or negative) of that token. Issuing of tokens on the CLi, "`issue-iou` -u user-name-account -a amount-ious -c code-ious", (code-ious cannot be XRP), creates a trust line between the transacting account to the issuing account with the amount-ious value as the capacity of the network edge and the currency code as well, or if such trustline already exists, updates the trust to let amount-ious be transacted. Then, the issuing wallet transacts the amount of IOUs with the wanted currency code. Special for the Inclusive Credit Network tokens have currency codes of *FID*, *SLY*, *DBT*, *OOO*, *DON*, *GFT* as introduced in the subsection 4.4.1. These tokens can also be freely issued by anyone using the generic command or special commands (decorators). However, it does not mean everyone will be able to use them. Users need to trust each other for the transaction to take place, *i.e.,* have a trust line (see 4.5.3).

Special Use Cases. To simplify the execution of the special use cases by users, this step is hidden. That is, the user is not made aware that it is issuing tokens (unless an error occurs which allows the user to resume from the failed step), instead, the tokens are issued on demand and for a purpose, which is executed promptly. The issuing is intrinsic to the commands such as "send-fidelity-points", "pay-salary", "register-debt", "donate-as-institution", and also "start-marketing-campaign", "ask-for-donations", "sell-gift-card". The first step of these commands is to issue tokens such as FID, SLY, DBT, DON, OOO, GFT and then other commands are composed, which makes the issuing be performed seamlessly.

4.5.3 Set Trust Command and Special Use Cases

Every user with a valid account can issue tokens, but there is no point in doing so if no one is willing to accept the tokens (*i.e.,* extending a trust line to their issuing wallet). The purpose of this command is to make the network reflect the amount of trust there is in real life between two people. Figure 4.4 illustrates the trust lines that limit the amount of tokens that each wallet can send. IOUX:Y means tokens with code IOUX issued by wallet Y are accepted. The segregation and configuration of each wallet allows other users in the network, for example, users that trust Alice, to make payments to Bob through Alice even if they do not know Bob. To set trust, users need to input into the **CLi!** the command "`set-trust` -u user-name-account -a amount [-i issuer-address] [-in issuer-name] -c currency_code". In every command, users can choose to indicate either the issuer-address or the issuer-name. This shows that trust is per issuer and currency code. Trust line limits can only be exceeded by acquiring more of the token from the Decentralized Exchange (DEX), by decreasing the limit of the trust line below the amount of tokens already in possession, or by cashing a check.

Special Use Cases. The above command can be simplified to only indicate the issuer and the amount, since the *FID*, *SLY*, *DBT*, *OOO*, *DON*, *GFT* can be trusted from commands such as "trust-fidelity-points", "trust-salary", "trust-debt", "trust-donations". For example, "trust-salary [-i CURRENCY_ISSUER] [-in CURRENCY_ISSUER_NAME] -a TRUST_AMOUNT" which translates to "trust-salary -in AliceStartUpWaller -a 100", which is equivalent to running the generic command: "set-trust -a amount AliceStartUpWaller -c SLY". The name of the user ("-u username") has always to be indicated to let the CLi know who is interacting.

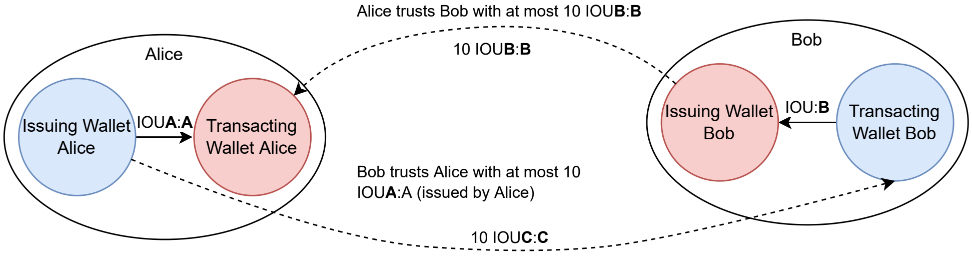

Figure 4.4: A representation of trust lines between Alice and Bob

4.5.4 Payments with Tokens, XRP and Special Use Cases

Making Payments is the second most central feature from the Inclusive Credit Network. After issuing custom or tokens and making the trust connections from the real life known to the network, the trust becomes the main driver for transactions. In XRPL, only XRP payments do not use trust lines, therefore, for to make IOU payment, a path with available (not exhausted) trust must exist between the sender and the destination. The XRPL engine searches at most 6 hops and uses the decentralized exchange to find the lowest cost path for the payment. The amount that can be filled partially is reported by the engine and in turn, from the CLi to the user in a user-friendly manner. Thus, to make an XRP payment using the CLi, run "`make-payment-xrp` -u user-name-account -a amount-xrp [-d destination-address] [-dn destination-name]". For example, "make-payment-xrp -u alice -a 10 -dn bob" (or the address of Bob using -d instead of -dn). To make custom token payment, "`make-payment` -u user-name-account -a amount-ious [-d destination-address] [-dn destination-name] [-i issuer-address-of-the-ious] [-i issuer-address-of-the-ious] [-c code-ious]". For example, "make-payment -u bob -a 6 -dn alice -in alice -c IMA".

Special Use Cases. This command enables a set of decorators, such as "pay-with-salary", "pay-with-donation", "pay-with-fidelity-points" and "confirm-debt-repaid" (which sends the debt back to the issuer of the debt, freeing them from the obligation). Partially, this command also enables "send-fidelity-points", "pay-salary", "register-debt", "donate-as-institution" in combination with other commands automatically executed (issuing IOUs and sending Checks).

4.5.5 Trade IOUs in the Decentralized Exchange and Special Use Cases

The DEX allows users to express willingness of holding a certain amount of an asset while exchanging for an amount of other asset. Assets can be XRP and non-XRP tokens. When the offer is created, the default behaviour is to partially fill the offer with offers that match it in the opposed direction (coincidence of wants), and which exchange rate (the ratio between amount) at least as good as expressed in the created offer. To buy and sell tokens, there does not need to be a trust line as the issuer and currency code is specified, it is implicitly created by the XRPL. The generic command in the CLi for exchanging is "`exchange-asset`", and the currency codes and amounts of selling and buying currency as well as their issuer names or addresses are necessary for the offer to be defined. For example, "exchange-asset -u alice -a1 10 -c1 ALE -i1n alice -a2 1 -c2 BOB -i2n bob". To buy or sell XRP (not possible to exchange XRP for XRP), only the amount should be filled. Additionally, there are multiple strategies for placing offers, such as making the off indivisible (`all-or-nothing`), `immediate-only` offers (not placed into the ledger, consumed with matching offers), offers which objective is to `sell` rather than buy the other token, or make the offer `permanent`. These options are added as flags (-s/–sell, -e/–entire, -n/–now, -p/–permanent) to the main generic `exchange-asset` command. The offers from the account can be seen with "`show-my-offers` -u alice" and removed with "`remove-offer`". Additionally, the offers from the order book can be seen with "`show-market-offers`".

Special Use Cases. This command is called when decorator commands are executed due to user input such as "buy-fidelity-points", "buy-gift-card", "buy-donation". Partially, this command pairs with issuing IOUs for the inputs of "start-marketing-campaign" (divisible, sell offer), "ask-for-donations" (divisible buy offer), "sell-gift-card" (indivisible sell offer), which issue the corresponding token of FID, OOO and GFT and then place it to the exchange with the correct offer type. The cancelling or removal of the offer is used by "`finish-marketing-campaign`".

4.5.6 Send and Redeem Checks, and Special Use Cases

Checks are an XRPL inbuilt method of payment which does not need trust lines to be executed. The payment is divided in two phases: the sender sends the check of currency they own or not (the tokens are not locked), and the receiver can redeem/accept the check or not. If the check fails due to lack of funds, it can be tried to be redeemed again later. To send a check, `send-check` input is used. and details about the destination and currency should be provided (if XRP check, the issuer and code name are not specified, while in tokens are). Additionally, an expiration date can be set up. For example, "`send-check` -u alice -dn bob -a 3 -c ALE -in alice -e 10-10-2023". The checks are visualized in the account with "`show-account`", the number is presented to then redeem the check (*e.g.,* "`redeem-check` -u bob -c 32366704").

Special Use Cases. Checks enable a considerable amount of use-cases with the two-phase payment logic (and still satisfying non-functional requirements such as safety and trust). Decorators for the "SendCheckCommand" are "pay-with-salary-promise", "send-gift-card", "pay-with-promise", "promise-salary-payment", "donate-as-individual". Checks provide the mechanism of promising, which is when a currency is expected to be in the wallet any time soon, a check can be sent and the receiver can redeem the check when the currency arrives to the account. "RedeemCheckCommand" decorators are: "redeem-fidelity-points", "redeem-gift-points", "accept-debt". Adding the "SendCheckCommand" to IOU issuing and payment commands, more use-cases are enabled, such as "send-fidelity-points", "pay-salary", "register-debt", "donate-as-institution". These commands issue the corresponding IOU (FID; DBT; DON; SLY), attempt to make a payment, and if there is not enough trust, a redeemable check is sent (the user can control what happens after the payment failure).

5

Evaluation

Contents

The evaluation of the credit network in this stage of development consists in testing its functionality correctness and in a simulation of the economy where each agent has the possibility to issue custom tokens, which is the most fundamental and broad, concept of the Inclusive Credit Network. The simulation with users should be done at a later stage, after more granular simulations for each functionality are designed, developed and run with synthetic and real world data.

5.1 Functionality Testing

Programming using a public, shared, open and append-only database is fundamentally different to programming using centralized databases. Therefore, the typical approach of testing beforeAll and setUp and tearDown approach do not work, as the XRPL is append-only and not yet has a testing framework. For this reason, the developed test, which use `pytest`, test the fundamental functionalities automatically, but their output needs to be analysed independently, and any of them fails, the test has a 'NOTE' (a comment in the function of the test) that may troubleshoot the reason, which can be due to the input passed to the test, the ledger fortuitous state, system restrictions such as not having a set trust line to make a payment, *etc.*. The key store of the tests (inclusiveCryptoEconomyProject/keystore) is separate to the keystore of the CLi (inclusiveCryptoEconomyProject/inclusiveCryptoEconomy/keystore). The defined tests comprise the fundamental operations of generating accounts, setting trust lines, issuing IOUs, making XRP and token payments, making exchange offers, seeing balance, seeing own offers, seeing market offers, sending a check, redeeming a check.

5.2 Inclusive Economy Simulation

5.2.1 Rationale

Complementary currencies' (CCs') life is typically short, with a few notable exceptions, such as WIR. However, we usually forget about stores' fidelity points and coupons, which can also be looked at as CCs. These CCs are characteristically from large companies that have set up a marketing scheme. Large companies are usually less than 1% of an economy. SMEs may not have the resources, such as budget, infrastructure, or technology to easily set up a similar marketing scheme, but they are 99% of most economies. What would happen if SMEs also had fidelity point? More than that, what would happen if anyone in an economy could issue debt and make payments with it, as long as it did not surpass the trust in each of their connections? How can quantified trust become a form of money?

5.2.2 Modelling

People's trust for each other and companies can be viewed as a weighted directed graph. In an economy, bigger companies are the ones that have the most trust and connections, while smaller economies have fewer connections.Therefore, Barabási-Albert algorithm can generate similar graphs as it uses preferential attachment, which leads to the emergence of hubs. However, for the model to resemble more accurately the reality, each edge (i.e., trust connection) is randomly decided to be directed towards one side, the other, or removed, using the following probabilities 45%, 45%, 10%. This allows to potentially create disconnected graphs, as trust being a connected graph is not an assumption but part of the experiment.

The graph sets node attributes such as fiat_currency to represent the quantity of money, and debt_currency to quantify the amount of other's debt (i.e., other people owe them) at each time step. The total amount of fiat_currency is fixed and starts unevenly distributed to simulate the supply of fiat money in an economy and the debt_currency's supply is elastic, on-demand, and is only limited by the trust connections of a node. Instead of using a normal/Gaussian distribution, to distribute the initial amount of fiat_currency for each node, power law is a more reliable representation of wealth in an economy, where some (very few) nodes are extremely rich, while the vast majority are considerably poorer.

The graph's edge attributes are trust to simulate the amount of money a node trusts the other to owe to them, and debt_flow which represent how much debt is currently in place for that connection.

5.2.3 Assumptions

1. Each node prefers receiving fiat_money and spending debt_currency. This assumption creates the payment dilemma, as for users to get what they want they have to cooperate (not be selfish).

2. The balances of fiat money are visible, and so are trust connections. The simulation has perfect information.

3. 90% of the time, when a payer node has fiat money, the payee node will reject the debt_currency payment proposal and ask for fiat_currency.

4. Any node prefers receiving debt payment than no payment.

5. Trust relationships are typically oriented (have a direction) to who lends more money to the other.

6. The shortest paths for debt_currency are the cheapest, thus chosen before the longer paths to conduct payments.

5.2.4 Experiment

1. At each time step, two nodes (payer and payee) are randomly selected using uniform distribution to participate in a payment
2. If payer has enough fiat_currency to make the payment:

    (a) Randomly choose, with 90% probability of fiat_currency, the type of payment (fiat or debt currency)

    (b) If fiat_currency was chosen, perform payment and pass to the next time step.

3. If payer does not have enough fiat_currency or the debt_currency was chosen to be used:

    (a) Find paths between payer and payee and sort them according to their length, which cannot be more than 6 hops (as the system does not process such distant payments)

    (b) For each path, see if there is enough room in the flow of debt (debt_flow) to push the debt along that path, i.e., that will not surpass edge's trust.

        i. If there is a path, make the payment by updating debt_flow along the path, increasing the debt_currency in the destination and decreasing it in the source.

    (c) If there is no non-saturated path or path at all, and if there is fiat money, then make payment with fiat money.

    (d) If there is no fiat money also, make the payment as failed.

5.2.5 Limitations & Consideration

1. There is no relation of initial distribution of wealth and number of connections while in reality there might be.
2. Generalizing that every cryptocurrency works in a big scale as a safer mutual credit can hide important details. A separate study should be conducted to evaluate the applicability of the system with agents, before testing in the real world.
3. Since it is not yet a production ready system, there were no stress tests to the network, however, scalability needs to be tested eventually. 4. Since the effect of individual features such as salary payments was not yet simulated, there is no confidence in saying that this feature will help the economy. It is so because it can be used also by large companies as a reliable option to not pay the employee's salary with fiat currency when they can do so, but it's not strategic from the company's point of view.

6

Conclusion

Contents

We started with the goal of increasing SME's liquidity to increase the economic welfare in the nation, as the quantity of SME's in most economies is incomparable to the amount of large enterprises (¿99%). The success of the WIR currency motivated the search for CCs for economic stability and protection against economic downturns. To find a reliable way to help SME's liquidity using CCs (a broader class that comprises mutual credit, the underlying mechanism of WIR), we conducted a SLR which was divided in two parts. The first part consisted of exploring the types, context, benefits and main issues of complementary currencies revealed that the systems lack scale to be more explored, researched, and experimented. we then moved to understand the issues being solved on complementary currencies and credit networks in the CSE literature. The research revealed that scale is not a preoccupation in current research. Therefore, we focus on bringing scale to complementary currencies. Blockchain technology is revisited, and mutual credit blockchains are researched and compared. XRPL reveals to be the most suitable technology to develop our solution. The solution is implemented and the simulation proposed.

6.1 Contributions

The contributions of this report are as follows. (1) A robust link in research between real world needs stated by the economic literature and the state of the art in CSE is provided using transparent and reliable methodology of SLR, and future research directions are proposed to the CSE research. (2) A comprehensive overview of the current blockchain solutions tailored for complementary currency usage is provided. (3) An design of an inclusive credit network is provided, with exhaustive identification of use cases, benefits and user incentives to onboard the maximum amount of users, thus addressing the CCs small scale problem. (4) A prototype /proof of concept is developed in the form of a CLi to attend the specified design.

6.2 System Limitations and Future Work

Interesting functionalities that were thought of but not implemented to narrow the scope of the project and testing. The above core features need to be tested and simulated/validated using agents before advancing on to adding more features. Future work ideas follow. (1) The escrow feature of XRPL with non-XRP tokens. It is a two-phase payment mechanism where funds are locked (unlike Checks) that enable holding payment and confirm only when the service is received. (2) Clawback payments, which burns a payment (similar to Stellar feature [36]). (3) Soft peg of one issued IOU to €1, such as in reSource [38]. Can be achieved via passive offers in the decentralized exchange, which links the value of the token to another token in the chain. (4) Simulate and investigate if the designed credit network against the Braess's Paradox (from 3.5).

Bibliography

[1] C. Okoli, "A guide to conducting a standalone systematic literature review," *Communications of the Association for Information Systems*, vol. 37, no. 1, Nov 2015. [Online]. Available: https://aisel.aisnet.org/cais/vol37/iss1/43

[2] J. Jaccard and J. Jacoby, *Theory construction and model-building skills: A practical guide for social scientists.* The Guilford Press, 2009.

[3] A. Michel and M. Hudon, "Community currencies and sustainable development: A systematic review," *Ecological Economics*, vol. 116, p. 160–171, Aug 2015.

[4] J. Huttunen and M. Joutsenvirta, "Monies, economies and democracy: cultivating ambivalence in the co-design of digital currencies," *CoDesign*, vol. 15, no. 3, p. 228–242, 2019.

[5] D. Reppas and G. W. Muschert, "The potential for community and complementary currencies (ccs) to enhance human aspects of economic exchange: El potencial de las monedas sociales y complementarias (msc) para mejorar los aspectos humanos del intercambio económico." *DIGITHUM*, no. 24, p. 1–11, Jul 2019.

[6] S. Lucarelli and L. Gobbi, "Local clearing unions as stabilizers of local economic systems: A stock flow consistent perspective," *Cambridge Journal of Economics*, vol. 40, no. 5, p. 1397–1420, 2016.

[7] G. Seyfang, "Carbon currencies: A new gold standard for sustainable consumption?" *Working Paper - Centre for Social and Economic Research on the Global Environment*, no. 1, p. 1–16, 2009.

[8] ——, "Bartering for a better future? community currencies and sustainable consumption," *Working Paper - Centre for Social and Economic Research on the Global Environment*, no. 1, p. 1–20, 2004.

[9] S. Tsivopoulos, "History zero and alternative currencies: An archive and a manifesto, greek pavilion, 55th venice bienniale," *Journal of Visual Culture*, vol. 14, no. 2, p. 161–175, Aug 2015.

[10] P. Kayal and P. Rohilla, "Bitcoin in the economics and finance literature: a survey," *SN Business Economics*, vol. 1, no. 7, p. 88, Jul 2021.

[11] J. Long, C. Zhang, C. Li, L. Wei, Q. Sun, and X. Zhang, "Private and fast routing in credit networks," *2020 International Conference on Networking and Network Applications (NaNA), Networking and Network Applications (NaNA), 2020 International Conference on, NANA*, p. 1–7, Dec 2020.

[12] G. Panwar, S. Misra, and R. Vishwanathan, "Blanc: Blockchain-based anonymous and decentralized credit networks," 2019, p. 339–350.

[13] M.-S. Pedro, R. Tim, and K. Aniket, "Pathshuffle: Credit mixing and anonymous payments for ripple," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 3, p. 110–129, Jul 2017.

[14] R. Fugger, "Money as ious in social trust networks a proposal for a decentralized currency network protocol," p. 6, Apr 2004.

[15] R. Yu, Y. Wan, V. T. Kilari, G. Xue, J. Tang, and D. Yang, "P4pcn: Privacy-preserving path probing for payment channel networks," *2019 IEEE Global Communications Conference (GLOBECOM), Global Communications Conference (GLOBECOM), 2019 IEEE*, p. 1–6, Dec 2019.

[16] S. Thakur and J. Breslin, "An edge colouring-based collaborative routing protocol for blockchain offline channels," 2020, p. 343–350.

[17] V. Sivaraman, W. Tang, S. B. Venkatakrishnan, G. Fanti, and M. Alizadeh, "The effect of network topology on credit network throughput," *Performance Evaluation*, vol. 151, p. 102235, Nov 2021.

[18] L. Subramanian, R. Vishwanathan, and K. Kolachala, "Balance transfers and bailouts in credit networks using blockchains*," 2020.

[19] V. Sivaraman, W. Tang, S. Bojja Venkatakrishnan, G. Fanti, and M. Alizadeh, "The effect of network topology on credit network throughput," *ACM SIGMETRICS Performance Evaluation Review*, vol. 49, no. 3, p. 59–60, Mar 2022.

[20] G. Ramseyer, A. Goel, and D. Mazières, "Liquidity in credit networks with constrained agents," in *Proceedings of The Web Conference 2020*, ser. WWW '20. New York, NY, USA: Association for Computing Machinery, Apr 2020, p. 2099–2108. [Online]. Available: https://doi.org/10.1145/3366423.3380276

[21] D. Ofori-Boateng, I. Dominguez, C. Akcora, M. Kantarcioglu, and Y. Gel, "Topological anomaly detection in dynamic multilayer blockchain networks," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12975 LNAI, p. 788–804, 2021.

[22] S. C. Goldstein, D. Goktas, M. Conn, S. P. T. Pitchuka, M. Sameer, M. Shah, C. Swett, H. Tu, S. Viswanathan, and J. Xiao, "Bolt: Building on local trust to solve lending market failure," p. 14, 2020.

[23] I. Petri, O. F. Rana, and G. C. Silaghi, “Service level agreement as a complementary currency in peer-to-peer markets,” *Future Generation Computer Systems*, vol. 28, no. 8, p. 1316–1327, Oct 2012.

[24] S. Balbo, G. Boella, P. Busacchi, A. Cordero, L. De Carne, D. Di Caro, A. Guffanti, M. Mioli, A. Sanino, and C. Schifanella, “Commonshood: A blockchain-based wallet app for local communities,” 2020, p. 139–144.

[25] P. Moreno-Sanchez, N. Modi, R. Songhela, A. Kate, and S. Fahmy, “Mind your credit: Assessing the health of the ripple credit network,” 2018, p. 329–338.

[26] L. M. Subramanian, R. Vishwanathan, and K. Kolachala, “Balance transfers and bailouts in credit networks using blockchains,” no. arXiv:2003.03409, Mar 2020, arXiv:2003.03409 [cs]. [Online]. Available: http://arxiv.org/abs/2003.03409

[27] L. Ramabaja, “Hypersyn: A peer-to-peer system for mutual credit,” no. arXiv:2206.04049, Jun 2022, arXiv:2206.04049 [cs]. [Online]. Available: http://arxiv.org/abs/2206.04049

[28] R. Rahman, D. Hales, T. Vinkó, J. Pouwelse, and H. Sips, “No more crash or crunch: Sustainable credit dynamics in a p2p community,” in *2010 International Conference on High Performance Computing Simulation*, Jun 2010, p. 332–340.

[29] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” p. 9.

[30] K. Saito, “Wot for wat: Spinning the web of trust for peer-to-peer barter relationships,” *Ieice Transactions on Communications*, vol. E88B, no. 4, p. 1503–1510, Apr 2005.

[31] K. Saito, E. Morino, and J. Murai, “Reduction over time: Easing the burden of peer-to-peer barter relationships to facilitate mutual help,” 2005, p. 28–37.

[32] ——, “Incentive-compatibility in a distributed autonomous currency system,” in *Agents and Peer-to-Peer Computing*, Z. Despotovic, S. Joseph, and C. Sartori, Eds., vol. 4118. Berlin: Springer-Verlag Berlin, 2006, pp. 44–+. [Online]. Available: https://www.webofscience.com/wos/woscc/full-record/WOS:000244583200004

[33] A. M. Antonopoulos, *Mastering Bitcoin.* O’Reilly Media, Inc., Dec 2014. [Online]. Available: https://github.com/bitcoinbook/bitcoinbook

[34] V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform.” p. 36.

[35] “Concepts — xrpl.org.” [Online]. Available: https://xrpl.org/concepts.html

[36] “Stellar documentation.” [Online]. Available: https://developers.stellar.org/docs/

[37] “Faq — xrpl.org.” [Online]. Available: https://xrpl.org/faq.html

[38] “Resource finance documentation.” [Online]. Available: https://resource-network.gitbook.io/resource-technical/

[39] M. Petticrew and H. Roberts, *Systematic reviews in the social sciences.* Blackwell Publishing, 2006.

[40] W. Bandara, E. Furtmueller, E. Gorbacheva, S. Miskon, and J. Beekhuyzen, “Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support,” *Communications of the Association for Information Systems*, vol. 37, 2015. [Online]. Available: https://aisel.aisnet.org/cais/vol37/iss1/8/

[41] F. Chasin, F. Schmolke, and J. Becker, “Design principles for digital community currencies,” vol. 2020-January, 2020, p. 4122–4131.

[42] B. Dash and N. Sandhu, “Time banking: The missing link,” *Development*, vol. 61, no. 1–4, p. 164–171, Dec 2018.

[43] L. Larue, C. Meyer, M. Hudon, and J. Sandberg, “The ethics of alternative currencies,” *Business Ethics Quarterly*, vol. 32, no. 2, p. 299–321, 2022.

[44] M. Bhargava and D. Rao, “Sentimental analysis on social media data using r programming,” *International Journal of Engineering and Technology(UAE)*, vol. 7, no. 2, p. 80–84, 2018.

[45] M. Zook and J. Blankenship, “New spaces of disruption? the failures of bitcoin and the rhetorical power of algorithmic governance,” *Geoforum*, vol. 96, p. 248–255, 2018.

[46] “Holochain core concepts - holochain docs.” [Online]. Available: https://developer.holochain.org/concepts/

[47] Jul 2022. [Online]. Available: https://github.com/holochain/holochain-proto/blob/a0ad5b4a2c5aac257703dc5fba8cab0d2e4660d2/holochain.pdf

[48] “Xrpl hooks concepts documentation.” [Online]. Available: https://xrpl-hooks.readme.io/

A

SLR - Search Protocols and Results

A.1 Search Protocols

A.1.1 Part One – Complementary Currencies' Context

Studies that summarize the application of digital currencies and cryptocurrencies as complementary currencies to generate economic growth were the target of the searches. A review of the implementations of mutual credit (*i.e.* multilateral barter) or private money using blockchain would be ideal, but it is also convenient to find literature reviews that compare digital solutions (from the technological point of view) as is the comparison of the functional mechanisms (*i.e.* how the currency works from the perspective of the end user). The reports meeting these criteria and presenting a section with future work directions might be of special importance even if from a different field of work as they present challenges that can be overcome with the blockchain technology. Although there are several fields of study involved, it is not relevant for us to understand the central questions of humanities, social sciences, ethics, ecology (although green sustainable science technology is included), art, business, politics, management, *etc.*. The focal point for us is the technology or underlying mechanism, that is why the reviews that do not relate to CS were skimmed, targeting the description of such mechanisms, and included in case there was a potential to contribute to our research. Reviews from CS and similar fields were inspected for alignment with our purpose, those were skimmed, and some slow read and summarized and analysed in this subsection. These mostly included technology, models, and protocols for P2P digital currencies, including cryptocurrencies.

A.1.1.A Databases

To find out the already covered topics in prior reviews, we have searched the B-on[1] (*Biblioteca do Conhecimento Online*), which is a service (using EBSCOhost services) provided by University of Lisbon and combines the following resources[2]: **ACM Digital Library**, **Academic Search Complete (EBSCO)**, **Business Source Complete**, and **Web of Science**, it is a more practical way (and less time-consuming) than to search these databases separately as the results are filtered for duplicates and the results are in one page. Additionally, University of Lisbon provides access to the **Scopus** database which is not integrated with B-On search services, thus will be searched separately, and the accepted results scanned for duplicated articles. We also searched in **IEEE Xplore**. All databases were searched with the search strategy denoted below (A.1.1.B).

A.1.1.B Search Strategy

Articles that are not of type *review* but that contain extensive, comprehensive or thorough reviews were also accepted, and their quality is assessed separately. The papers need to have a certain level of granularity, as overviews are searched rather than detailed and specific implementations. Therefore, reading the literature review sections of articles that may be or not reviews, but that contain useful information and the correct level of details is appropriate even if the same articles will be used further in the process.

Figure A.1 illustrates the expansiveness of our research across three areas of studies: Digital Currencies and Cryptocurrencies from the CS perspective **(A)**, Complementary Currencies

The keywords by area are:

- **(A):** (cryptocurrency OR "digital currency" OR "programmable money" OR "electronic money" OR blockchain OR DeFi OR "Decentralized Finance" OR "digital gold" OR "digital cash" OR "P2P money" OR "peer to peer money")
- **(B):** ("complementary currency" OR "alternative currency" OR "residual currency" OR "private money" OR "community currency" OR "private currency" OR "liquidity saving mechanism" OR "economic circle" OR "credit network" OR "multilateral exchange" OR "multilateral

[1] Available on: https://www.b-on.pt/

[2] Source: https://bist.tecnico.ulisboa.pt/pesquisa/biblioteca-digital/bases-de-dados/; https://www.b-on.pt/en/collections/; https://bist.tecnico.ulisboa.pt/pesquisa/biblioteca-digital/b-on/

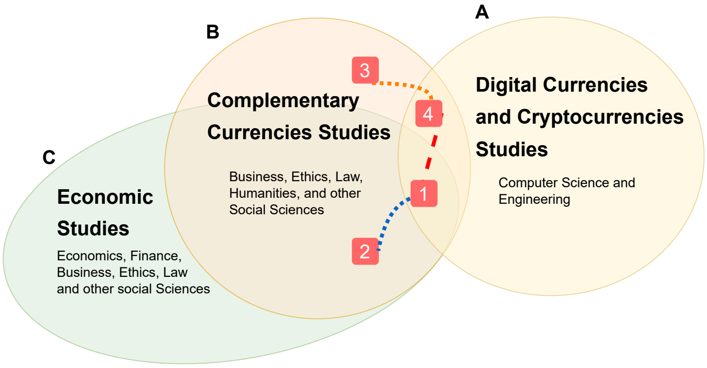
B
A
C
3
4
1
2
Complementary Currencies Studies
Business, Ethics, Law, Humanities, and other Social Sciences
Digital Currencies and Cryptocurrencies Studies
Computer Science and Engineering
Economic Studies
Economics, Finance, Business, Ethics, Law and other social Sciences

Figure A.1: Venn diagram of research topics included in the search for prior work and the corresponding fields of study.

barter" OR "credit clearing" or "mutual credit" OR "auxiliary currency" OR "secondary currency" OR microcurrency)

(C): ("economic growth" OR "economic stability" OR economic)

A.1.1.C Queries

Our research strategy thus comprehends four separate queries. All the search strategies were complemented with "AND ("literature review" OR "systematic review" OR "review")" (written inside double quotes, which was specified to be contained in the abstract, when possible in advanced search) to indicate we were searching for a systematic or a literature review in those topics. Searching the keywords in the full text has proved, in our trial runs on databases, to provide insufficient information, thus being counterproductive to our study as more results would have to be scanned without adding more relevant results. The typology searched for were articles of the type review or simply articles, and no dates were specified.

The first query comprised (A AND B AND C). The search in the intersection of the three fields prospects an overview of the interdisciplinary research on this topic. Although economic growth *per se* is out of the scope of the project, it is fundamental to know what is the economic impact of using cryptocurrencies as complementary currencies. The second query, (B AND C), is the search in the intersection of economic growth, and CCs intends to associate the typology of CCs to their economic outcomes. This intersection is the best to grasp the general idea of what works best and what doesn't regarding the underlying mechanisms of complementary currencies. The third query, B, is the search for CCs. In this category fit articles about CCs that were not (yet) assessed for economic growth (*i.e.*, do not mention economic growth in their abstracts). The fourth query, (A AND B)[3] search, is the application of cryptocurrencies and digital currencies as complementary currencies. A query searching only A was

[3] In this search, we also included the term "complementary cryptocurrency" with OR, as it encompasses both topics.

purposefully excluded, as it only includes fields searched in detail in part two of this study.

A.1.2 Part Two – Complementary Currencies and DLTs

A.1.2.A Research Questions

RQ1. What are the main issues addressed in credit networks and complementary currencies?

RQ2. What are the implementations of the solutions and their innovations?

RQ3. What are the main technological challenges or future work of the solutions?

A.1.2.B Search Strategy

The search was run on multiple databases and no "stopping rules" were used in order to seek comprehensiveness [39].

- ***Databases***: B-On[4] (*Biblioteca do Conhecimento Online*), which is a service (using EBSCOhost services) provided by University of Lisbon and combines the following resources[5]: **ACM Digital Library**,**Elsevier**, **Sage**, **Springer**, **Academic Search Complete (EBSCO)**, **Business Source Complete**, and **Web of Science**), **Scopus**, **IEEE Xplore**
- ***Query*** *(search run on abstracts only)***:** (peer-to-peer OR blockchain OR cryptocurrency) **AND** ("complementary currency" OR "complementary cryptocurrency" "alternative currency"OR "auxiliary currency" OR "private money" OR "private currency" OR "credit network" OR "multilateral exchange" OR "multilateral barter" OR "credit clearing" OR "mutual credit" OR "mutual exchange" OR "multilateral clearing" OR "multilateral credit system" OR "scrip")
- ***Dates***: January 2012 – September 2022
- ***Filters***: (see Table A.1) Language, Typology, Peer-reviewed

The keywords for our search are similar to the keywords used in the context research section (A.1.1.B). Some keywords were dropped and others added as a result of discovering new terminology in the previous reviews' literature (mostly synonyms for *mutual credit*) and observing that some terms rarely were used. Moreover, we are removing the keyword *review* and the general term of *digital currencies*, but keeping *cryptocurrencies* as it is the subject of this thesis. The term *complementary cryptocurrency* is frequently used for the designation of complementary currencies that use blockchain, thus it was included.

A.1.2.C Screening and Selection Criteria

"Once a question has been formulated, the research protocol serves as the road map towards its answer" [1] and "establishes when the review is completed" [1]. "It defines the locations to be searched for literature and the various screens each paper will need to pass through to be considered for inclusion" [1].

[4] Available on: https://www.b-on.pt/

[5] Source: https://www.b-on.pt/en/collections/; https://bist.tecnico.ulisboa.pt/pesquisa/biblioteca-digital/b-on/

Table A.1: Inclusion and exclusion criteria

Inclusion Criteria	**Exclusion Criteria**
IC1. Written in English	***EC1***. Economic assumptions and context diverges from the European (*e.g.* underdeveloped countries)
IC2. Peer-reviewed	***EC2***. CC has a different focus/end goal rather than increasing liquidity or help businesses with exchange (*e.g. social cohesion, culture, etc.*)
IC3. Typology of academic journal, article, conference material, conference paper, conference review	***EC3***. Focus is not on technology or system but on economics, social sciences, *etc.*
IC4. Title, abstract, and keywords are relevant for our study and aligned to our thematics	***EC4***. Does not contain information about the implementation, technological or systemic design, innovation, or challenges
IC5. Free version available on the Internet	***EC5***. Presents only a high level description or does not elaborate about the implementation, technological or systemic design, innovation, or challenges
IC6. Research field of the publication is related to Computer Science, Computer Engineering or Information Systems	***EC6***. Does not help answer any research question and does not contribute with significant elements to the research

While the amount of studies that can be analysed by a reviewer is limited, a review should be comprehensive. The "goal of the practical screen is to reduce the number of studies to be analyzed" [1] to make the review manageable, but should also yield a sufficient amount of studies [1]. "To a large extent, it is the decisions made here that make the difference between a comprehensive and trustworthy literature review and an unsatisfactory one" [1]. The inclusion and exclusion criteria should be explicit for reproducibility and credibility [40]. For this reason, we present our Inclusion and Exclusion Criteria in the Table A.1 and provide an explanation for them.

Criteria explanation. (from Table A.1) *Inclusion Criteria* are applied first, before the *Exclusion Criteria*, and immediately after the query to the database. *IC1, IC2* and *IC3* are filtered during the search since most databases allow for the filtering of these options in the form of checkboxes (some include for filtering *IC6* as well - *e.g.* Scopus), however, other databases may not include such feature, or it can have a bug which is the reason these criteria are mentioned explicitly. After the retrieval of the database, the titles, abstract, and keywords are scanned (*IC4*), if they seem relevant for our research or if there is doubt, the full text version is searched on the Internet (*IC5*) and the research field of the journal should be the same as ours (*IC6*). From the list of accepted studies, the full texts are scanned (by skimming) for the *Exclusion Criteria* to further narrow the search. No criterion related to the number of citations was added to favour the innovation in this study, as blockchain and cryptocurrencies is a fairly recent research topic. *EC1* removes articles that have a different economic context, *EC2* removes articles that focus on different types of complementary currencies (*i.e., not mutual credit nor private money*), *EC3* removes articles that might be more directed towards the philosophy, ethics, politics, or other areas of the complementary currency rather the technology or system itself (unlikely to happen due to *IC6*, but can happen in interdisciplinary journals), *EC4* filters articles that focus on technology however, don't present the implementation, design, innovation, or challenges of the technology or system, whereas *EC5* removes those that do present them, but without the required amount of detail, finally, *EC6* removes articles that are similar to the ones that were already examined and/or do not contribute to the research by not advancing with different knowledge on our research questions.

A.2 Search Results

A.2.1 Part One – Complementary Currencies' Context

Table A.2 denominates the number of studies accepted from the number of studies yielded in each query, and Table A.3 presents the articles that were accepted as well.

Search →	1	2	3	4	**Total**
Query →	(A AND B AND C)	(B AND C)	B	(A AND B)	
B-On	1 / 1	4 / 7	3 / 18	0 / 1	8
Scopus	0 / 4	7 / 10	4 / 28	2 / 5	13
Total	1 / 5	11 / 17	7 / 46	2 / 6	21
Total (no dup)	1	7	5	2	15

Table A.2: Filtered search results of prior SLRs per database and query (formatting: *accepted* / *inspected*).

A.2.1.A Analysis of Results

The search results are presented in Table A.2 are analysed as follows[6]. IEEE Xplore was also searched but did not return any results. From the results of the first query (A AND B AND C), rejection reasons comprised different focus (n=3) (politics, capitalism, central bank digital currencies), and different typology (n=1) ('Book Chapter'). The field of cryptocurrencies is recent, thus reviews on cryptocurrencies, complementary currencies and economic growth are limited. The rejection reasons from query two (B AND C) comprised fitting best to a different intersection (n=2) of the diagram A.1, different focus (n=3) (a fund model, politics of blockchain, central bank digital currencies), unmatching granularity (n=1) (a review of a single article), and duplicates (n=4). Query three (B) rejections included: belonging to another intersection (n=14), different focus (n=9) (housing, stock market, batteries, surveillance capitalism, privacy, politics of blockchain, knowledge markets, central bank digital currencies); different topic (n=2)

[6] **Scopus**: filtered by *Document Type*:'Article', 'Review', 'Conference Paper' and *Language*: 'English'; **B-On**: filtered by 'Peer Reviewed', *Document Type*: 'Conference Materials', 'Academic Journals', 'Reviews', and *Language*: 'English'.

(review of a wastewater system built with private money, farmers), different goal (n=4) (higher education, grassroots, community service money, public libraries); different economic context (n=2) (poverty); being assessed for economic impacts (n=1); being a different format (n=3) (experts' opinions, model, theory); not being a review nor containing an extensive review of the literature (n=2); and duplicate studies (n=2). Rejections in query four (A AND B) were better suitability in different intersection (n=1) and different focus (n=3) (privacy, politics of blockchain, central bank digital currencies).

A.2.1.B Accepted Studies

Table A.3 contains the accepted articles for the review separated by query. Although the query search strategy can be the studies' coding, grouping queries 2,3 and 4 as shown in the table, is more coherent as the recurring topics are more tightly coupled.

Coding	Search	Query	Accepted Studies	Total
Bitcoin	1	(A AND B AND C)	[10]	1
CCs	2	(B AND C)	[4] [6] [3] [5] [8] [7] [9]	7
	3	(B)	[41] [42] [43]	5
	4	(A AND B)	[44] [45]	2
Total				15

Table A.3: Accepted studies from the prior literature reviews search per query

A.2.2 Part Two – Complementary Currencies and DLTs

A.2.2.A Analysis of Results

Querying Scopus, B-On and IEEE Xplore and applying the inclusion and exclusion criteria resulted in the flowchart of Figure A.2. The rejection reasons are depicted in the figure as they comprise either not be complacent with inclusion criteria or matching exclusion criteria.

A.2.2.B Coding of Selected Papers

The accepted studies were separated by their focuses, resulting in the coding of the results, which is illustrated in Table A.4, and could be divided into two groups: directing their study towards the credit network or studying the complementary currency. Each of these groups can then focus on the technology behind the credit network or complementary currency, or the systemic challenges or innovations. The latter is harder to find in journals that relate to Computer Science, since it relates more closely to the Economics journals, and this part focuses on technology.

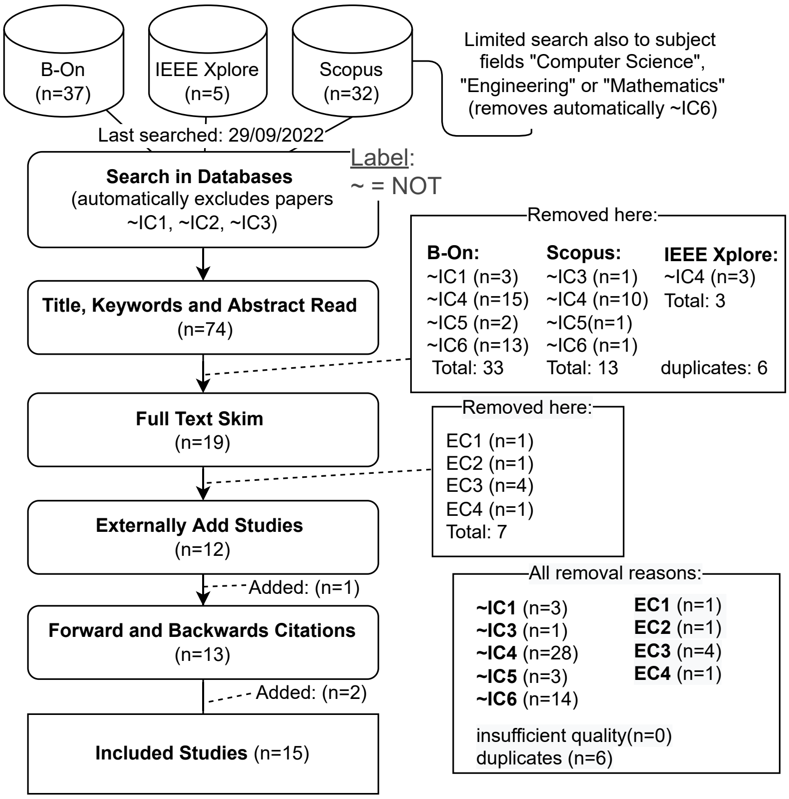
B-On (n=37)
IEEE Xplore (n=5)
Scopus (n=32)
Limited search also to subject fields "Computer Science", "Engineering" or "Mathematics" (removes automatically ~IC6)
Last searched: 29/09/2022
Label:
~ = NOT
Search in Databases (automatically excludes papers ~IC1, ~IC2, ~IC3)
Title, Keywords and Abstract Read (n=74)
Removed here:
B-On: ~IC1 (n=3) ~IC4 (n=15) ~IC5 (n=2) ~IC6 (n=13) Total: 33
Scopus: ~IC3 (n=1) ~IC4 (n=10) ~IC5(n=1) ~IC6 (n=1) Total: 13
IEEE Xplore: ~IC4 (n=3) Total: 3
duplicates: 6
Full Text Skim (n=19)
Removed here:
EC1 (n=1) EC2 (n=1) EC3 (n=4) EC4 (n=1) Total: 7
Externally Add Studies (n=12)
Added: (n=1)
All removal reasons:
~IC1 (n=3) ~IC3 (n=1) ~IC4 (n=28) ~IC5 (n=3) ~IC6 (n=14)
EC1 (n=1) EC2 (n=1) EC3 (n=4) EC4 (n=1)
insufficient quality(n=0)
duplicates (n=6)
Forward and Backwards Citations (n=13)
Added: (n=2)
Included Studies (n=15)

Figure A.2: Flowchart of the application of inclusion and exclusion criteria to the query results

Theme	Focus	Niche	References	Total
CCs	Systemic/Applications	IOU	[22]	1
	Technology Related	IOU	[23] [24]	2
Credit Networks	Systemic/Applications	Agent Behaviour	[25] [21] [20]	3
	Technology Related	Performance in Routing	[17] [19] [18] [26]	4
		Privacy in Routing	[11] [13] [15] [12] [16]	5
Total				15

Table A.4: Coding of the accepted studies for full text read

B

DLTs for Mutual Credit / CCs

B.1 Hypersyn

Hypersyn is a permissionless P2P payment network proposed in [27] that uses the concept of Merkle trees, mutual arbitrage and mutual credit (MC, which behaves similar to credit clearance [27]). It does not require consensus mechanisms, a distributed ledger, or validators [27].

Merkle trees are secure data structures (binary trees with cryptographic hashed on its leaves) that allow to determine in $O(logn)$ time if a certain element is present in a list, without having to reveal the elements of the list or providing the complete list. In the Bitcoin blockchain, Merkle trees were intended for SPV nodes, *i.e.,* lightweight clients such as wallets, which do not store the entire ledger, just blocks' headers, and on demand retrieve blocks by requesting it to multiple full nodes, who have the entire copy of the ledger for the transaction of the blocks of interest [33]. A SPV node "locally and independently creates, validates, and transmits transactions" [33].

Double Spending. The author argues that since the supply of money is elastic in MC systems, the double spending problem does not exist. "By redefining what money is, we manage to dissolve the double spending problem" [27]. Therefore, there is no need for a blockchain, whose intended purpose was to mitigate the double-spending problem. Thus, no need for consensus but rather a robust data structure to store the state of the system, a SMT.

Sparse Merkle Tree (SMT) solve some limitations of Merkle trees. While verifying presence of elements in the list is $O(log(n))$, the update, insertion, deletion and proving the absence of elements is inefficient [27]. Therefore, Hypersyn uses SMTs, which present the properties of Conflict-free Replicated Data Type (CRDT), making them a suitable data structure to keep the state of MC edges.

Mutual Arbitrage. "[M]oney in Hypersyn is treated as freely tradable debt, which inherently requires trust" [27]. But "what is really being transferred when transacting in Hypersyn is not money in the conventional sense, but a system-wide change in one's exchange value (or purchasing power)" [27] which "is determined through its connections E, also known as edges or relations, with other nodes" [27]. While "nodes cannot own another node's credit" [27], they "change the exchange value between their credit and that of their peers by modifying the credit reserves of their edges" [27]. Since credits do not have the same value, edges between nodes work as AMM, which "were originally designed to create decentralized exchanges (DEXs) for digital assets in the blockchain space" [27]. "Hypersyn however, instead of using the constant function to trade digital assets in a DEX, we use it to make peer-to-peer credit payments between peers, and to determine the exchange values between different credits" [27].

Benefits. Hypersyn is "a tool that aims to offer a qualitative change in the way we exchange [... and ...] enable mutual credit systems to scale beyond small communities" [27]. "It has the potential to increase the autonomy and self-organization that people can have, by enabling people to become both the creditors and debtors of their own "money" through mutual credit" [27].

B.2 ReSource Protocol

Framework and Protocol. ReSource is an application layer protocol launched in the Celo blockchain that provides a flexible and comprehensive framework for the development of distributed MC systems [38].

On-chain Mutual Credit. ReSource groups and makes available to use common elements to MC systems "such as 1) endogenously created stable credits, 2) overdraft-enabled current accounts, 3) distributed underwriting and risk management, and 4) distributed debt collection and obligation enforcement" [38]. It also provides several participant roles in the network: member, who trades with other members; ambassador, who onboards members and conducts brokerage; underwriter, who deals with risk; and delegating stakers, who delegate stake to underwriters, assuming the risk [38].

Underwriting. Underwriters stake SOURCE, the governance token of the protocol, when evaluating new members credit line requests with the help of an underwriting algorithm, which is taken if the member defaults or a fraction of future transaction fees is received otherwise. The underwriting algorithm aggregates bank and social media networks data to assess credit scores, which helps underwriters decide on the credit term offerings to submit in a competitive auction with other underwriters [38]. Underwriters aggregate accounts into packages that represent debt portfolios offered to delegating stakers as a staking pool.

Default Insurance. A member is considered in default after "maintaining a negative balance for more than 6 consecutive months (adjustable by governance)" [38]. Defaults in MCs mean inflation and contraction of supply, as other users are entitled to fewer resources after the default, devaluing their positive balances. Therefore, ReSource reimburses network's members for the defaulting agents, taking SOURCE from transaction fees, confiscated underwriter stakes, ambassador penalities and debt sales and converting to RSD (the unit of account of the MC network), which is pegged to the US Dollar and can be redeemed in the open market [38].

Negative Balances. "Traditionally, account balances in decentralized systems only maintained positive balances" [38]. Therefore, RSD was created using "CIP36 (Celo Improvement Plan) which is a fungible token standard designed to implement and abide by the ERC20 standard but behave like a mutual credit currency" [38].

B.3 Holochain

Framework and Protocol. Holochain is a framework to develop P2P applications [46], designed to work with MC. The framework manages the distributing computing, data persistence and the P2P communication layer protocols to enable developers to focus on their applications and keep development minimal [46].

Application Organization. Holochain dApps are highly modular and referred to as *hApps.* A hApp granular functionality is "called a DNA, has its own business rules, isolated peer-to-peer network, and shared database" [46]. "A client running on a participant's device talks with their conductor, which runs multiple hApps. Each hApp is made of one or more cells, which are the live instances of DNAs that run on behalf of the participant. These DNAs, in turn, are made of one more executable zome modules" [46]. A zome (short for chromosome) "define the core business logic in a DNA, exposing their functions to the conductor" [46], as an API, which is also available to other zomes, and do not keep state. In sum, zomes (functions exposed with APIs) are bundled into DNA (microservices) that run as cells in the hApp. The conductor mediates the hApps' network access.

Agent Centricity. Holochain uses an agent centric approach, meaning that every participant of the network, "is running their own copy of the application and connecting directly to their peers" [46], they are "the ones who use the application are also the ones who keep it alive" [46]. Each participant supply their computational resources and storage to store and validate data of the network [46]. Agent centricity contrasts with data centricity used in blockchains. "Blockchains don't record a universal ordering of events – they manufacture a single authoritative ordering of events – by stringing together a tiny fragment of local vantage points into one global record that has passed validation rules" [47]. In an agent centric approach, nodes “participate in the system as whole even though they are not constrained to maintaining the same chain state as all other nodes” [47].

Distributed Hash table. Unlike in blockchains, Holochain does not replicate the distributed ledger on every peer. Instead, peers keep the information that is relevant to them and extra information from the other peers’ data to create redundancy. “[A] Holochain application consists of a network of agents maintaining a unique source chain of their transactions, paired with a shared space implemented as a validating, monotonic, sharded, distributed hash table” [47]. Pieces of data are attributed an address in the hash graph, and each peer is responsible for a range of addresses [46]. The data of a peer’s actions on the network is kept in an append-only immutable record called source chain, which can be public or private, and is stored in the devices of the peers. Asymmetric cryptography is used to write entries on source chains [46]. “Each piece of public data is witnessed, validated, and stored by a random selection of devices” [46]. In a Holochain network, “all cooperating participants detect modified or invalid data, spread evidence of corrupt actors or validators, and take steps to counteract threats” [46].

B.4 Stellar Network

Blockchain. Stellar is a blockchain that enables developers to build application, issue assets and building anchors. Anchors are on and off ramps, *i.e., ways to convert tokenized assets into the objects and vice-versa, such as converting cryptocurrencies to fiat money* [36]. The network is composed by a pub net, intended for production use, and a dev net for development testing [36].

Development. While developing a product, an SDK to access the RESTful API, can be used to interact with the blockchain, but it is advised to run an independent instance of the Horizon server that serves the API [36].

Consensus. Stellar Consensus Protocol (SCP) uses Federated Byzantine Agreement (FBA), which “differs from [...] consensus mechanisms like Proof of Work (which relies on a node’s computational power) and Proof of Stake (which relies on a node’s staking power) by instead relying on the agreement of trusted nodes” [36]. From the three desirable properties of distributed systems, SCP “prioritizes fault tolerance and safety over liveness” [36], meaning the system can fail to make progress if there is no consensus. The network is open for new nodes, and there is no incentive to validate and store transactions other than for the system’s security and resilience. Each validator trust a set of other nodes in the network, called the quorum set, and sets a threshold (a quorum slice representing the minimum amount of nodes from the quorum set) to vote in the consensus.

Operations and Features. Operations using the Horizon API include creating account, making payments, managing offers from the decentralized distributed exchange’s order books, changing trust (trustlines serve to allow transfers of assets from an issuer), merging accounts (transfer balance and destroy the empty account), create claimable balance (that split payments in two parts, the creation of the balance, and it's claim, which can be useful for new anchors that do not have trustlines set up), sponsoring ("allow an account (sponsoring account) to pay the base reserves for another account (sponsored account)" [36]), clawback (burns the specific asset from the receiving account), and liquidity pool deposits and withdrawals [36]. There also are features of channel accounts, that "provide a method for submitting transactions to the network at a high rate" [36], address federation that attributes Stellar addresses to email-like identifiers, which helps with payments, fee bumping allows paying the fee without saving to sign the transaction again, which can help when employing fee strategies, path based payments (either the initial quantity of the asset or the final received quantity must be specified), multiple users accounts (pooled accounts without user separation and muxed accounts that separate users in a shared account) and multi party signatures [36].

Interoperability. Stellar focuses on the interoperability with real world assets, as there is support for setting up cross-border payments (transfers between two anchors), and deposits and withdrawals on and off the Stellar network using a wallet that connects to an anchor.

B.5 XRPL

Protocol and Framework. The XRPL is an open-source permissionless blockchain [35] that offers many functionalities to enable different types of payments.

Consensus. The XRPL Consensus Protocol prioritizes "the following principles, in order of priority: Correctness, Agreement, Forward Progress" [35], meaning "the network fails to make progress rather than diverging or confirming invalid transactions" [35]. Unlike blockchains such as Bitcoin or Ethereum, XRPL cannot switch to the longest chain as approved (validated) transactions are final [35] and will never be disapproved (correctness property), which increases the transaction confirmation speed. Blocks in XRPL are called *ledger versions* and contain the current state of all balances (unlike many blockchains), new transactions and metadata about the block, such as its index and hash [35]. The participants in the network (nodes) are called *rippled* servers. Each rippled server has a Unique Node List (UNL) which is a set of validator nodes it trusts (*i.e.,* "believes will not conspire to defraud them" [37]), which do not need to be directly connected as the gossip protocol is used for communications. "Since anybody can run a validator, the burden is on the network participants to choose a reliable set" [37], therefore, there are recommended default UNLs (*dUNLs*) "of high quality validators, based on past performance, proven identities, and responsible IT policies" [37], published by accredited entities such as XRPL Foundation, Ripple and Coil [37]. A validator can, however, choose its own trusted validators and not follow any of the dUNLs. A consensus is reached when the majority of nodes from the network agree and fewer than 20% are faulty [35]. " But if more than 20% of the network did not follow the same protocol rules as the majority, the network would temporarily halt" [37], needing validators' reconfiguration of UNLs. The network stops making progress when the number of faulty nodes is more than 20% and less 80% of the trusted validators. XRPL's native currency is XRP, and it is used to pay fees (reserve and transaction), protecting the network against spam (transaction fees are dynamically set for this purpose based on demand), and (automatically) help bridge currencies when it is necessary [35]. XRP supply is fixed and new XRPs are not mined, their value increases as XRP from fees is burned.

Validator Incentives. A rippled can become a validator or simply store the ledger, but all rippleds are full nodes (store the entire copy of the ledger) [35]. Running a validator in terms of electricity cost is similar to running an email server [37]. Since the cost of running a rippled is minimal, incentives are not necessary [37]. The "primary incentive to run a validator is to preserve and protect the stable operation and sensible evolution of the network" [37].

Application Stack. To interact with the XRPL, apps such as exchanges, wallets, explorers can connect to a REST API, which import a library that apps can also use directly (eases the data format conversions), or resort to web sockets or JSON-RPC to connect with a rippled server from the network [35]. Web sockets are bidirectional communication channels, allowing push functionalities from the server to the client (subscribing to topics), while RPCs are unidirectional and comprise client to server calls. XRPL provides a Mainnet for deployment, dev net for advanced development stages and Testnet for initial developments. Moreover, it is possible to run a local rippled server for testing, or deploy a sidechain for the app ecosystem (see B.5.0.A).

B.5.0.A Operations and Features

Although XRPL's primary purpose is payments, it also enables special kinds of payments, which would usually require smart contract programming, but are available in the XRPL out of the box. Every operation is registered using a transaction - "[t]ransactions are the only way to change the XRP Ledger" [35]. Transactions are authorized by digital signatures using EdDSA [35]. An account in XRPL is identified by an address, holding XRP balance, containing a sequence number for operations order and single execution, history of the transactions and operation signing methods [35]. Non-XRP currencies are stored in trust lines instead of accounts as XRP [35]. To **create an account**, a payment (from an existing account, *i.e., funding*) must be performed to a mathematically-valid address, which automatically creates the account if it does not exist and the payment's amount is at least the reserve (minimum balance defined in XRPL) [35].

Payment Types. There are **direct**, **cross-currency**, **checks**, **escrow**, **partial payments** and **payment channels** [35]. Direct payments are XRP transfers which can be transacted without trust, unless account settings prohibit unknown accounts transactions. Operations such as **escrow** (holding payment until confirmation or certain conditions are met) and **payment channels** (paying without committing each single transaction to the ledger for better throughput) are only available for XRP payments [35]. Partial payments subtract from the transaction fees from the transacted amount instead of delivering the entire amount in the destination and charging fees from the balance, which is useful when returning payments [35]. Checks “let users create deferred payments that can be canceled or cashed by the intended recipients” [35], applied to non-XRP tokens as well, however, the resources are not locked in the issuing account, which can make the check redemption fail if there are not enough funds. Cross-currency payment feature is based in payment routing across multiple wallets and finding the best route for the currency conversion and payment.

Multi-signing “is a method of authorizing transactions for the XRP Ledger by using a combination of multiple secret keys” [35]. Use cases for multi-signing include sharing custody of a wallet, delegating signing of a wallet, multiple authentication and backup [35]. A list of signer addresses (XRPL supports up to 8 addresses), each address with a weight and a signer quorum, must be provided to configure multi-signing [35]. The transaction cost of this operation is at least the number of signatures needed + 1 higher than a normal transaction [35].

Deposit Authorization. Using the account setting of deposit authorization, it is possible to block payments from all accounts except the previously preauthorized [35]. Transfers of checks, escrows, and payment channels occur in two-step fashion (transfer and confirmation), and with this setting enabled, they need a preauthorization to do so. [35]

Collecting Fees. Aside from neutral fees from transactions and minimum reserve requirements (to prevent network from abuse), issuers can define transactions fees of their token to other addresses, and can enable a *trust line quality* setting which “allows an account to value balances on a trust line at higher or lower than face value” [35].

Source and Destination Tags. Tags “can indicate specific purposes for payments from and to multi-purpose addresses” [35] by specifying the beneficiary or destination [35]. They are not on-ledger functionality, but provide information to off-ledger systems [35]. Use cases include specifying the destination account for payment for exchanges or gateways, or information regarding what is being exchanged off-chain [35].

Token Issuing. XRPL allows anyone to issue tokens on “relationships called trust lines between accounts” [35]. Trust lines allow non-XRP tokens to be sent according to the maximum amount specified in the trust line, if it is not froze. Tokens in XRP Ledger (XRPL) represent digital assets such as stablecoins [35] (which can be any asset backed 1:1 with the token, usually it is a tangible asset), community credit to track debt between users who trust each other (debts can be settled automatically and atomically in XRPL) [35], *i.e. rippling*, or ICOs [35]. Tokens are used for cross-currency payments and traded in the decentralized exchange, they can have transfer fees and a variable number of significant digits [35] (divisibility).

Hooks. Hooks resemble the smart contracts functionality in XRPL. Hooks are small pieces of code, written in any programming language compilable to web assembly, typically C, that add logic to the incoming and/or outgoing transactions such as forwarding transaction, interaction with DEX, blocking transactions that do not meet certain criteria [48]. XRPL allowed for many operations and payment types which serve multiple use cases, which typically require smart contract development (*e.g.,* issuing tokens) as they do not exist embedded in blockchains. Hooks add even more functionality and power to XRPL dApps. Hooks are purposefully not Turing complete (all loops need an upper boundary) [48], to not allow wasting computational power and overloading the network and identify the worst possible executing scenario, which will also serve to calculate the associated fee. Each account can have a chain of at most 4 installed hooks [48]. Since it is a more costly operation, and Hooks can be configured with different parameters/settings, it is possible to upload the hook once and the code once and reuse it with reference counting by several accounts to save fees [48]. At the time of the writing, Hooks are a very recent feature of XRPL currently in alpha testing, undergoing code revising and quality assurance to be incorporated in the official open source XRPL repository.

Decentralized Exchange. "The exchange allows users to buy and sell tokens for XRP or other tokens, with minimal fees" [35]. The XRPL DEX pairs currencies (identified by issuer and currency code) during trades. A trade consist of an offer, which works as "a limit order to buy or sell a specific amount of one currency (XRP or a token) for a specific amount of another" [35], that is (partially or totally) consumed if/when matching offers exist (multiple offers can match) in the Order Book or saved in it otherwise. The DEX is not recommended for high-frequency trading as trades are only executed every 3-5 seconds [35].

Federated Side Chains A sidechain is a parallel network of rippled servers and validators that can interact with other chains of XRPL, such as the Mainnet, but have different consensus and rules, working together as simultaneously an independent and interoperable blockchain based on the XRPL technology [35]. Use cases include building permissioned interoperable networks, creative a native token, and multiple functional customizations. The *door* accounts allow making cross-chain transactions (by sending the transaction to these doors), *i.e.,* moving assets from one chain to another [35]. These transactions are listened and mirrored by *federators* (servers) in both chains [35]. "Transactions within the sidechain are not visible to the servers on the mainchain" [35].

Fraud Detection. XRPL is a public ledger, all transactions and accounts are publicly visible in explorers such as bithomp and xrpscan. Therefore, fraudulent activities such as money laundering and scams can be spotted by the public. In particular, "Ripple is committed to monitoring and reporting any AML flags across the XRP Ledger network, as well as reporting suspicious activity" to authorities [37].

C

CLi Commands

When running `python main.py -h` in the `inclusiveCryptoEconomyProject\inclusiveCryptoEconomy` directory, a similar to the following output is produced:

Listing C.1: Output of CLi after python main.py -h

```
Interact with your credit network

    create-account    Create account or ask to create account
    generate-account  Generate account in XRPL testnet
    show-account      Show you account details such as wallets, balances, trusts
    set-trust         Create or update trust/trust line
    issue-iou         Issue IOUs on your behalf
    make-payment      Make a payment of any currency in wallet
    make-payment-xrp  Make a payment of xrp
    exchange-asset    Exchange IOUs, Fidelity Points, Gifts, Debt for other or XRP
    remove-offer      Remove an offer you created from the decentralized exchange
```

```
show-my-offers    Display your offers in the decentralized exchange
show-market-offers Display market offers from the decentralized exchange
send-check        Send a redeemable check of an amount of currency you own or going to own
redeem-check      Redeem a check
trust-salary      Trust salary points by a salary issuer
trust-fidelity-points
                  Trust fidelity points by an issuer
trust-debt        Trust debt of an issuer
trust-donations   Trust donation by an issuer
pay-with-salary   (Employees) pay with salary by a salary issuer
confirm-debt-repaid
                  Confirm a debt has been repaid by a debt issuer
send-fidelity-points
                  (Businesses) send your fidelity points to your costumers
pay-salary        (Businesses) pay salary with your SLY IOUs to your employees
register-debt     Pay with your DBT IOU to any lender (will try transfer the amount
                  and if it fails, a check of the amount is sent on your behalf)
donate-as-institution
                  (Charities) Issue and send DON tokens for people to use the token on your name
pay-with-salary-promise
                  Send a redeemable check of SLY you expect to own
send-gift-card    (Businesses) Send a redeemable check of GFT you own or going to own
pay-with-promise  Send a redeemable check of a currency you own or going to own
redeem-gift-points Redeem check and receive GFT from issuer
accept-debt       Redeem check and receive DBT from issuer
buy-fidelity-points
                  Buy discounted FID (fidelity points) from issuer with XRP
buy-gift-card     Buy discounted GFT (gift cards) from issuer with XRP
buy-donation      Buy a zero note "000" from issuer with XRP to donate
sell-gift-card    (Businesses) sell your GFT cards to your costumers for XRP
start-marketing-campaign
                  (Businesses) sell your FID points to your costumers for XRP
ask-for-donations (Charities/Businesses/Individuals) ask for XRP donation
finish-marketing-campaign
                  Remove an offer you created with FID (fidelity points)
```

D

Credit Network Domain Model Diagram

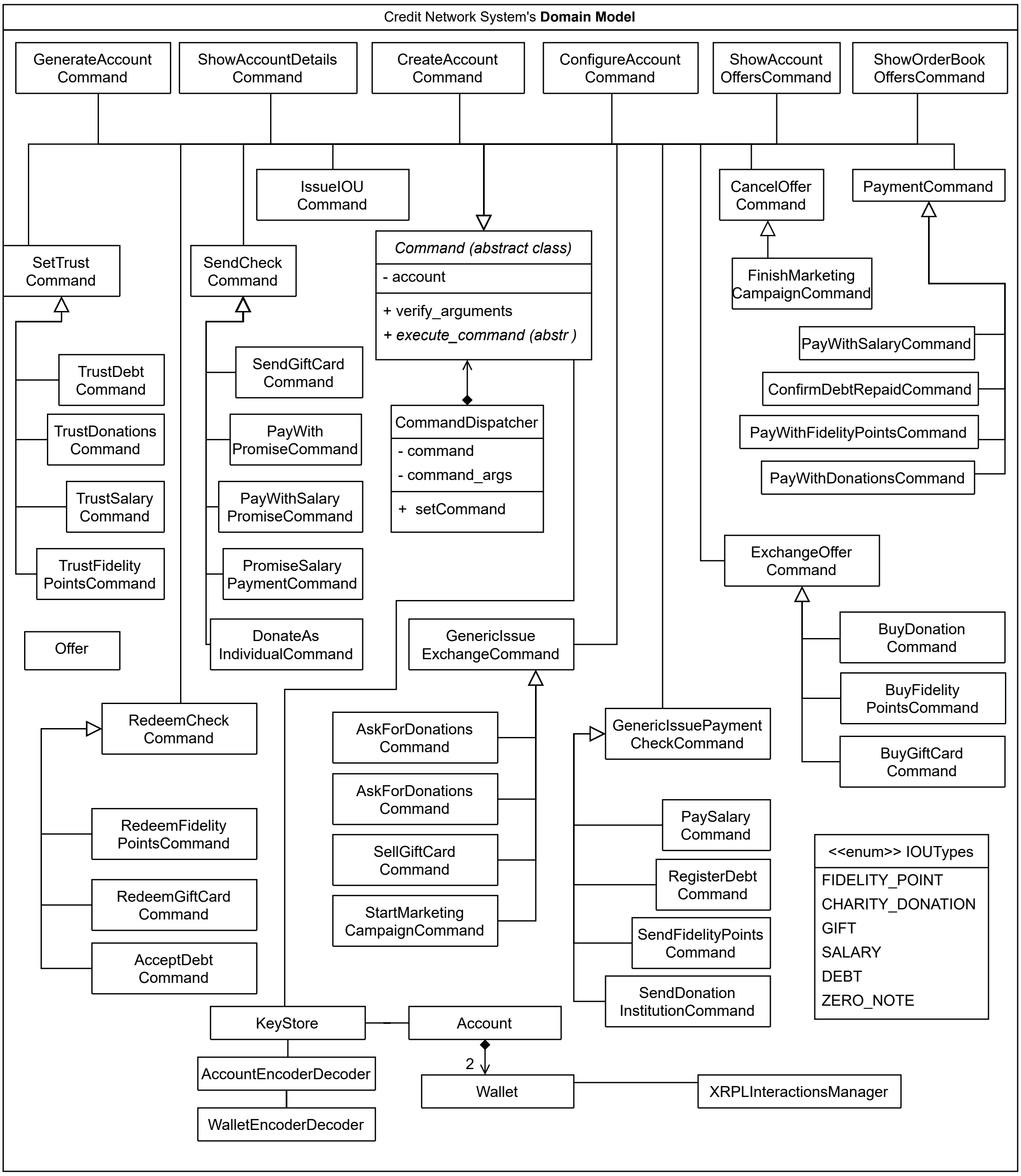

Figure D.1: Class diagram of the solution