IJCCR

www.ijccr.org · ISSN: 1325-9547

Friis, G. & Glaser, F. (2018). Extending Blockchain Technology to host Customizable and Interoperable Community Currencies. *International Journal of Community Currency Research 22* (2), 71-84. https://doi.org/10.15133/j.ijccr.2018.017

International Journal of Community Currency Research

2018 VOLUME 22 (SUMMER)

EXTENDING BLOCKCHAIN TECHNOLOGY TO HOST CUSTOMIZABLE AND INTEROPERABLE COMMUNITY CURRENCIES

Gustav R.B. Friis* and Florian Glaser**

* Brainbot Technologies AG, Mainz

** Karlsruhe Institute of Technology (KIT), Karlsruhe

ABSTRACT

The goal of this paper is to propose an open platform for secure and interoperable virtual community currencies. We follow the established information systems design-science approach to develop a prototype that aims to combine best practices for building mutual-credit community currencies with the unique features of blockchain technology. The result is a specification of an open Internet platform that enables users to join and to host customized community currencies. The hosted currencies can be classified as credit-based future type of money with decentralized issuance. Furthermore, we describe how the transparency, security and interoperability properties of blockchain technology offer a solution to the inherent problems of existing, centrally operated community currency software. The characteristics of the prototype and its ability to fulfil the design-objectives are examined by a relative evaluation against existing payment and currency systems like Bitcoin, LETS and M-Pesa.

KEYWORDS

Virtual community currencies; blockchain technology; mutual-credit; LETS; Trustlines Network

To cite this article: Friis, Gustav R.B. and Glaser, Florian (2018) 'Extending Blockchain Technology to host Customizable and Interoperable Community Currencies' *International Journal of Community Currency Research* 2018 Volume 22 (Summer) 71-84 <www.ijccr.net> ISSN 1325-9547. DOI http://dx.doi.org/10.15133/j.ijccr.2018.017

1. INTRODUCTION

Community currencies are created by groups of citizens or businesses and circulate as a complementary to national currencies that are jointly created by governments, central and commercial banks. Being either commercial or community oriented, complementary currencies, is not an alternative to but a complement to the conventional money system, by providing new tools that can operate in parallel with it, without replacing it (Lietaer 1997, Kennedy et al 2012). For Internet based virtual community currencies, mutual-credit systems such as a LETS (Local Exchange Trade System) and Time dollars have been argued to have particular desirable characteristics (Lietaer 1997). This is because credit/IOUs exchanged by participants within a mutual-credit system, serve as a particular good medium of exchange, as they are a cost free, elastic and dispersive issued type of money (Schraven 2000, Kichiji and Nishibe 2012). However, there are still constraints that limit the usefulness of community currencies as outlined below. The overall goal of the prototype proposed in the second part of the paper is to alleviate these current constraints.

First, the trust between participants in a mutual-credit system declines after it reaches a certain number of participants (Schraven 2001). This limits the scope of using IOUs as a medium of exchange. The scope is limited further due to the constraint that the few software solutions (i.e. digital trading platforms), which enable exchange of community currencies, constitute a central weak link (Slater and Jenkin 2016). These platforms are not transparent, rely on the honesty of the operators and bear an inherent risk of being targeted by malicious attacks. As a response to the limitation on participant size and to reduce the opportunistic free-rider behaviour, mutual-credit systems are advised to have governance mechanisms in place (Schraven 2001). Moreover, to enhance accountability among participants, it has been proposed to design bilateral instead of multilateral mutual-credit systems (Fugger 2004). To address the weak link of centralised exchange platforms, blockchain technology enables exchange without relying on trust in third parties (Nakamoto 2008). However, the security enhancing property of blockchain technology has thus not yet been put to good use to create robust and interoperable mutual-credit community currencies. This raises the question how to combine the best practices of both mutual-credit and blockchain technology in order to empower Internet based virtual community currencies. Hence, we formulate the following research question that guides this work:

How can existing blockchain infrastructure be extended to allow for secure and interoperable virtual community currencies?

To answer the research question, a design-science approach is followed in order to present a prototype that addresses design objectives identified in the fields of community currencies and blockchain technology. The remainder of this paper is structured as follows: Chapter 2 presents the background and literature regarding virtual community currencies and mutual-credit systems. In particular, in that chapter we identify the benefits and limitations of community currencies in the role of a medium of exchange. This is followed by an analysis of the strengths and shortcomings of current blockchain based virtual currencies, which eventually leads to the identification of the design objectives for the prototype. Chapter 3 describes the properties of the proposed prototype. In chapter, 4 we discuss and evaluate its usefulness compared to the design objectives. Finally, chapter 5 comprises the implications and conclusion of this study.

2. BACKGROUND & LITERATURE

2.1. Virtual community-currencies

According to the EU funded Community Currencies in Action (CCIA) initiative, community currencies are defined by being "tied to a specific, demarcated and limited community" (People Powered Money 2015). Derived from Latin, 'community' translates "to give among each other", which can be interpreted to reveal "the key relationship between gift exchanges and community building" (Lietaer 1997). To exchange gifts is a genuine collaborative act, fundamentally based on qualitative human values such as trust, respect and gratitude. This leads to the conclusion that communities are characterised by a high degree of highly interpersonal relationships. A community-based concept of exchange is thus in contrast to national currencies (i.e. fiat money). The majority of national currencies are artificially scarce money created by banks extending loans, and is, by design, bearing interest. These properties induce competition rather than collaboration among currency participants (Kennedy et al: 2012). The present

reality of a worldwide monetary monoculture has been demonstrated to cause community corrosion and to be a main catalyst for the global recurring economic systemic crashes (Lietaer et al 2010). In contrast, community currencies induce countercyclical effects (Stodder et al. 2009, Lietaer et al 2010), insofar monetary sustainability is a function of providing resilience through diversity (Ulanowicz et al. 2008).

With the rise of the Internet, crowdsourcing, open-source and creative commons movements have emerged, and brought along internet-based virtual community currencies. In 1997 this led Bernard Lietaer to identify 5 desirable characteristics for virtual community currency designs. These are 1) to be efficient and secure in an electronic payment system, 2) convertible into local expenses, 3) non-national, 4) self-regulating on the net itself and 5) supporting the creation of communities (Lietaer 1997). After realizing that no virtual currency meeting these characteristics existed, Bernard Lietaer elaborated:

"Currency systems modeled after Michael Linton's: LETSystem (Local Exchange Trading System) and Edgar Cahn's Time Dollars hint at an answer. They are Mutual Credit Systems where two participants agreeing on a transaction create the necessary currency respectively as a debit and credit. They are therefore self-regulating, needing no Central Bank to monitor money supply. Most are already completely computerized. Finally, most important for our purposes here, there is ample pragmatic evidence that using such currencies actively promotes cooperation rather than competition among participants" (Lietaer 1997).

To get an idea of why such mutual-credit systems are feasible compared to other systems, the Value-Sequence Typology of Money (Bendell and Slater 2015), is a useful framework. This typology is, with inspiration from historian (Zarlenga 2002), antropolog (Graeber 2011) and Chartalist economist (Wray 2007), based on interpreting money and currency as systems of agreements and symbols that support claims on goods or services.

Table 1: The Value-Sequence Typology of Money

	Past Money	**Present Money**	**Future Money**
Symbolizes	Past value created	Present intrinsic value	A promise of future value
Issuance	Quasi	Concentrated	Dispersive
Accepted	Because people know it represents and/or rewards past value created	As it is backed or has value in itself which can be exchanged for an equal value	Based on the perception it can be exchanged for value later in time
Function	Rewarding effort	Store of value	Medium of exchange
Example	Bitcoin	Gold coin	Credit/IOU

Summarized by table 1, the typology defines how types of money can be distinguished by representing past, present or future value. The present value type of money, say for example a gold coin, is expensive to produce, can be hoarded, and has to be issued by a central institution taking care of production and supply. As a medium of exchange, it is therefore limited in its availability for all the people that have an interest in making mutually beneficial transactions. Hence, as gold is perceived as a valuable commodity in itself, it has, throughout history, provided a certain value, which has made it a good store of value (Bendell and Slater 2015). As LETS is an interest-free mutual-credit system there are no (physical) stocks or commodities required to perform transactions. This is because in a mutual-credit system, money is represented as a promise of future value (IOU) between all LETS participants. This value is realized when one LETS participant provides goods or services to another participant at a future point in time. Transactions leading to negative and positive credit for buyer/seller are recorded in a central ledger in a traditional double-entry bookkeeping fashion. As a consequence of the cost-free, elastic and decentralised issuance of money triggered by participants' actual transactions, the IOUs exchanged in a LETS system are by design a useful medium of exchange (Schraven 2000).

Nonetheless, a mutual-credit LETS system based on multilateral agreements between a number of participants imposes significant challenges. As highlighted by Slater and Jenkin (2016) a LETS system is all about trust between its participants and, as more people join, the average level of trust between the participants declines. A decline in trust lowers the willingness to accept issued credit, and jeopardizes the stability of the system. This social dynamic can be depicted as an inverted U-Shape (Schraven 2001), in which the system stability initially increases with size (i.e. number of participants) and, at a certain point, declines with any further increase in size. One way to deal with the decline of trust is to impose governance mechanisms in order to eliminate opportunistic behavior (Schraven 2001). For example, reducing free riding by restricting the upper limit of debit of a single participant's account (Kichiji and Nishibe 2012). To bring more accountability into the spending of credits, the Canadian LETS member Ryan Fugger published "A Proposal for a Decentralized Currency Network Protocol" (Fugger 2004). This design proposes a bilateral instead of a multilateral mutual-credit system. In essence, it results in an interconnected network of LETS systems, each operated by an individual participant.

A limited size of participants in a bilateral or multilateral mutual-credit system sets inherent boundaries for the use of IOUs as a medium of exchange. That is, there will be an unmet need for a variety of services and goods that are not offered within the community. For this reason, it might be beneficial for participants to be able to exchange with participants of other communities that are able to supply such unmet needs (Martignoni 2015). Centralized platforms for this purpose have existed since 2004, and have typically been based on interconnected Clearing Centrals or Regional Sub Hubs (Huber and Martignoni 2013). This way of exchange has been argued to constitute a weak link due to the centralised platform software (Slater and Jenkin 2016).

This centralization has two crucial implications. First, community participants have to rely on the honesty of the 3rd party platform operators to process the electronic payments in the correct way according to predefined rules. As the transactions are processed and mediated by the platform operators they are reversible and modifiable, which in turn makes it non-transparent for community participants to assess their legitimacy. Second, centralised platforms have a 'single-point of failure' architecture, which makes them vulnerable to malicious attacks. While security and transparency breaches affect the process of exchange on centralised platforms in general, they also affect the accounting processes in particular. That is, centralised accounting systems, digital or offline (e.g. manual accounting by community participants), are vulnerable to malicious attacks.

2.2. Shortcomings of blockchain based community currencies

As a solution to the inherent problem of exchanging virtual value on centralised platforms the anonymously individual/group known as Satoshi Nakamoto published the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008. The bitcoin whitepaper concludes "We have proposed a system for electronic transactions without relying on trust". In order to prevent the trust and double-spending problem, the white paper proposes a fully transparent and peer-to-peer transaction network using a byzantine fault tolerant consensus algorithm. The bitcoin blockchain in essence is a shared ledger visible to all participants but only a consensus majority can edit it. The technical protocol that records transactions in blocks connects those blocks into a chain coined the term "blockchain".

Blockchain technology does, in our regard, provide a solution to the above-identified security and transparency problems that Internet based community currencies are subject to. In reference to table 1, bitcoin as a cryptocurrency is argued to be a past value type of money. Put differently, the value and issuance of bitcoin is derived from the energy spent in the past by the network of computers that constitute the bitcoin transaction network (Bendell and Slater 2015). At the same time, one can argue that bitcoin also encompasses aspects of the present value type of money. This is due to the fact that it also has intrinsic value, as a bitcoin transaction requires the sender to provide a small amount of a bitcoin as a transaction fee to the underlying computer network. Regardless if it is representing past or present value, bitcoin properties as money are shared by all present cryptocurrencies. They are all more or less past or present value types of money. Hence, all of them are good for rewarding early participants of the system, as an investment or store of value, but they do not offer the superior medium of exchange properties like the future value type of money does. Today blockchain-based virtually min(t)ed crypto currencies are hard to handle as an average user has to: Create an account at an exchange platform, transfer fiat money from a bank account to the exchange, buy tokens, take into account their volatility, before eventually using them to make any payments.

In summary, as current cryptocurrencies have difficulties to represent or host past or present value type of money, the potential that blockchain technology can provide in terms of security (regarding centralisation) and transparency to community currencies is not yet leveraged. In their current form, cryptocurrencies simply do not fit the vision of community currencies to operate as a fair and easy to use alternative to incumbent fiat money.

2.3. Objectives for the Prototype

To summarize the previous analysis, the objective for the prototype is to combine the best-practices for community currencies design and blockchain technology to create a secure and interoperable medium of exchange. Hence, the identified objectives are:

- Create a future value type of community currency, which allows the participants to exercise governance rules while offering accountability by being based on a bilateral dispersive money creation process.
- Utilize the properties of blockchain technology in order to provide a freely accessible medium of exchange, which can be used for community exchange in a secure, transparent and cross-community interoperable manner.

3. A GENERIC ARCHITECTURE FOR COMMUNITY CURRENCIES

3.1. Methodological Approach

In order to describe the prototype along scientific guidelines and ensure scientific rigor, we choose design science research as an appropriate approach. A general introduction to design science research in information systems is provided by Hevner et al. (2004). We follow a prescriptive set of guidelines for design science research which, according to Peffers (2007), comprises the following methodological steps:

1. Problem identification and motivation
2. Define the objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

The first two steps are contained in sections 1 and 2 respectively. The objectives to be addressed by the prototype (artifact) are made explicit in section 2.3. Hence, the subsequent sections describe a prototype that addresses the problems of current virtual community currency systems and corresponding exchange platforms. Due to the still early stage of the project, we choose to evaluate the prototype by logical reasoning. Put differently, we describe how the specification of the Trustlines Network is able to address the identified objectives. An extensive analysis of acceptance, usage and usefulness based on qualitative and quantitative metrics is about to follow in a later stage of the project. Negotiations with smaller communities that already use a complementary currency are currently taking place and will result in a real-world case study. Communication is achieved by this research article, i.e. we follow a structured and established process and describe the design specifications of the artifact in sufficient detail to evaluate the efficacy of the artifact with respect to the predefined objectives. At least in terms of face value validity. We start with an overall description of the prototype's features in the next section. Simultaneously, we establish a common terminology that is used throughout the paper. It is worth noting that major parts of the next sections will also be made available in a whitepaper on the website "trustlines.network".

3.2. Trustlines Network Concept Overview

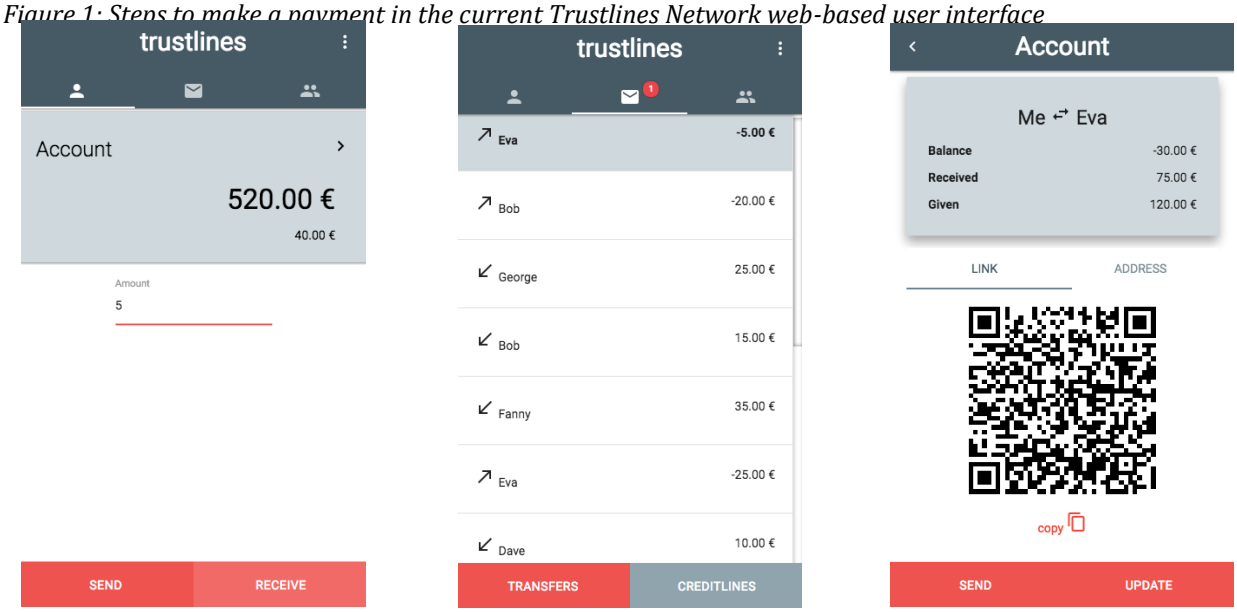
The proposed prototype is named Trustlines Network. It is a decentralised, permissionless, open source blockchain protocol to host multiple currency networks. In these currency networks, money is represented as bilateral obligation issued in form of "credit lines" between people that trust each other. The proposed Trustlines prototype allows everyone with a smartphone to send payments to other participants - even to those that they don't know or trust. In that way, the system resembles the decentralised issuance of IOU's taking place in Local Exchange Systems (LETS). Where LETS are built on the mutual-credit principle, Trustlines is an interconnected network of multiple LETS. People can only be liable up to the amount they decided to entrust in direct connections to

other people. The enforceability of IOU claims is therefore informal and up to the two participants that set up a Trustline between each other. The next two sections describe the system from user and a technical perspective respectively. We start with the user perspective to provide a general understanding of the purpose and functionality.

3.3. User Interaction with the System

Users join the network by downloading a mobile app, which automatically creates a wallet for the user. Next, users select a currency network they want to join and create a Trustline with at least one friend in order to be connected to the network of Trustlines. Note that users neither have to register with some organisation nor do they have to deposit money, or link a credit card or bank account. Furthermore, no upfront ETH (the innate currency of Ethereum - the underlying Blockchain infrastructure) is required and users can start spending based on the credit line given by a friend.

Figure 1: Steps to make a payment in the current Trustlines Network web-based user interface



Adding friends on the Trustlines Network is very similar to other applications but with higher privacy standards. Friends can be added in the real world by one phone scanning a QR code displayed on the other phone. This is also possible by receiving an "add me" link, or by pasting the address of the friends account. Users can furthermore see who of their friends are using the Trustlines Network. Friends (contacts) already participating in the network can be automatically discovered. When adding a friend, a Trustline is created and both explicitly agree to the mechanics of the system by giving each other a credit line with an individually chosen limit.

Once a Trustline is set up, users can start sending payments to anyone in the network. For making payments, a target address and amount is needed. Addresses are either available in the apps contact list, received by text message or by scanning QR codes (which can also include the value). Before sending payments, a mandatory fee is displayed. Both users get a notification once the transfer is initially confirmed and once it is finalized. Users are shown their (total) available, next to their (total) balance on the main screen of the app. A positive balance is the total amount their friends owe them, while a negative balance is the total amount they owe to their friends. The available amount is the sum of all their credit line limits plus their balance. Users can also inspect the balances with their friends individually but this is of limited information, because these are changed with every transfer that is routed through their account (i.e. these balances change without user interaction). Note, that the overall balance is not changed when routing transfers through an account, except for tiny amounts, which represent interest or earned fees.

3.4. Currency Networks and Trustlines Payments

The system supports payments denominated in customized currencies, denominated according to the preferences of the users. There is a distinct Trustlines currency network for each currency. Users can participate in multiple networks. Users can send cross-currency payments to users, which only have Trustlines in other currencies.

To initiate a payment either the received payment instructions contain the target address, amount and currency or the user enters them manually. Users are then presented the best conversion rate offer and fee and the total amount the payment would cost them, before confirming the transfer. Adding or withdrawing funds to the Trustlines Network can be done by interacting in the real world with any other participant in the network. It is basically implemented as a Trustlines payment for cash received. If a user handles cash to a receiving user, the receiver sends a payment to the initiating user, thus crediting him the amount in the network. Withdrawing works the other way around. Note, that the parties involved in the transaction don't need to be friends. Converting cash to Trustline money is also the method to pay back debt in the Trustline Network, which might be necessary if a user, on average, spent more than he received. Withdrawing cash is the method to reduce balance surpluses given in the Trustline Network (i.e., if a user on average receives more than he spends). Just like with commercial money based bank accounts, adding or withdrawing cash is possible but not necessary for the system to operate and be useful.

Credit relationships exist between trusted friends/parties only. The system guarantees that payments which are routed through untrusted accounts are unaffected if one of these accounts defaults. So, a payment from Alice - Bob - Charlie is secure for Charlie even if Alice defaults shortly after. This is because Charlie gets the amount credited from Bob. Bob might suffer a loss, which is "okay", as he trusted Alice. Thus, the default of a payment initiator doesn't affect the receiver. Friends paying back the credit are not guaranteed and are not legally enforceable within the Trustlines Network. All IOUs on the network are notarized on the Ethereum blockchain. Therefore, there is a tamper proof record of all agreements and their balances. In case of a friend not being able to pay back the obligation, there's also always the option to forgive debt or settle in other ways than initially anticipated; a Trustline payment from the creditor to the debtor would reflect this. Users can reduce the set credit lines limits, e.g. if they want to reduce their risk exposure to a friend. If their friend has sufficient credit in other Trustlines - indebtedness between the friends can immediately be reduced to the newly set credit line limit. Users can update the credit line limits at any time unless they agreed on more restrictive terms. If users want to quit using the Trustline Network, they can issue a request to do so by appointing a limited number of friends with whom they want to have their consolidated debt or credit in the network. The result of this action is a log, which attests the balance with a friend after leaving the network.

Each Trustline can have optional interest rates for both credit lines. If there is a non-zero balance in a Trustline, every transfer and balance update will reflect for the applied interest since the last update. Users will earn interest if their overall balance is positive and have to pay otherwise. Users can update the interest rates of the given Trustlines at any time unless they agreed on more restrictive terms. Users are required to pay fees for initiated transfers, which are composed of a base fee and optionally a percentage of the transferred value. In order to send transfers to the network, users also need ETH to pay for parts the gas fee. Acquiring the necessary ETH is done in the background by the app and payed for using Trustline Money.

Users get rewards for transfers that are facilitated using their Trustlines. The more transfer capacity they provide through their Trustlines, the more value can be transferred through them and the more rewards they may collect. Note: Users don't need to know about Ethereum or acquire tokens at an exchange.

3.5. Exchanging Currencies

There is constant demand for ETH in the system, as it is needed to pay for the operation of the system as well as to facilitate cross-currency transfers or bridge gaps between unconnected partitions in a currency network.

Any user can be an ETH Gateway by selling ETH for Trustline money in the system. This works by sending an offer to an on-chain ETH/Trustline Money exchange. ETH Gateways can earn money on the spread between their ETH price and the market price. They can also receive ETH when being used in a cross-currency transfer and credit

money in the Trustline network in exchange. The option to sell or buy ETH is on an exchange labelled as an advanced feature in the mobile app and regular users don't have to bother with it. The mobile app will automatically buy ETH necessary to pay for transaction fees. This is done whenever necessary and requires limited user interaction. Regular users can also buy ETH for purposes beyond transaction fee payments.

When entering the exchange function of the mobile application, a user is presented with the cheapest available exchange rate, representing the cheapest of the paths to an exchange offer. They can send limit or market orders to the exchange. Users are free to send acquired ETH from the Trustlines wallet to any other external wallets like Mist, which allow them to use other decentralized applications (DApps). This is a very convenient way to buy ETH, as one does not have to setup an account with an exchange or meet in person with a seller. The option to buy ETH for Trustline Money makes it very easy to get access to the wider blockchain ecosystem, as it allows to interact with all kinds of services and tokens.

4. TECHNICAL IMPLEMENTATION

There are three main components that constitute the Trustlines Network system architecture.

1. The mobile application allows regular users to interact with the system using their smartphone.
2. Relay servers bridge between the mobile apps and the Ethereum Blockchain and offer services which are not feasible to be implemented on the platform or the mobile app. Most notably the path finding required for multi-hop transfers.
3. The platform is the foundation and implemented as a framework of smart contracts on the Ethereum blockchain.

The following assumes there is a network of Trustlines, which users set up using their smartphone. Then, if a user wants to do a payment, the following happens:

- A request to find a path on the network which has sufficient capacity is sent to a relay server by the user's smartphone application
- The relay server has a cached graph view of all Trustlines based on their state as seen on the blockchain. It uses a path finding algorithm to find the path with the lowest fees and returns it to the smartphone
- A transaction which encodes a call to the transfer function of a smart contract with the sender, value, path parameters is signed on the smartphone and sent to a relay server.
- The relay server forwards the transaction to the blockchain and listens for events emitted by it, which is then forwarded to the smartphone apps of the initiator and receiver of the transfer to inform the users of the status of the transaction.

4.1 Smartphone Application

Users interact with the system using a cross-platform mobile application that can be installed from an app store or directly. For payments the user interface resembles interaction patterns known from traditional mobile payment apps. URLs, QR codes or NFC are used to encode payment requests and recipient addresses. The app differs by the ability to manage Trustlines, i.e. add friends to a contact list and agree on the terms of the granted credit lines such as their limit and optionally an interest rate for imbalances. For contacts in the phonebook that are also using the Trustlines Network the establishment of Trustlines is automatically proposed. The application supports multiple user accounts and the participation in multiple currency networks. It also allows to initiate cross-currency payments and as a feature for advanced users, to trade ETH for Trustline Money. All transactions are signed locally on the mobile app, which also manages the private keys of the users. There is an option to appoint a set of friends that can cooperate to help registering a new controlling key in case it was lost.

4.2. Relay Servers

Relay Servers are a backend service implementing two main features:

1. Discovering a path between a payer and a payee in the social graph of Trustlines
2. Forwarding transactions to the Ethereum blockchain and sending smart contract events to the mobile app.

In theory the system could work without Relay Servers, but this would significantly decrease the user experience. The path finding algorithm depends on knowing all available Trustlines and a reconstructed graph of the network in memory. This would require the mobile app to sync with the state of the Trustline Network whenever it is activated, potentially loading many millions of Trustlines from the blockchain into the main memory. This introduces significant latency and would be a burden regarding bandwidth and RAM.

Users do not need to trust relay servers with their accounts, as transactions are signed locally on their device and validated by smart contracts on the blockchain. The worst case is, that relay servers fail to provide the cheapest path or give false information on the status of payments and accounts. This can be mitigated by setting up a network of independently operated and incentivised relay servers where the mobile app accesses a subset of them for every query and checks for consistency of their responses.

When relay servers forward a transaction to the blockchain they are paid by the app for their service using a probabilistic micropayments method. The relay server protocol is open and there is competition between relay server operators to provide the best service regarding quality and price. Clients do an internal accounting of the relay servers service quality and therefore develop preferences for the better services.

4.3. The Smart Contract Platform

The platform is at the core of the Trustlines Network. It implements a secure, tamper proof, decentralized, permissionless, environment to host currency networks. It has an open protocol and API which supports interoperability with other smart contract based services on the Ethereum platform. The platform can host multiple currency networks which can be denominated in real world fiat currencies (e.g. EUR), commodities (e.g. Gold) or user defined units (e.g. Beers). User defined currency networks can be customized in various ways, e.g. to restrict access, impose interest rate limits etc. All currency networks come with an on-chain exchange that allows trading their respective Trustline Money to and from ETH. Therefore all currencies networks on the platform are connected via ETH, which allows for cross-currency payments.

The following explains how the backend of the Trustlines Network is implemented on the Ethereum platform as a set of smart contracts.

4.3.1. Currency Network Token

The Currency Network Token contract is at the core of the system. One instance of it implements a currency by tracking user issued IOUs and the network thereof. The API is compatible with the ERC20 Token standard, which is an established interface in the Ethereum ecosystem. It hence established interoperability among all community currency system launched upon the platform and can make tokens interoperable. The contract records the name and symbol of a currency, all its users and their Trustlines. In its simplest version the Trustlines are modeled as "Accounts" which track the credit lines two parties agreed on and their current balance. In reality the data model is more complicated as also interest rates, last modification date and accumulated system fees need to be tracked. A design goal is, to fit all account data into 32 bytes, which is the word size of the EVM, so that we only have the gas cost of one sload/sstore per access to a Trustline. This is important, as transfers will usually use multiple Trustlines to facilitate a transfer. Going beyond the 32 bytes would therefore basically result in doubling the gas cost of a transfer. When transferring 5 tokens from Alice to Charlie via Bob, the contract's "transfer" method needs to be called by Alice with the value and the path, where the recipient is the last address in the provided path. As a result the accounts of Alice/Bob and Bob/Charlie are updated according to the call parameters and a Log is gener-

ated which records the payment event on the blockchain. The requirement to provide a path, when doing multi-hop transfers breaks the compatibility with regular ERC20 tokens. This can be worked around by a method to temporarily register the path for a payer-payee combination with the contract before calling the transfer method.

4.3.2. Currency Network Token Factory

This contract can be used to create and register a new currency network on the platform. It generates a new currency network instance with properties according to a supplied configuration.

4.3.3. Identity Proxy

In order to support recovery of lost accounts, we use a proxy contract, which is called with transactions signed by the users and forwards the actual transaction payload to its target, which authenticates the request based on the address of the calling proxy contract. This indirection is used to allow users to change the private key they are using to control the system. This is helpful in case a key is compromised. We are working on implementing a multisig scheme with uPort (an Ethereum based identity provision system) to allow appointing a set of friends or other trusted entities, that can cooperate to update the controlling key. The contract can also be used to implement spending limits and give other contracts access to the account of the user.

4.3.4. Probabilistic Relay Payment

Relay servers are paid for their service with ETH. It would be expensive (10k additional gas per tx) to have ETH micro transactions on the blockchain. Therefore, they are paid using a probabilistic payments scheme. Basically, every payment is set up in a way, that it can only be redeemed with a very low probability P on the blockchain, which would then result in a redeemable amount, which is 1/P of the actual fee per request. This is similar to a lottery, where one has only a tiny chance to win but can win a multiple of the price of the ticket. Users need to put a certain ETH amount into escrow with this contract. When paying a Relay Server (which they do for every tx they send), they sign a message with the recipient address, the eligible amount and a threshold value which encodes the probability that the relay can redeem the specified amount in N blocks from now if the hash of a block in the future is lower than the threshold.

4.3.5. ETH Exchange

This contract allows exchanging ETH for credit in the Trustline Network. Users who want to sell ETH can register an offer with the contract, which indicates the number of Trustline currency tokens they want to receive in return for the ETH deposited with the offer. There is one such contract instance for every currency network. Users who have a path with sufficient capacity to the seller can pick the offer, pay with Trustline Money and receive ETH in their account. The same contract can be used to offer to credit Trustline Money for ETH.

4.3.6 Fees and automatic acquisition of ETH

There are multiple fees, including a constant relay server fee, the mandatory Ethereum (gas) transaction fee and incentivising fees for reducing imbalances and to reward transfer capacity by maintaining Trustlines. For users only a single fee is though quoted before confirming a transaction. Fees are payable with Trustline Money, except for the gas and relay fees which are payable in ETH. Note that it was chosen to use Trustline Money for fees whenever possible to avoid unnecessary dependence on ETH supply in the system.

As the system is based on the Ethereum blockchain it is necessary to pay for transactions in its native currency ETH. Relay servers also need to be paid in ETH. The Trustline system aims to hide this complexity from users. The mobile application will automatically buy and maintain a certain amount of ETH tokens for the user. Therefore, when necessary it trades ETH for Trustline Money using the ETH Exchange contract.

4.4. Cross-Currency transfers and bridging gaps in the network

ETH can also be used as a bridge if there is a gap in the graph, i.e. when no path with sufficient transfer capacity can be found between two users. It works by finding a path from the sender to a seller of ETH (which has an offer at the exchange) and finding a path from someone trading ETH for Trustline Money to the recipient. Such a trans-

fer is split into two transfers and two ETH exchange interactions but can be executed atomically in one transaction. These kinds of transfers will be more expensive though, as the gas fee is higher and also because there will be a spread between bids/asks on the ETH exchanges.

4.5. Interoperability and scaling the system

The core value of Ethereum is Synergy. Meaning that smart contracts of the Trustlines network are, in general, able to interact with any other smart contract that exists in the Ethereum blockchain. In particular, any community currency issued with the Trustlines network can technically interact with every other community currency token that is either launched by Trustlines or adheres to the implemented standardized token interface used in Ethereum blockchain projects (namely the ERC 20 Token Interface).

Further, extensibility is provided by "Governance Hooks", which allow delegating the exclusive right to update credit lines and interest rates to smart contracts. As the parties of a Trustline can also be smart contracts, this allows to model more sophisticated logic and enables applications like Trustline-based loans or implementation of further governance mechanisms. Supporting 100 Million active users on the system would exceed the transaction throughput of the current Ethereum platform by a factor of ~100. Currency networks and clustering users by connectivity are obvious partitioning/sharding options enabling the system to handle the communities separately from a technical point of view while interoperability is maintained at the cross-community exchange level.

5. EVALUATION AND DISCUSSION

The evaluation of an artifact can be relative to another solution or in absolute terms, i.e. using the artifact vs. not using the artifact. In table 2 we evaluate the artifact in comparison to existing solutions for cryptocurrencies, community currencies and conventional payment systems.

Table 2: Comparison of money transfer systems.

	Trustlines	Bitcoin	Ripple	M-Pesa	LETS	Hawala	Paypal, etc.
Decentralized	Yes	Yes	limited	No	Yes	Yes	No
Permissionless	Yes	Yes	No	No	No	Yes	No
No bank account required	Yes	limited	No	Yes	Yes	Yes	No
Global Payments	Yes	Yes	Yes	limited	No	Yes	Yes
Mobile app	Yes	Yes	No	Yes	limited	No	Yes
User issued money	Yes	No	No	No	Yes	No	No
Open Platform (Turing Complete Smart Contracts)	Yes	No	No	No	No	No	No

Given the previous description of the Trustlines Network prototype, we identify three crucial advantages in comparison to other (cryptocurrency-based) community currencies: 1) Ease of adoption and joining the network 2) open smart-contract platform API and 3) enabling user issued (dispersive) money that can be used to make both intra- and inter-community payments. In regard to these three advantages, we consider the prototype to fulfil the design objectives. It combines the desired properties of credit based future type of money with the security, customizability and interoperability offered by blockchain technology.

When compared to traditional and current blockchain based payment services, accessibility and ease of adoption is the outstanding property of the system. A user only has to download the mobile application and create a Trustline with a friend in order to be able to send and receive payments within the network. In regard to the desired property of being an accessible medium of exchange, the app is designed to hide all the complexity of blockchain technology from regular users. In this way, users have the benefit of using blockchain powered mutual-credit based money, without having to deal with innate Blockchain currencies (e.g. Bitcoin or ETH), weird hex strings representing account IDs or to understand the underlying technology - not even at an abstract level. Furthermore, users do not have to register with any exchange to buy crypto tokens upfront, nor do they need to possess any national fiat money in the first place. This can be considered a huge leap forward with respect to the current access barriers of blockchain technology.

Finally, as the Trustlines Network is an open platform that can be extended by additional smart contracts on the Ethereum blockchain, it offers interoperability and can leverage synergetic effects with other Ethereum based decentralized applications. This implies, that the open-source nature of the Trustlines Network enables interested 3rd party developers to use 'governance hooks' in order to implement applications and governance modules on top of the protocol.

There are, of course, limitations to the capabilities of the proposed system that are not yet solved. First, it has a complex fee structure, which is essential to provide incentives for the operators of the decentralized Blockchain infrastructure. The nodes that are operating the Blockchain infrastructure require compensation for their computational resources, which are needed to keep the system running. Second, an evaluation of the robustness of the system regarding the social dynamics involved in such mutual trust based systems is not addressed in this work. We leave these questions open for future research. Third, the technical scalability of blockchains is limited. Potential sharding options for technically partitioning communities for scalability have therefore been mentioned. However, actual implementation of such partitioning/sharding is an ongoing challenge of the Ethereum ecosystem.

Nonetheless, running the system in a local community by setting up a local Ethereum blockchain is a feasible approach with the current state of the application.

6. CONCLUSIONS AND IMPLICATIONS

The objective of the paper was to propose a solution to the weaknesses of existing, centralised community currency software, in order to strengthen the use of mutual-credit based virtual community currencies as a medium of exchange. An additional objective was to incorporate the best practice of mutual-credit community currency design that has been identified in previous literature. To address these objectives, we presented the Trustlines Network system architecture that comprises a mobile application, a network of relay servers and a platform consisting of smart-contracts implemented on the Ethereum blockchain. In combination, these elements assemble an infrastructure for a decentralised, permissionless, open source blockchain protocol, which can host multiple community currency networks that are easily accessible via a mobile app. In these currency networks, money is represented as bilateral obligations issued in form of "credit lines" between people that trust each other. The proposed infrastructure demonstrates how to combine the future type of mutual-credit based money with the transparency, security and interoperability properties offered by blockchain technology. In direct comparison to other (cryptocurrency-based) community currency systems, we identified that ease of adoption, openness of the smart-contract platform and user-issued money for cross-community payments are significant improvements relative to the existing (community currency) systems. From a practical perspective, we provide a technologically feasible solution that can be used in real-world communities and serve as blueprint for future ways of exchange in communities. From a theoretical perspective, we contribute a technical feasibility study that can provide input for future theoretical models regarding social interactions and trust dynamics in mutual-credit system studies.

For future research, we plan to analyse how the most common and well-tested community governance mechanisms can be implemented in form of smart-contract “Governance Hooks”. In connection to this, we are eager to use quantitative approaches to better understand the resilience and efficiency of the Trustlines Network design. Finally, there is a need for qualitative or mixed-method oriented studies to better understand the acceptance of the system as well as implications of connecting financial activities with interpersonal social trust relationships.

REFERENCES

Bendell, J., Slater, M., & Ruddick, W. (2015). Re-imagining Money to Broaden the Future of Development Finance What Kenyan Community Currencies Reveal is Possible for Financing Development. Retrieved from http://www.unrisd.org/80256B3C005BCCF9/(httpAuxPages)/99FCA15CAF8E24F4C1257E7E00501101/$file/Bendell et al.pdf

Fugger, R. (2004). Money as IOUs in social trust networks & a proposal for a decentralized currency network protocol. Hypertext Document. Available Electronically at Http:// …. Retrieved from http://www.practicalmetaphors.com/decentralizedcurrency_orig.pdf

Graeber, D. (2011). Debt : the first 5,000 years. Brooklyn, NY: Melville House.

Hees, H., Friis, G., & Naerland, K. (2017). Trustlines Network. Retrieved from http://trustlines.network/whitepaper_v03.pdf

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1. Design Science in IS Research MIS Quarterly, 28(1), 75–105. Retrieved from http://wise.vub.ac.be/thesis_info/design_science.pdf

Huber, L., & Martignoni, J. (2013). Interchange By a Regional Hub-Solution. International Journal of Community Currency Research, 17, 1–7. http://doi.org/10.15133/J.IJCCR.2013.001

Kenney, Margrit; Lietaer, Bernard; Rogers, J. (2012). People Money : The Promise of Regional Currencies. Triarchy Press, (January). Retrieved from www.triarchypress.com

Kichiji, N., & Nishibe, M. (2012). A COMPARISON IN TRANSACTION EFFICIENCY BETWEEN DISPERSIVE AND CONCENTRATED MONEY CREATION. International Journal of Community Currency Research, 16, 49–57. Retrieved from https://ijccr.files.wordpress.com/2012/07/ijccr-2012-kichiji-nishibe1.pdf

Lietaer, B. (1997). Internet Currencies for Virtual Communities. Retrieved April 14, 2017, from http://www.transaction.net/money/internet/

Lietaer, B. (2014). The Future Of Money: Creating New Wealth, Work and a Wiser World. Igarss 2014, (1), 1–5. http://doi.org/10.1007/s13398-014-0173-7.2

Lietaer, B., Ulanowicz, R. E., Goerner, S. J., & Mclaren, N. (2010). Is Our Monetary Structure a Systemic Cause for Financial Instability? Evidence and Remedies from Nature. Journal of Futures Studies Special Issue on the Financial Crisis. Retrieved from http://www.lietaer.com/images/Journal_Future_Studies_final.pdf

Martignoni, J. (2015). Cooperation and Intertrade between Community Currencies: From fundamentals to rule-making and clearing systems. http://doi.org/10.15133/J.IJCCR.2015.014

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Www.Bitcoin.Org, 9. http://doi.org/10.1007/s10838-008-9062-0

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45–77. http://doi.org/10.2753/MIS0742-1222240302

People Powered Money: everything you need to know to set up a community currency | Community Currencies in Action. (2015). Retrieved April 14, 2017, from http://communitycurrenciesinaction.eu/peoplepoweredmoney/

Schraven, J. (2000). The Economics of Local Exchange and Trading Systems: a Theoretical Perspective *. IJCCR Vol Schraven International Journal of Community Currency Research, 4(4). Retrieved from https://ijccr.files.wordpress.com/2012/05/ijccr-vol-4-2000-5-schraven.pdf

Schraven, J. (2001). Mutual Credit Systems and the Commons Problem: Why Community Currency Systems such as LETS Need Not Collapse Under Opportunistic Behaviour*. IJCCR Vol Schraven International Journal of Community Currency Research, 5(5). Retrieved from https://ijccr.files.wordpress.com/2012/05/ijccr-vol-5-2001-4-schraven.pdf

Slater, M. (2015). for Financing Development Escaping Delusions of Development Finance Workshop contribution prepared for Social and Solidarity Finance : Tensions , Opportunities and Transformative Potential Organized in collaboration with the Friedrich-Ebert-Stiftung, (May), 11–12. Retrieved from http://www.unrisd.org/ssfworkshop-bendell

Slater, M., Jenkin, T., Belmonte, S., Hassan, D., Haugen, B., Demeulenaere, S., … Hausel, K. (2016). THE CREDIT COMMONS: A MONEY FOR THE SOLIDARITY ECONOMY. Retrieved from http://creditcommons.net/credit-commons-wp-screen.pdf

Stodder, J. (2009). Complementary Credit Networks and Macro-Economic Stability: Switzerland's Wirtschaftsring 1. Journal of Economic Behavior & Organization, 72, 79–95. Retrieved from http://www.ewp.rpi.edu/hartford/~stoddj/BE/WIR_Update.pdf

Ulanowicz, R. E., Goerner, S. J., Lietaer, B., & Gomez, R. (2009). Quantifying sustainability: Resilience, efficiency and the return of information theory. Ecological Complexity, 6(1), 27–36. http://doi.org/10.1016/j.ecocom.2008.10.005

Wray, L. R. (2007). Endogenous Money: Structuralist and Horizontalist. Retrieved from http://www.levy.org

Zarlenga, S. (2002). The lost science of money : the mythology of money, the story of power. American Monetary Institute. Retrieved from http://www.monetary.org/lostscienceofmoney.html