

COLU LOCAL NETWORK

Whitepaper



CLN



CONTENTS

1. INTRODUCTION	2
2. GUIDING PRINCIPLES FOR THE CLN NETWORK AND PROPOSED ARCHITECTURE	5
2.1. THE BUSINESS MODEL AND STAKEHOLDERS IN THE CLN NETWORK	6
2.2. NETWORK CAPABILITIES FOR ISSUERS AND GATEWAYS	9
2.3 PROPOSED ARCHITECTURE OF THE CLN NETWORK	9
2.3.1. Products and services layer	10
2.3.2. Clients Layer	11
3. THE ROLE AND DESIGN OF COMMUNITY CURRENCIES	12
3.1 THE ISSUANCE OF COMMUNITY CURRENCIES	13
3.2 THE PROVISION OF LIQUIDITY FOR COMMUNITY CURRENCIES	14
3.3 THE USE OF COMMUNITY CURRENCIES AS REWARDS FOR ECONOMIC ACTIVITY	16
4. SUMMARY	17
4.1 ACKNOWLEDGMENTS	18
5. REFERENCES	19
APPENDIX A—MATHEMATICAL EQUATION FOR THE MECHANICAL MARKET-MAKING CONTRACT	21
APPENDIX B—MATHEMATICAL FORMULATION OF THE ISSUANCE OF A COMMUNITY CURRENCY AND THE LOCK-UP OF INITIAL RESERVES	24
The process	24
Issuance with issuer's own funds	24
Issuance with investors' funds	24



1. INTRODUCTION

The Internet is making its way into every part of our lives. With the speed of adoption increasing, technical barriers are being lowered and we find our physical and digital lives beginning to integrate, creating a huge impact, especially on millennials. They are the first digital-native generation to be born into this world and the largest generation in history—significantly larger than the baby-boomer generation, and are expected to be in control of 24 trillion dollars of the world's wealth by 2020. They are more likely to live in cities, they own fewer cars, and they choose their brands based on values like ethical sourcing, social justice, and environmental effects. They are looking for meaning, and often find it in making a positive impact on the community around them, thus creating a demand for financial community ties.

Technology is dramatically changing the way millennials make payments and consume other financial services. As physical cash is being replaced by digital means, from cards to mobile, they come to expect payments to be quick, safe, cool to use, and available 24/7. This creates pressure on merchants to broaden the means of payments they accept, in an effort to catch up with user demand. This pressure is especially burdensome for smaller merchants in today's environment as they often pay the highest fees for payment processing, making for an uneven playing field for local initiatives.

Moreover, as a consequence of accelerating globalization, the diminishing frictions in cross-border commerce have incentivized corporate rent extraction through cost-externalization and the outsourcing of production. Encouraged by the continuation of open policies on multilateral trade, global supply chains have penetrated domestic markets, resulting in the incremental centralization of capital flows toward multinational organizations.^[1] While the free movement of goods is imperative to open markets, SMEs (small to medium size enterprises) get the short end of the stick, being unable to compete in their native markets. In particular, small businesses with less than 10 employees make up over 93 percent of all enterprises in the EU and account for around two-thirds of employment.^[2] In the US, small businesses account for 99.7 percent of firms with paid employees, and annually contribute almost 40 percent of US private, non-farm output.^[3] Yet, these small businesses often face difficulties accessing capital.

A comparison study published by the OECD shows that the share of SME loans in total business loans in 2014 was 22.5% in the UK, 21.2% in the US and France, and 14.2% in Canada.^[4]

Community financial service providers typically provide services to SMEs and consumers based on “relationship banking”; however, they encounter tough competition from large national and multinational financial institutions. Credit unions and community banks play an important role in the US by lending to small businesses and providing access to payments services for a large percentage of the population. However, their share in total deposits and loans has been decreasing significantly over the years.^[5] Credit unions are typically another type of community financial service provider. A study in Canada shows that they retain a higher share of net income to support future growth and investment in creating jobs, that they provide loans through periods where availability of credit is low, and that they lead in SME business lending.

The idea of a community currency as a secondary medium of exchange, store of value, and unit of account has also been around for a while. Community currencies have attracted attention from academics and policy makers alike, due to their unique ability to produce and retain wealth within communities.^[6] These currencies have the potential to increase overall profitability for local stakeholders and to facilitate countercyclical growth cycles and increased social welfare.^[7] Several projects have attempted to establish local payment systems; however, due to lack of sufficient infrastructure these initiatives have failed to provide a secure, liquid, and scalable environment for financial transactions.^[8]

Technological advancements, notably the emergence of blockchain technology, lower the barriers to offering payment processing solutions and establishing local payments systems. While the macroeconomic consequences of issuing digital peer-to-peer currencies remain hypothetical, regulators are exploring opportunities in distributed financial solutions.^[9] As the notion of digital currency manifests itself in private and regulatory institutions, the efficiency, resilience, and accessibility of disintermediated digital payment infrastructure is gaining momentum with a broader audience. The CLN is looking to build an ecosystem that will combine the two changes discussed above—technological and social—by creating a network that supports the evolution of local payment systems, each of which provides incentives to its local stakeholders, while sharing tools and services provided over the entire network.

A fresh approach to community “banking” using blockchain technology, where transactions are verified P2P and intermediaries are removed, shows the promising potential to generate value by increasing competition on the price, quality, and variety of services relative to existing means of payment and other relevant services.

Colu is firmly rooted in the open-source blockchain developer community as a leading member of the [ColoredCoins](#) project, and is investing additional resources in open-source code with the latest release of [Bankbox](#). This commitment is also reflected in the initial release of the Colu Local Wallet.



2. GUIDING PRINCIPLES FOR THE CLN NETWORK AND PROPOSED ARCHITECTURE

The current state of payment systems globally, even in well-developed markets such as the UK and the US, is such that the gap between end-user needs, both of consumers and of businesses, and what is being delivered by the current payments infrastructure is growing and creating significant detriment for users, who are demanding greater control, greater assurance, enhanced data, and reduced financial crime.^[10] A recent report by the Payments Strategy Forum in the UK, identifies key requirements that current legacy systems and the entire payment infrastructure must meet:^[11]

- The ability to respond to current and future end-user needs
- Improving trust in the safety and certainty of payments
- Simplifying access to data and to systems in order to promote competition
- A new architecture for the payment ecosystem

In thinking of a new architecture for the payment ecosystem, one that can support us in achieving the desired goals given today's technologies, a recent dedicated report (the "NPA Report") details a proposed conceptual framework.^[12] The guidelines listed in the NPA report include:

- A single set of standards and rules with strong central governance
- End-to-end interoperability (including Application Programming Interfaces and common messaging standards)
- A collaborative infrastructure, allowing multiple providers of overlay services to compete in the market simultaneously
- The need to ensure our payment systems are secure and resilient with financial stability as a key foundation

Somewhat surprisingly, both regulators and traditional financial players on the one hand, and disruptive innovators in the blockchain arena on the other, agree on most of the above guidelines, with the notable exception of the form of governance.

The blockchain space is currently experimenting with different methods of community governance, but it is already clear that this technology offers new capabilities that are not possible in the financial system when it comes to transparency and the ability to coordinate a large group of organizations around an open and secure protocol.

The proposed CLN network implements an infrastructure that will facilitate the evolution of an ecosystem that adheres to many of the above principles:

- The choice to develop the CLN as an open-source project on a public blockchain implies there is a transparent set of standards and rules that ensures interoperability.
- Moreover, the existence of a vibrant, fast-growing community of developers facilitates the emergence of overlay services offered by third parties that will compete on the network. This is evident by the Ethereum transaction volume, which has already surpassed Bitcoin's transaction volume by allowing new functionality that has attracted thousands of companies to develop on top of it.
- A new network evolving over the blockchain is more prone to being dynamic and adaptive to future end-consumer needs than would be any result of a mere transformation of an old network built, as it is, on the foundation of legacy systems owned and operated by traditional players.
- The ability to bypass the network or fork it and make changes where it is proving to be inefficient or failing to create value for end consumers provides ongoing, healthy competitive pressure on the network. Such competitive pressure is often missing in many other proprietary payment schemes owned and operated by banks and credit card companies.

2.1. THE BUSINESS MODEL AND STAKEHOLDERS IN THE CLN NETWORK

The key business goals that the CLN network is designed to support are:

- Providing economic incentives that will facilitate the development and provision of new services to the network
- Providing services in an accessible manner, which will support broad adoption of the technology ("bringing the use of crypto currencies to the masses")
- Using economic incentives as a growth engine by facilitating the introduction of community currencies [See Chapter 3 for details]

The importance of designing the network in such a way that it will organically provide adequate incentives to the various participants in order to facilitate broad adoption is also reflected in a recent report by the US Faster Payments Task Force concerning the design

of a faster payments system in the US.^[13] The report discusses the need to provide incentives to consumers and merchants to encourage them to learn, access, and use the system, and to provide solution operators and service providers with incentives to develop and deliver solutions and participate in an ecosystem that enables interoperability among competing solutions. Moreover, the report acknowledges the importance of enabling financial service providers of all sizes to participate and deliver solutions “by fostering competitive fairness, continued innovation, and flexibility to take advantage of emerging technologies.” Therefore, the network should be structured to provide incentives to entities providing those financial services that address everyday needs, entities often referred to as gateways.

The CLN network proposes a framework via which to provide incentives using blockchain technology. Next, we discuss the multiple stakeholders that could participate in the CLN network and the fundamental role they each play in establishing, developing for, and maintaining the network, on the one hand, and in using the services provided, on the other. The incentives to the various players would be provided through the circulation of the network’s native token (CLN) and community currencies in the form of rewards or fees.

Role	Description
Financial Gateways	<p>A financial gateway accepts fiat or crypto deposits from users, and acts as a custodian for user funds flowing in and out of the network. A gateway can be any institution, including financial institution, as long as it provides services that accompany the custody of consumers funds, such as KYC and other regulatory requirements. Gateways act as entry and exit points for fiat currencies. They are in a position to play a vital role in the network by providing transaction verification and settlement across the network, without a central operator and without reliance on a single gateway. Gateways are compensated for their services in CLN fees.</p>
Community Currency Issuers	<p>A community currency issuer uses the tools provided by the CLN network to issue a community currency for its community and provide liquidity for it. This role can be taken by merchant networks, local businesses, consumer clubs, and other entities that have a community of users for which they wish to facilitate consumption, payments, lending, crowdfunding, or credit.</p>
Developers and Service Providers	<p>Developers and service providers will build tools and services on top of the CLN network, enhancing its capabilities. The network will support partnerships with products or other networks that complement the CLN network's services, such as credit providers, credit-scoring service providers, or integrators to legacy networks.</p>
Merchants	<p>Local merchants accept fiat payments for the services they provide. Merchants are rewarded in their community currency for transactions that take place at their point of sale.</p>
End-users	<p>Consumers pay at merchants' point of sale with digital fiat currency. They are rewarded in their community currency for pursuing this economic activity on the network.</p>

2.2. NETWORK CAPABILITIES FOR ISSUERS AND GATEWAYS

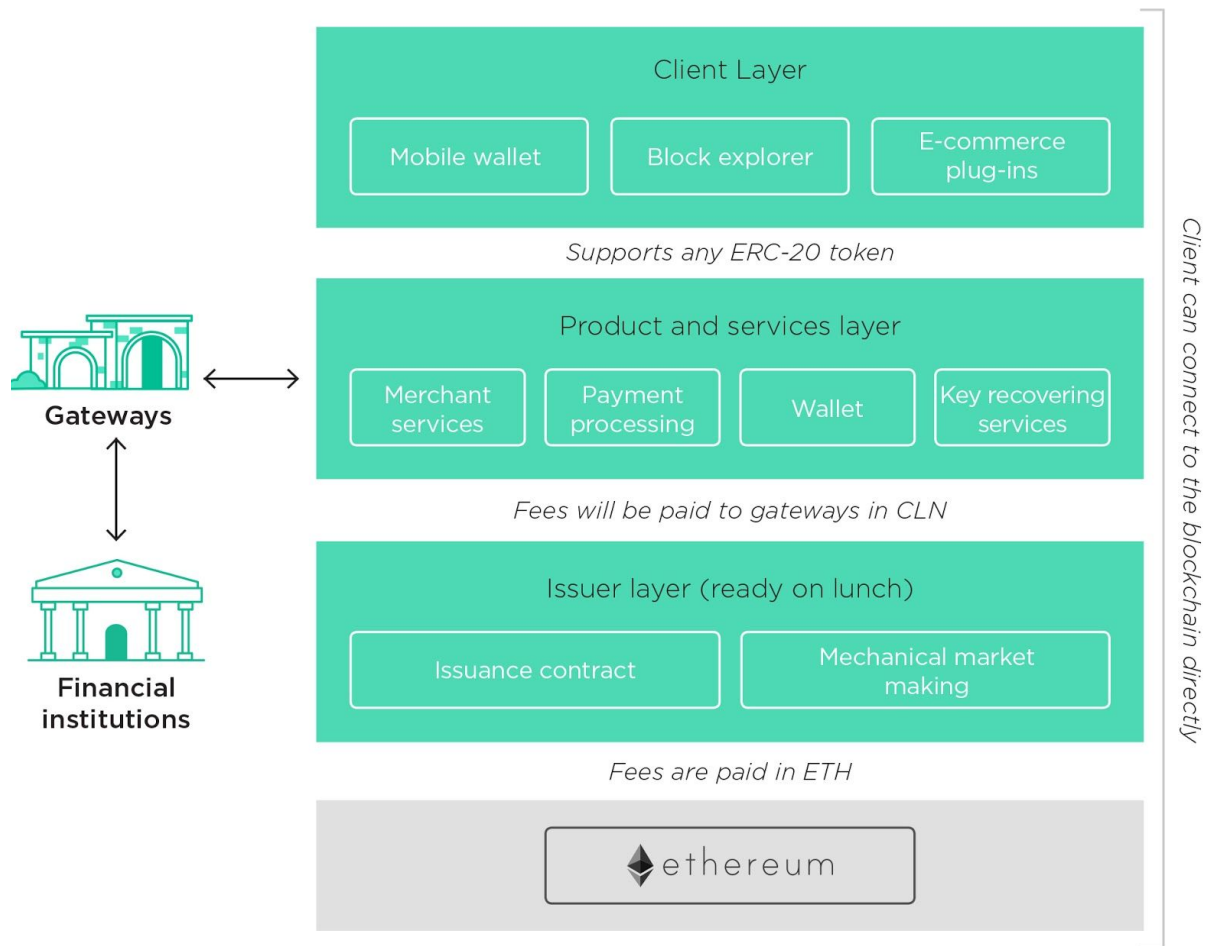
Issuers are entities that issue cryptocurrencies and provide them with liquidity. This role can be taken by merchant networks, local businesses, consumer clubs, and other entities that have a community of users for which they wish to facilitate consumption, payments, lending, crowdfunding, or credit. Issuers are at the heart of the network, and they are also in a position to act as gateways, although it is not mandatory. The network will launch with two key functionalities for issuers—the ability to issue community currencies using a template that is easy for developers to use and to provide a smooth exchange between community currencies, as well as ERC-20 tokens, via the CLN token. Both functionalities will be implemented using a set of smart contracts.

→The issuer tools are discussed in detail in Section 3.

2.3 PROPOSED ARCHITECTURE OF THE CLN NETWORK

A successful token is one with a distribution pattern that creates a system of incentives that support the business goals set for the token. For the CLN, it is creating a token that provides access to a network of local payments. The CLN token allows financial gateways, developers, and service providers to make payments, exchange between currencies, and provide additional services that address local communities' needs, thus providing an alternative to traditional financial institutions. Moreover, the goal of community currencies is to be a store of value for local communities, connecting consumers and businesses.

In the previous section we discussed the network capabilities for issuers and gateways. We refer to these capabilities as the issuer layer. Next, we discuss how the proposed architecture enables two layers of services that facilitate various stages in the payment process to be developed on top of the issuer layer.



2.3.1. Products and services layer

Products and services developed by anyone in the community could be integrated to the network as the network is an open-source public blockchain. The development of payment processing capabilities will provide merchants with an easy, bundled API/SDK to collect payments made using all types of payment means, including POS or e-commerce. Payment processing services will also support innovation in advanced payment types—for example, the introduction of recurring payments or of decentralized fiat exchange between gateways. Merchant services will handle merchant-related operations, such as the generation of invoices or fund withdrawals to the merchant's bank account. Any operation using SDK tools will pay the applicable gateway or service provider a fee in CLN.

The goal of using community currencies as rewards to facilitate payments in fiat between consumers and merchants is enabled by the network architecture, which allows for the development of the capability to issue crypto-fiat pegged to the corresponding fiat money by gateways holding fiat deposits.^[14]

2.3.2 Clients Layer

The clients layer interfaces with end-users—consumers and merchants. Tokens issued on the CLN network will be compatible with any Ethereum wallet. A key requirement of this layer is that it is independent of the CLN network. The CLN network will incentivize many potential players to build clients on top of the CLN, and it will be attractive thanks to the capabilities it will provide for processing fiat payments and cryptocurrencies. The freedom of clients to bypass the CLN network in order to process payments will drive the CLN network to focus on providing value-added services that reduce the technical barriers and increase usability of payments on the blockchain.



3. THE ROLE AND DESIGN OF COMMUNITY CURRENCIES

The CLN network lowers the barriers that stakeholders are facing when attempting to launch and maintain a new financial system in their community by providing them with tools and services that make it easier to launch a new digital payment infrastructure and design the growth engines that will make it flourish.

Community currencies that could be issued on the CLN network, may be used to offer incentives to end-users in the community (consumers and merchants) as well as developers and service providers. Thus community currencies could support an organic reward scheme for transactions being made within the community. The community currency will be issued by community gateways, with a transparent supply schedule and distribution rules.

The community currency will serve as an alternative medium of exchange and store of value, allowing users to transact with it freely with any Ethereum-compatible wallet. In order to create a mechanism that allows this functionality, the CLN network will provide two main network tools:

Issuance—Community currencies will be issued as ERC-20 tokens on Ethereum, leveraging Ethereum smart contract capabilities to set and enforce business rules like milestone-based access to funds for issuers. This will remove the current need for users to have blind trust in issuers. Any deviation from, or agreed change in, supply or governance is visible and verifiable by the public.

Liquidity provision—Providing liquidity for newly issued currencies requires major effort, and is addressed by the automatic market-making contract. In order for the community currency vision to be realised there is a need for liquidity, so that supply and demand forces will manifest in the price. This is achieved by leveraging smart contracts' capabilities and by using the CLN as a reserve currency.

The CLN network thus solves the fundamental chicken-and-egg problem, as engaged communities will be able to launch currencies regardless of their size, location, or transactional volume. In doing so, they will be able to benefit from having access to a decentralized group of stakeholders and service providers that take on a variety of roles in the value chain. The implication is an open-source and distributed financial framework, facilitating a safe and transparent payment system, accessible to all.

3.1 THE ISSUANCE OF COMMUNITY CURRENCIES

Community currencies will be issued by stakeholders within the community. These stakeholders will have a vested interest in the success of the community. Organizations like community banks, credit unions, merchants' associations and the like are potential issuers. We refer to these organizations as community issuers. All communities will be interconnected through the CLN.

Each community issuer can launch a new community currency for its local community. The issuance and allocation process will be transparent and publicly verifiable using an Ethereum smart contract. The currency will be an ERC-20 token that will be compliant with any Ethereum wallet.

As part of the issuance process the issuer locks a certain amount of CLN in an automatic market-making contract. The lock-in of CLNs releases a portion of community currency tokens to the issuer and establishes an "issuance price" for the community currency. That is, the amount of CLNs locked in by the issuer determines the initial value of the local community, measured by the product of the amount of circulating tokens and the issuance price. From this point onwards, this price evolves according to the flow of trades sent by anyone to the market making contract. If the issuer chooses not to lock any CLNs in the reserve of the market making contract, the issuance price is set to zero and all community currency tokens are locked in the contract initially, implying a starting value of zero to the community. Any appreciation in value from this point onwards will be as a result of demand for the community currency, paid for in CLNs.

In fact the issuer can allow investors to participate in the issuance process and receive community currency tokens in exchange for their investment in CLNs. See Appendix 2 for a detailed description of the process.

The two reserves established by the issuance process will provide a functionality of exchange, and thus liquidity, for community currencies, without having to list these currencies on centralized exchanges in the early stages, during which the potential value of doing so is relatively small.

The issuance process of a community currency could allow a milestone-based process for the allocation of CLN funds received and tokens issued. This supports an alignment of interests whereby additional community currency is released to a community issuer as the economic activity in the community—measured, for example, by the volume of transactions—increases, in order to cover their growing operational costs.

As the community currency network expands, new issuers and gateways will integrate into the network. Through the CLN network, financial institutions and companies will be able to offer value-added services, further stimulating local economic development and growth.

3.2 THE PROVISION OF LIQUIDITY FOR COMMUNITY CURRENCIES

Once a local payment system, supported by a community currency, is up and running, it will generate value by increasing competition on the price, quality, and variety of services relative to existing means of payment and other relevant services. However, this value will have to be built up over time, and be reflected in the value of the community currency. Consequently, consumers and merchants will likely value the option to exchange a community currency for the CLN network token or for other cryptocurrencies that can be used as means of payment or stores of value. Furthermore, participants may want to convert these tokens to fiat money.

However, it is unlikely that there will be sufficient liquidity for community currencies at their inception. Participants looking to exchange community currencies may not find a counterparty to trade with. On a typical exchange, the price of the asset is determined in response to the supply of and demand for the traded asset, and so the price reflects a willing exchange between a buyer and a seller. While there is no way to mimic the behavior of such an exchange mechanically, the CLN network will provide the community currency gateway with a tool that allows it to act as a market maker for the community currency, from the time of issuance. It will do so by executing exchange transactions automatically using a smart contract according to a preset formula. We will refer to this process as “mechanical market making”.

There are a number of important features that a liquidity model should satisfy. First, as argued above, it is important to realize that mechanical market making, predetermined and “set in stone” (or smart contract), cannot mimic the behavior of a real-time market exchange. In fact, hypothetically, were the community currencies to be traded on an exchange, there could be a gap between the exchange rate on the exchange and the one determined by the mechanical market-making contract. Therefore, it is important that the way that the contracts are implemented should not prevent the CLN and the community currencies from being traded on exchanges (other than through the mechanical market maker) or prevent other entities from providing an exchange service in parallel (i.e., function as competing market makers for community currencies). Moreover, the model should not create unfair conditions that would preclude this in practice. Consequently, we find it preferable that the mechanism should not have the authority or capability to alter the amount of community currency issued through the operation of liquidity provision. Otherwise, the ability of the mechanism to issue or destroy tokens in the process and affect the value of the currency could potentially harm the incentives to others to provide liquidity, and could potentially be used to manipulate the exchange rate. Moreover, the more available means there are for arbitrageurs to correct a mis-pricing caused by mechanical market making relative to the market perception, the smaller such possible gaps in pricing are likely to be.

Second, the model should mimic the basic behavior of a market, and therefore should possess the following characteristics:

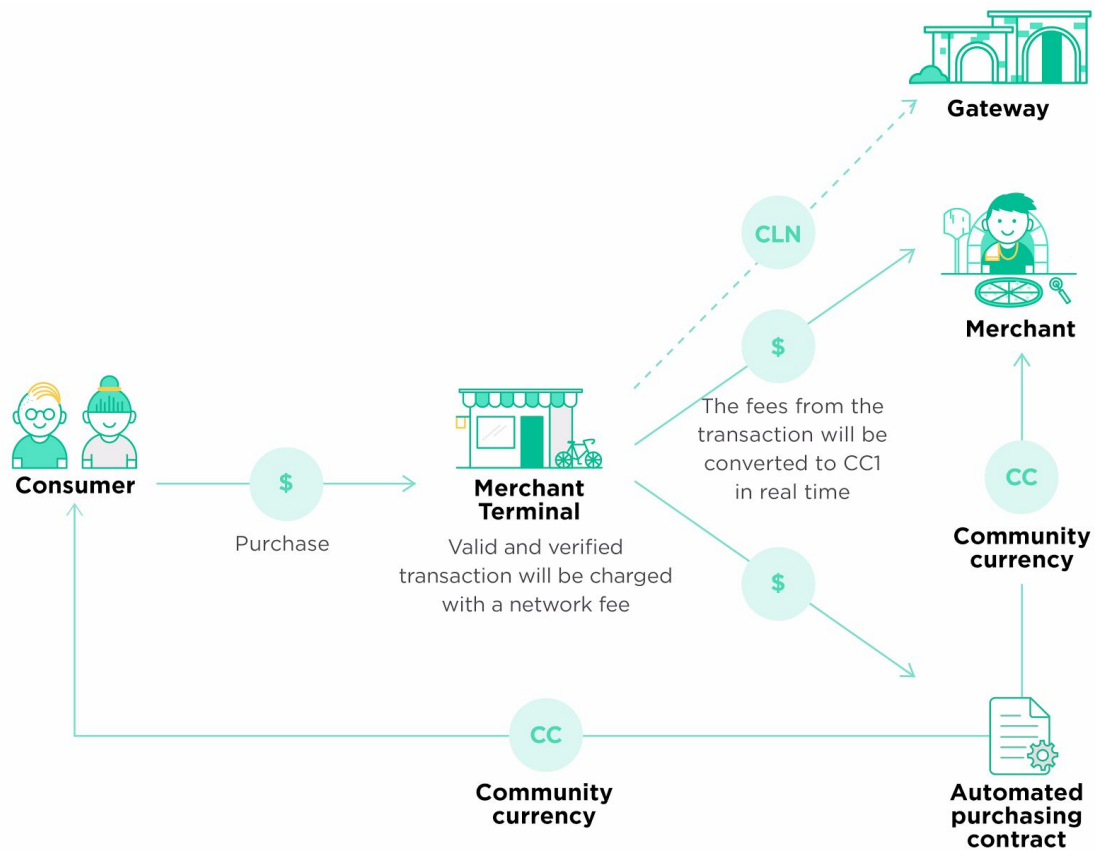
- When there is demand for a community currency its price (relative to the CLN) should increase, and vice versa when there is demand for CLN in exchange for the community currency.
- There should be sufficient liquidity to execute each trade. Our proposal is to maintain two reserves—one in CLN and another in the community currency—that are dedicated to serve as a counterparty for each exchange transaction.
- The price instrument should be used to implement the above characteristics, and in particular to ensure that the reserves do not exhaust themselves in the process, unless the entire money supply from one side is being added to the reserve (in which case it can exhaust the reserve on the other side).
- The price is only a function of the state of the two reserves and other fixed parameters (e.g., the amount of tokens issued in total). Therefore, whenever reserves are in the same state, the exchange price should be the same.

The equations that will be used to set the exchange rate for a community currency against the CLN are provided in the appendix. We show that they maintain this set of desired properties.

3.3 THE USE OF COMMUNITY CURRENCIES AS REWARDS FOR ECONOMIC ACTIVITY

The goal of community currencies is to be a store of value for local communities by connecting consumers and businesses. Thus we envision that the distribution of community currency will be carried out through purchasing transactions taking place at a brick-and-mortar merchant's terminal, as this form of distribution implements the focus of the CLN network on strengthening economic activity in local economies. To facilitate this, a portion of each transaction at a merchant's terminal will be subtracted from the payment to the merchant and allocated, as a **reward in community currency**, to the consumer and the merchant involved in the transaction for their economic activity in the community and on the network. In particular, when a consumer conducts a transaction using digital-fiat or crypto-fiat, a portion of the fiat payment will be exchanged to CLN and then to community currency using the market-making contract before being allocated to the parties. The use of the community currency in this manner will allow the network to offer a competitive alternative to traditional financial models.

Transaction flow diagram:



4. SUMMARY

The CLN creates a decentralized network of tools and services that support community payment systems. Through the introduction of community currencies, the CLN network creates a potential link between the economic activity taking place at brick-and-mortar merchants within the community, which is facilitated by fiat payments (whether digital or crypto-fiat), and the distribution of the community currency among stakeholders as a reward for engaging in this economic activity. The CLN network provides a platform for currency issuers and local gateways to support payments for goods and services and provide other financial services. Therefore, community currencies lower the barriers for communities to upgrade their payment infrastructure and reduce costs to intermediaries.

4.1 ACKNOWLEDGMENTS

This is a collaborative effort of multiple individuals within the Colu team, and involves reviews, comments, and contributions from Colu's board members, advisors, and partners. This paper was written by Mark Smargon, Amos Meiri and Dr. Dana Heller from Colu and by Dr. Omri Ross and Johannes Jensen, both from Blockchain Labs and the University of Copenhagen. The paper was built on the foundations and contributions of Eden Shochat, Tal Beja, Rotem Lev, and Elad Shabi.

Also special thanks—for feedback provided through comments and stimulating conversations—go to Meltem Demirors, Lou Kerner, Prof. Daniel Tsiddon and Prof Dan Ariely, Yaron Klainer, Leon Rossiter, Talia Soen, Joey Azizoff and Oded Leiba.

5. REFERENCES

- [1] Financial Globalization and Capital Flows Volatility Effects on Economic Growth, Carp, L. (2014).
- [2] [European Commission, Annual report on European SME's, 2015/16](https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf)
https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf.
- [3] Small Business Lending in the United States, 2014-2015, Office of Advocacy, U.S. Small Business Administration. Release Date: June 2017,
https://www.sba.gov/sites/default/files/Banking_study_Full_Report_508_FINAL.pdf.
- [4] Financing SMEs and Entrepreneurs 2016, An OECD scoreboard, Table 1.4,
http://dx.doi.org/10.1787/fin_sme_ent-2016-en.
- [5] The Role of Community Banks in the U.S. Economy,
<https://www.kansascityfed.org/Publicat/econrev/Pdf/2q03keet.pdf>; The Increasing Importance of Credit Unions in Small Business Lending, by the James A. Wilcox Haas School of Business, U C Berkely, Berkeley, CA 94720-1900, <https://www.sba.gov/sites/default/files/files/rs387tot.pdf>.
- [6] Scott, M. and Dodd, N., People Powered Money, Designing, developing and delivering community currencies.
- [7] Lluís, J., Rosa, D. La, and Stodder, J., 2015. On Velocity in Several Complementary Currencies. *International Journal of Community Currency Research*, Volume 19. Stodder, J., 2009. Complementary Credit Networks and Macro-Economic Stability: Switzerland's Wirtschaftsring. *Journal of Economic Behavior & Organization*, (2000), pp.79–95.
- [8] The Economic Viability of Complementary Currencies: Bound to Fail. Beat Weber, Oesterreichische Nationalbank (2015).
- [9] Bank of England - Staff Working Paper No. 605 - The macroeconomics of central bank issued digital currencies. John Barrdear and Michael Kumhof (2016 July).
- [10] For the UK, see “A Payments Strategy for the 21st Century—Putting the needs of users first”, Payment Strategy Forum, November 2016, p.5,

- https://implementation.paymentsforum.uk/sites/default/files/documents/A%20Payments%20Strategy%20for%20the%2021st%20Century%20-%20Putting%20the%20needs%20of%20users%20first_0.pdf ; for the US, see The U.S. Path to Faster Payments, Final Report Part One: The Faster Payments Task Force Approach, January 2017, p.16
<http://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-final-report-part1.pdf>.
- [11] Payments Strategy for the 21st Century (see previous footnote), p.7.
- [12] NPA Design and Transition Blueprint, Payment Strategy Forum, December 2017,
https://implementation.paymentsforum.uk/sites/default/files/documents/Design%20and%20Transition%20Blueprint_0.pdf
- [13] <http://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf> , p. 18.
- [14] The issuance of crypto-fiat tokens will reflect the gateway's liabilities to consumers. The token will behave like any other cryptocurrency except that the trust in the value of the token issued is merely the trust in the gateway that issued it to back it up with a fiat deposit and allow its convertibility back to fiat money.

APPENDIX A—MATHEMATICAL EQUATION FOR THE MECHANICAL MARKET-MAKING CONTRACT

The mechanical market-making contract is a formula that adjusts the exchange rate between two tokens—the CLN and a community currency—based on the total supply of tokens from each and the state of the reserves in each currency, which the contract controls. The reserves and the price evolve over time in response to demand for the tokens. The formula has a number of desired properties.

Given the total supply of the two tokens S_1, S_2 , the reserves owned by the contract for the two tokens, denoted by R_1 and R_2 , must satisfy at any time the following equation:

$$\text{Eq (1): } \left(\frac{S_1 - R_1}{S_1} \right)^2 + \left(\frac{S_2 - R_2}{S_2} \right)^2 = 1.$$

Alternatively stated, denote the percentage of tokens circulating outside the reserve of the contract by

$$x = \left(\frac{S_1 - R_1}{S_1} \right), y = \left(\frac{S_2 - R_2}{S_2} \right), \text{ then}$$

$x^2 + y^2 = 1$. In particular, given the reserve in Token1 R_1 , which determines x , we can express y and the reserve of Token2

$$y = \sqrt{1 - x^2},$$

and this determines R_2 in return,

$$R_2 = S_2 \left(1 - \sqrt{1 - \left(\frac{S_1 - R_1}{S_1} \right)^2} \right).$$

Note that given that starting conditions for the two reserves satisfy the relationship above,¹ the reserve of either of the tokens exhausts itself only when the entire supply of the other token is put into the opposite reserve—that is,

$$x = 1 \rightarrow y = 0 \text{ and } y = 1 \rightarrow x = 0,$$

or, alternatively stated, when $R_1 = S_1$ it implies $R_2 = 0$ and, symmetrically, when $R_2 = S_2$ then $R_1 = 0$.

¹ The smart contract responsible for the issuance of a new community currency ensures that starting conditions are satisfied. This is discussed in detail in Appendix B.

To derive the price of Token1, differentiate Eq (1) with respect to R_1 ,

$$\frac{2(S_1 - R_1)}{S_1^2} + \frac{2(S_2 - R_2) \frac{dR_2}{dR_1}}{S_2^2} = 0$$

$$P_1 = -\frac{dR_2}{dR_1} = \frac{(S_1 - R_1)}{(S_2 - R_2)} * \frac{S_2^2}{S_1^2} = \frac{S_2(S_1 - R_1)}{S_1 \sqrt{R_1(2S_1 - R_1)}}.$$

Price can also be expressed in terms of x and y ,

$$P_1 = \frac{x}{y} * \frac{S_2}{S_1}.$$

Note that when the limit cases are approached, the price approaches zero or infinity—that is, when $\lim_{R_1 \rightarrow S_1} P_1 = 0$, $\lim_{R_1 \rightarrow 0} P_1 = \infty$.

$R_1 = S_1$ then $P = 0$, and when $R_1 = 0$ then P_1 approaches infinity.

The smart contract needs to calculate for any amount E_1 of Token1 sent to the contract, and thus added to the reserve of Token1, the corresponding amount E_2 (in Token2) to be released from the reserve in exchange.

$$\begin{aligned} E_2(E_1) &= \int_{R_1}^{R_1 + E_1} P_1 dR_1 = \frac{S_2^2}{S_1^2} \int_{R_1}^{R_1 + E_1} \frac{S_1 - R_1}{S_2 - R_2} dR_1 \\ &\quad \text{s.t.} \\ \frac{S_2 - R_2}{S_2} &= \sqrt{1 - \frac{(S_1 - R_1)^2}{S_1^2}} \\ E_2(E_1) &= S_2 \int_{R_1}^{R_1 + E_1} \frac{S_1 - R_1}{S_1^2 * \sqrt{1 - \frac{(S_1 - R_1)^2}{S_1^2}}} dR_1 \\ E_2(E_1) &= S_2 \left(\sqrt{1 - \left(\frac{S_1 - R_1 - E_1}{S_1} \right)^2} - \sqrt{1 - \left(\frac{S_1 - R_1}{S_1} \right)^2} \right). \end{aligned}$$

To understand the price behavior, we can derive the percentage change in the price of Token 2 in response to an amount E_1 of Token1 sent to be exchanged. Assume that before the exchange of E_1 ,

$$R_1^0 = \beta S_1, E_1 = \alpha R_1^0.$$

This can be expressed as

$$x_0 = (1 - \beta), y_0 = \sqrt{1 - (1 - \beta^2)}.$$

After the exchange of E1,

$$\tilde{R}_1 = R_1^0 + E_1 = (1 + \alpha)R_1^0 = (1 + \alpha)\beta S_1, \text{ where } (1 + \alpha)\beta < 1.$$

Resulting in

$$\tilde{x} = \frac{S_1 - \tilde{R}_1}{S_1} = 1 - (1 + \alpha)\beta$$

$$\tilde{y} = \sqrt{1 - (1 - (1 + \alpha)\beta)^2} = \sqrt{\beta(1 + \alpha)(2 - \beta(1 + \alpha))}.$$

Thus the percentage change in the price of Token2 can be expressed as

$$\Delta P_2 = \frac{\tilde{P}_2}{P_2^0} - 1 = \frac{\tilde{y}/\tilde{x}}{y_0/x_0} - 1 = \frac{\sqrt{\beta(1 + \alpha)(2 - \beta(1 + \alpha))} * (1 - \beta)}{(1 - \beta(1 + \alpha)) * \sqrt{\beta(2 - \beta)}} - 1.$$

As can be seen from the equation, the percentage price change depends on the size of the reserve relative to the total supply of Token1, and on the size of the amount sent to be exchanged relative to the size of the reserve.

Alternatively, we can derive an expression for the percentage price change when E_1 is measured as a percentage of circulating supply outside the reserve of the contract. Let

$$E_1 = \alpha x_0, \text{ where } \alpha < 1.$$

After the exchange of E1,

$$\tilde{x} = (1 - \alpha)x_0$$

$$\tilde{y} = \sqrt{1 - (1 - \alpha)^2 x_0^2}.$$

Thus, the percentage change in the price of Token2 can be expressed as

$$\Delta P_2 = \frac{\tilde{P}_2}{P_2^0} - 1 = \frac{\tilde{y}/\tilde{x}}{y_0/x_0} - 1 = \frac{\sqrt{1 - (1 - \alpha)^2 x_0^2}}{(1 - \alpha)\sqrt{(1 - x_0^2)}} - 1.$$

APPENDIX B—MATHEMATICAL FORMULATION OF THE ISSUANCE OF A COMMUNITY CURRENCY AND THE LOCK-UP OF INITIAL RESERVES

The process

We want to define the parameters that an issuer has to provide the smart contract in order to facilitate a process that: a) issues a community currency, and b) establishes a two-side reserve in the CLN (Token 1) and in the community currency (Token 2). Denote the total supply of CLN by S_1 . There are two types of issuance procedures:

- Where CLN tokens are sent to the issuance contract by the issuer, referred to as “issuance with issuer’s own fund”
- Where the issuer specifies certain parameters for the issuance, but CLN tokens are sent to the contract by “investors” (i.e., any CLN token holder), referred to as “issuance with investors’ funds”

Issuance with issuer’s own funds

When issuing using this option, the issuer follows certain steps.

- Step 1: The issuer specifies to the contract the desired amount of tokens to issue, S_2 . The contract issues the tokens and locks them in the reserve—that is to say, $R_2=S_2$. This sets the price of Token 2 to zero, as

$$P_2 = y_0/x_0 \text{ where } x_0 = 1, y_0 = 0.$$

- Step 2: The issuer then sends an amount, I_1 , of CLN to the market-making contract, thus establishing

$$R_1 = I_1, x_0 = \frac{(S_1 - I_1)}{S_1}, y_0 = \sqrt{1 - x_0^2}$$

$$P_2^0 = \frac{\sqrt{1 - x_0^2}}{x_0} * \frac{S_1}{S_2}.$$

- Step 3: The issuer receives $y_0 * S_2$ of Token 2, P_2^0 is the **issuance price**, and the total value of Token 2 in circulation (i.e., outside the reserve of the contract) in CLN terms is equal to

$$V = P_2^0 * y_0 * S_2 = S_1 \frac{(1 - x_0^2)}{x_0}.$$

- Step 4: The market-making contract opens to any Token 1 or Token 2 holders.

Issuance with investors’ funds

When issuing using this option, the issuer follows certain steps.

- Step 1 is the same as in the first option.
- Step 2: The issuer specifies the amount, I_1 , of CLN expected to be received (“hard cap”) and a fraction β of the amount (“soft cap”) designated to be locked in reserve for the purpose of market making and establishing an issuance price.
- Step 3: The contracts test the validity of the (I_1, β) pair, verifying that if βI_1 of Token 1 are received, then the value of Token 2 in circulation (in CLN terms) is at least I_1 —that is, assuming that βI_1 of Token 1 are received, then

$$R_1 = \beta I_1, x_0 = \frac{(S_1 - \beta I_1)}{S_1}, y_0 = \sqrt{1 - x_0^2}$$

$$P_2^0 = \frac{\sqrt{1 - x_0^2}}{x_0} * \frac{S_1}{S_2}.$$

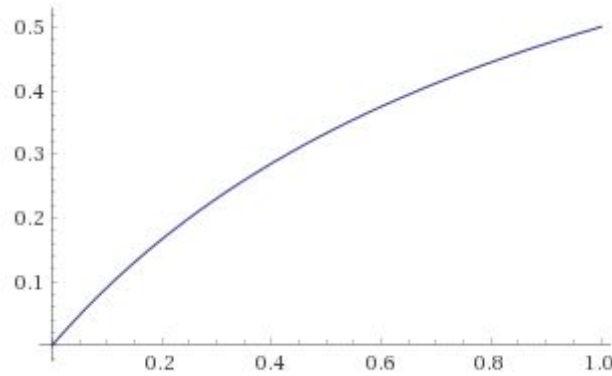
And the requirement is that

$$V = P_2^0 * y_0 * S_2 = S_1 \frac{(1 - x_0^2)}{x_0} \geq I_1 = \frac{R_1}{\beta} = \frac{(1 - x_0)S_1}{\beta}.$$

Thus requiring that

$$\beta \geq \frac{x_0}{1 + x_0}.$$

Note that the expression $\frac{x_0}{1 + x_0}$ is less than 0.5 for $0 \leq x_0 \leq 1$, and so $\beta \geq 0.5$ satisfies it automatically.



- If the contract passes the validity test, the contract opens to accepting CLN tokens from investors. Tokens sent to the contract are locked in the reserve.
- If less than βI_1 tokens are sent within the specified time, the contract returns the tokens to their holders and the contract shuts down (as funds received are below the “soft cap”). Any tokens in excess of I_1 (“hard cap”) are not accepted by the contract. Assuming the amount of tokens sent is within the range $(\beta I_1, I_1)$, any tokens in excess of βI_1 are sent to the issuer.
- Token 2 released from the reserve R_2 are distributed to investors so that their value given the issuance price is equal to the value of the investment sent in CLN. The validity test ensures that there are enough Token 2 in circulation to satisfy this condition given the issuance price established by the contract. Any excess Token 2 are sent to the issuer.