# Generic and Universal Local Cryptocurrency: LCoin

Frédéric A Hayek, Pascal Lafourcade, Ariane Tichit

# Generic and Universal Local Cryptocurrency: LCoin

Frédéric A. Hayek
*Université Clermont-Auvergne, CNRS*
*Mines de Saint-Etienne, LIMOS*
Clermont-Ferrand, France
0000-0003-1083-0625

Pascal Lafourcade
*Université Clermont-Auvergne, CNRS*
*Mines de Saint-Etienne, LIMOS*
Clermont-Ferrand, France
0000-0002-4459-511X

Ariane Tichit
*Université Clermont-Auvergne, CNRS*
*CERDI*
Clermont-Ferrand, France
0000-0001-5453-7901

***Abstract*—Different cryptocurrencies aim at solving different problems or offering different services. One underused application of cryptocurrencies is local currencies. Local currencies are currencies that float in a restricted area in purpose of growing the local economy by forcing local spending. Current digitalizations of local currencies have many drawbacks, whether taking the form of cryptocurrencies or not. We introduce the concept of geographical demurrage: money loses of its value the farther away it is spent. We construct four generic types of local cryptocurrencies: a regular one mimicking local paper money; a second that restricts spending to the dedicated geographical area; and a third that utilizes geographical demurrage for incentivizing shops. Finally, by lifting the geographical restrictions and maintaining geographical demurrage, we create a universal local cryptocurrency: a currency that loses value correspondingly to the distance between its point of reception and point of spending. So without the need to restrict spending to a given geographical sphere, the currency will always encourage local spending, no matter where it is spent; yielding a universal local cryptocurrency we name LCoin.**

***Index Terms*—Blockchain, Cryptocurrency, Local Currency**

## I. Introduction

Emulating cash in a digital form has been a cryptographs' goal for a long time. David Chaum's "Untraceable Electronic Cash" (e-cash) [1] was a first attempt. It focused on emulating the untraceability aspect of cash in a digital format. However its reliance on a trusted third party (bank) may have been detrimental to its development among users, and its untraceability may have been detrimental to its development among financial institutions. With the introduction of Bitcoin in 2008, cryptocurrencies changed the monetary paradigm.

### A. Blockchain

A blockchain is an append-only consistent synchronized distributed ledger that is maintained by a trustless network. It takes the form of a sequence of blocks, chained together by incorporating the hash of the previous block in the next. Starting from an arbitrary block called *genesis*, miners append to it block after block. The data written in these blocks must meet certain criteria and rules. In Bitcoin's blockchain for instance, the data are transactions, and they must be solvable (*i.e.*, more units owned by sender then units sent). Other blockchains have different applications and thus different rules. Ethereum [2] is a decentralized application platform, and thus its data are transactions, and more generally, smart contracts. Many blockchains are finding concrete real world applications, such as in healthcare [3], or in rewarding human behaviors [4]; other blockchains focus on privacy and keep the core of the blockchain malleable [5]. However, blockchain's most disruptive effects are felt by the banking industry [6].

A distinction is made between entities that maintain the blockchain and entities that create entries for the blockchain. They may or may not be the same entities. Maintainers of the blockchain are called *miners*, while those who create entries are called *users* or *clients*. Miners have the last word on what goes into the blockchain. The blockchain's openness can be categorized into:

- *permissionless* if the set of miners is unspecified;
- *permissioned* if the set of miners is specified;
- *public* if the set of clients is unspecified;
- *private* if the set of clients is specified.

Different blockchain settings have different applications. In some cases it is better to have high blockchain openness, such as cryptocurrencies; while in others it is not desired, such as a blockchain type ledger for a consortium of corporations.

Reaching consensus among miners is the key factor in blockchains. Blocks are appended to the blockchain by *miners*. This is done in one of two ways:

- either miners compete against each other to get the right to create the next block, this is called *Nakamoto-style* consensus, and it can be used with both permissioned and permissionless blockchains;
- or miners agree together on the next block using a *Byzantine Fault Tolerant* consensus, and it must have a finite set of miners of known size, hence it can only be applied on permissioned blockchains.

Nakamoto-style consensuses tend to be energy consuming. Agreeing on one entity in a trustless decentralized way among an unspecified set of unbounded size is extremely difficult. To solve this, Nakamoto-style consensuses give mining rights to the first entity to solve some specific problem. In Bitcoin [7] it is called Proof of Work and it consists of solving a partial hash inversion, in Primecoin [8] it is finding a special sequence of prime numbers (either a Cunningham chain or a Bi-Twin chain), in Peercoin [9] it is solving a partial hash inversion whose difficulty depends on one's amount of coins and their age, others propose to give mining rights to the first person to finish computing a highly sequential function [4] such as a

verifiable delay function [10]–[12]. Similarly, some introduce the notion of Proof of Sequential Work [13], [14].

BFT consensuses are typically less energy consuming and rely on communication much more between the nodes. They have been used for replicated services, such as in PBFT [15]. With BFT protocols' application to blockchain, the idea is for nodes to communicate their acceptance or rejection of a specified block for instance; and when enough acceptations are received by a node, it appends the block to its local blockchain. BFT consensuses have been improved over time, but not to accomodate huge numbers of participants; and the set of participants must be known ahead of time, making it unpractical for most blockchain usage: all permissionless blockchains and even permissioned blockchains where the set of miners can dynamically vary over time. Algorand [16]–[18] proposes solutions to both these problems: it is very scalable and permits dynamically shifting sets of miners. Algorand is a blockchain which supports the Algo cryptocurrrency. However, its $BA\star$ protocol is its most interesting feature. $BA\star$ is a BFT protocol to reach consensus in a scalable, secure and efficient manner. To accomodate huge numbers of miners, $BA\star$ randomly chooses a comittee in a private and non-interactive way. It is then this comittee that gets to effectively create the next block.

### B. Cryptocurrency

The original goal, as Bitcoin's whitepaper [7] states, is to be a "peer-to-peer electronic cash system", as such it aims at retaining the cash's peer-to-peer transaction property. However traceability in Bitcoin is persistent. Bitcoin's success is due to its lack of third-party reliance. Other cryptocurrencies try to contain untraceability, with varying degrees of success, such as Monero [19], [20] (based on CryptoNote [21], [22]), Zcash [23], [24], DeepOnion [25].

Cryptocurrencies have to address regular monetary policies, such as (i) money minting: cadence and total supply (limited or unlimited); as well as (ii) transaction fees (*i.e.*, taxes).

Another aspect of cash and regular digital currencies is their ease of use. Cryptocurrencies have to contend with this. One aspect of the ease of use is the cryptocurrency's throughput. This depends mainly on: (i) the block creation time and (ii) the block size. Indeed, Bitcoin's block creation time is an average of 10 minutes. And Bitcoin's block confirmation is 6 blocks, yielding an average of 60 minutes. As a result, the Lightning Network was introduced [26], [27]. The Lightning Network aims at scaling off-chain instant payments. Though there is a speed-security tradeoff [28], more recent cryptocurrencies bypass this problem by having a very short block creation time. For instance, Litecoin [29] was based on Bitcoin, but changed the block creation time to 2.5 minutes, Primecoin [8] has a block creation time of 1 minute and Ethereum's [2] block creation time is 12 seconds.

A *currency*, in the scope of a specific set of people, is something that satisfies the three following properties within that set of people:

- medium of exchange;
- store of value;
- measure of value.

Though cryptocurrencies adapted very much to be easy to use, their volatility remains a major hindering factor in their status as currency [30]. Indeed, very volatility disqualifies cryptocurrencies for they do not store value through time.

### C. Local Currency

There are many types of currencies. One form of currency is local currency [31]. Local currencies are not issued nor used by a country's highest administrative authority. A Local currency circulates over a dedicated geographical sphere which is smaller than the country's. In some cases a local currency can go over sovereign state borders. The goal of local currencies is to reinforce the local economy [32]. This is done by forcing people to spend their local money locally; and by forcing the recipients of the local money to also spend it locally. Local currencies are governed by local insitutions (usually local associations). Local currencies are emerging with momentum since the 2000's. They started being in paper format. With the digitalization of the economy, some are entering the digital world and some are reluctant to do so. The local currencies who do enter the digital world most often take the form of a centralized payment system. This permits accurate statistics on the local currency's usage. On the other hand it creates a single point of failure, it invades people's privacy and can give the entity that controls the servers full control over the digital financial space. The local insitutions are generally disinclined to the use of blockchains for local currencies because of cryptocurrencies' reputation of use in illegal activities as well as being uncontrollable.

We propose a framework for local cryptocurrencies. To do that, we also need to prove locality or distance. Many protocols have been developped for such ends.

### D. Distance Bounding

*Distance bounding* protocols were introduced by Brands and Chaum [33] in order for a specific device, the prover, to prove to another device, the verifier, that they are close by. Distance bounding protocols rely on the special theory of relativity stating that $C$, the speed of light, is the upper limit for the speed at which conventional matter or energy (and thus any signal carrying information) can travel through space [34]. Distance bounding protocols work by timing the delay between sending out a challenge bit and receiving back the corresponding response bit. Since information cannot travel faster than $C$, we can bound the distance between the prover and verifier to the distance travelled by light during the same delay. Distance bounding protocols defend against many fraud types [35], [36]. Each distance bounding protocol has its own security properties.

### E. Contributions

In this paper we tackle the issue of local cryptocurrency. We propose four generic constructions for local cryptocurrencies. The geniricity of the constructions resides in the modulable

| | Restricted Area | Geographical Demurrage |
|---|---|---|
| Generic 1 | $X$ | $X$ |
| Generic 2 | ✓ | $X$ |
| Generic 3 | ✓ | ✓ |
| Universal | $X$ | ✓ |

TABLE I: Four constructions properties.

parameters of the blockchain, most prominently the consensus mechanism and what it entails in terms of block confirmation time, but also in terms of block size, and thus throughput. The first construction emulates local paper money, even with its flaws such as allowing monetary circulation outside of the dedicated area. It is comparable to other existing local cryptocurrencies such as the e-Léman. The second construction builds on the first and restricts monetary circulation outside of the dedicated area. We do this by using the shops as Certificate Authorities to produce certificates proving that clients who wish to receive funds are indeed in the dedicated area. Shops verify proximity of clients with distance bounding protocols. The third construction introduces the concept of geographical demurrage: clients have to pay for transacting over distances. This is the first mention of geographical demurrage to the best of our knowledge. This geographical demurrage can be used to maintain the insitution's working capital and/or to incentivize shops to join the network. The fourth and final construction rids the third one from the geographical restriction and keeps the geographical demurrage. This yields a cryptocurrency that loses of its value when spent farther away, which incentivizes local spending without any restriction on the locality of the currency. We call this a universal local cryptocurrency and we name it: LCoin. Table I summarizes each construction's characteristics.

### F. Related Work

Adopting blockchain for local currencies has been quite strenuous [37]. Mainly because decentralized blockchains are theoretically prone to attacks such as the 51% attack on Nakamoto-style consensuses or nothing-at-stake attacks on proof of stake, which rendered the benefit to risk ratio too obscure [38]. However, blockchains are starting to emerge in the world of local currencies [39]. We explore below the two most prominent examples: Colu and Léman.

*a) Colu:* Colu is an Israeli company. They intend to bridge the gap between local currencies and cryptocurrencies. And as such they built their business on this idea. They are implemented in many parts of the world now. Colu provides a link between the local economy and Ethereum's blockchain; Colu's smartphone application being the intermediary. Colu works in the following way: Some local authority contacts Colu to implement a Colu local currency. Colu creates an ERC20 dedicated coin for this region (the "local Colu"), and they fix its price of 1 Colu to 1 sovereign currency unit. Local shops sign up with Colu to be allowed to receive local Colu transactions via their app. Local shops pay Colu a fee which is less than that of credit cards. Colu initially created the Colu Local Network coin on Ethereum as an ICO. Colu seems very centralized since transactions are processed solely by Colu. The only advantage of using this architecture with dedicated ERC20 acting as local coins is the immutable transaction history. Furthermore, the very goal of local currencies is to force a currency to circulate inside its dedicated geographical sphere; but Colu takes away part of this money as the fees charged to local shops go back to the Colu corporation.

*b) Léman:* The Léman is a set of two local currencies around the Geneva Lake (called *Lac Léman* in most French speaking regions). Geneva Lake lies between France and Switzerland and is one of the largest lakes in Western Europe. The two currencies are the Swiss Léman which is of fixed parity with the Swiss Franc; and the French Léman which is of fixed parity with the Euro. Both Léman currencies exist in paper format. Digital Léman currencies do exist. The Léman Foundation created a specific blockchain to support the digital Léman, called Com'Chain. The Com'Chain is a clone of Ethereum's blockchain. Anybody can become a miner of the Com'Chain, given they get approval by the Léman Foundation. The Léman Foundation gives accreditation to people who are invested in the local currency's well being. The Léman Foundation created a smartphone application to be the interface between users and miners. Only shops who are registered with the Léman Foundation are allowed to receive transactions. Most of this information was harvested by interviewing Léman Foundation members.

### G. Outline

In Section II we develop relevant monetary economics notions, and we introduce the concept of geographical demurrage. Then in Section III we formally define distance bounding protocols, which we use for location verification for the geographical demurrage. We introduce our first generic local cryptocurrency, mimicking local paper money, without geographical demurrage, in Section IV-A. Then we restrict money circulation to the dedicated area in Section IV-B. We build on it by adding geographical demurrage in Section IV-C. We expand the concept by lifting geographical restrictions and maintaining geographical demurrage to obtain a universal local cryptocurrency in Section IV-D. Finally we conclude in Section V.

## II. Economics Background

Local currencies have been on the rise since the early 2000s, especially in the West. The impact local currencies can have is clear from the Miracle of Wörgl [40] in the XX$^{\text{th}}$ century. During the great depression, Wörgl, a town in Austria, could develop their economy for a span less than a year, before being shut down by the Austrian Central Bank. Modern local currencies have legal frameworks. They are spearheaded by the Bristol Pound [41] in the UK, the Chiemgauer [42] in Germany and the Eusko [43] in France.

### A. Currency

*Definition 1 (Currency):* A *currency*, in the scope of a specific set of people, is something that satisfies the three following properties within that set of people:

- medium of exchange;
- store of value;
- measure of value.

As such, the sovereign state cannot decide what is or is not a currency, since the currency's three properties depend on its usage between people.

### B. Demurrage

An interesting aspect of Wörgl's miraculous currency was the existence of temporal demurrage [44], inspired by the works of Silvio Gesell [45]. Demurrage is when the amount of money lessens. Traditionally, demurrage refers to temporal demurrage (demurrage with time). Demurrage is similar to inflation. However, inflation is when the prices of goods and services go up – often mischaracterized by saying the currency's value goes down – while demurrage is about the amount of currency shrinking. We define two types of demurrage.

*Definition 2 (Temporal Demurrage): Temporal demurrage* is the cost associated with owning or holding currency over a given period.

*Definition 3 (Geographical Demurrage): Geographical demurrage* is the cost associated with spending currency over a distance from where it was acquired.

*a) Example:* The Swiss banks are known to provide negative interest rates. With time, the depositors' money shrinks. The depositors are still happy to put their money there thanks to banking secrecy and/or trust in Switzerland's banking sector stability. The temporal demurrage rate is constant.

*b) Example:* Many jobs reward their employees with meal vouchers or gas vouchers on top of the salaries. Shops also give out vouchers to clients from time to time. These vouchers are each worth a specific amount of money. However, the voucher has an expiration date, and after this date the voucher becomes worthless. This is an example of temporal demurrage where the demurrage rate is $100\%$ after the expiration date.

### C. Local Currency

A *local currency* is usually defined as a currency whose circulation is restricted to a geographical sphere. One can argue that such currencies have demurrage rate 0 (no demurrage) when spent inside their geographical sphere, and have demurrage rate 1 (100% demurrage) when spent outside their geographical sphere. Note that it is impossible to restrict a paper currency's circulation to any geographical sphere. It suffices for a spender to find a willing currency buyer outside the sphere and to make the transaction.

We will define a local currency in a broader way:

*Definition 4 (Local Currency):* A *local currency* is a currency with geographical demurrage.

In practice, many countries outlaw the use of local currencies. When they are approved, it is usually given the local currency does not compete against the state's currency, and following a set of rules and regulations. The complementary local currency must be proposed by an insitution which manages it. In order to have the right to transact in the local currency, shops must adhere to the insitution and sign the local currency's charter. Furthermore, the local currency must be pegged to the sovereign currency at a fixed rate. Finally, no fractional reserve is permitted: the insitution must hold 100% of the local currency's backing. However, users cannot convert their local currency back to sovereign currency: once a local unit of currency has been created (by depositting one unit of sovereign currency), it cannot be destroyed and is bound to circulate in that area forever. There is a catch however: because such a system is not viable since shops must import things or pay taxes, which are not accepted in local currency; local shops (and not regular users) are allowed to convert back the local currency to the sovereign currency by paying a fee to the insitution. Those conversation fees are what the insitution uses as working capital to keep going. Furthermore, there is no way to enforce the unlawful transactions in paper local currency. It suffices one customer holding local currency in paper format and one shop not adhering to the insitution that accepts it. The shop's owner can later pay some of its expenses with said local currency. In some local currencies those fees are kept at 0 (no fees to date).

### D. Cryptocurrency

A *digital currency* is any currency in digital form. All sovereign currencies exist as digital currencies. A *cryptocurrency* on the other hand is based on the distributed aspect. Based on [46], we define cryptocurrencies more straightforwardly:

*Definition 5 (Cryptocurrency):* A *cryptocurrency* is a digital currency relying on cryptographic primitives that requires no central authority to be created, spent or verified in any way.

To achieve this, cryptocurrencies rely on a distributed ledger [47], most often in the form of a blockchain [7], [48].

## III. Distance Bounding

Many technologies allow devices in proximity to communicate directly, such as NFC [49] or RFID [50]. These technologies rely on Radio Frequency (RF). They do not prevent attacks such as relay attacks for they are only communication protocols [51]. In this context, distance bounding protocols were invented to prevent such attacks from happening.

Distance bounding protocols [33] permit a specific device, the prover, to prove to another device, the verifier, that they are physically close by. Distance bounding protocols time the delay between challenge bits and response bits, and conclude that the prover must be less than the distance travelled by the speed of light in space during that delay. Distance bounding protocols identify many types of fraud [35], [36]:

- *Impersonation.* An *impersonation fraud* is an attack where an adversary acting alone purports to be a legitimate prover.
- *Distance Fraud.* A *distance fraud* is an attack where a dishonest prover purports to be in the neighborhood of the verifier. He cheats without help of other entities located in the neighborhood.
- *Mafia Fraud.* A *magia fraud* is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle between the verifier and an honest prover located outside the neighborhood.
- *Terrorist Fraud.* A *terrorist fraud* is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle between the verifier and a dishonest prover located outside of the neighborhood under the following circumstances. The dishonest prover actively helps the adversary to maximize her current attack success probability but without giving her any advantage for future man-in-the-middle attacks. (In such attacks, the man-in-the-middle would attempt to pass the distance bounding protocol as a valid prover/tag that the man-in-the-middle does not represent/possess.)
- *Distance Hijacking.* A *distance hijacking* is an attack where a dishonest prover aims to convince a verifier that he is located within the verifier's neighborhood, abusing some other provers who are indeed in the verifier's neighborhood.

Surveys [35], [36] show different distance bounding protocols resisting differently to the different identified attacks. In this paper we suppose the use of a distance bounding protocol resistant to all aforementioned attacks.

## IV. Local Cryptocurrency

We present four types of local cryptocurrencies. First, a local cryptocurrency that mimics the behavior of regular paper local currency. Secondly a local cryptocurrency restricting the proliferation of money to the dedicated geographical area. Thirdly a local cryptocurrency restricted to a specific area where geographical demurrage is applied. And fourthly a local cryptocurrency with geographical demurrage but without geographical restriction, yielding a universal local cryptocurrrency.

All the local cryptocurrencies we propose have similar fundamentals. The first type of local cryptocurrency is the basis for the other three.

### A. Generic Local Cryptocurrency I

First and foremost, the local currency insitution is in charge of the project, as for local paper money. It gets legal approval, it writes up a charter and calls for local shops to participate.

*Blockchain:* All local cryptocurrencies have the same type of blockchain. The blockchain needs to be permissioned, where the set of miners is a subset of associated local shops. Any associated local shop can become a miner. Depending on the blockchain's infrastructure, the shop must let other miners know of its intent to participate in the blockchain's mining.

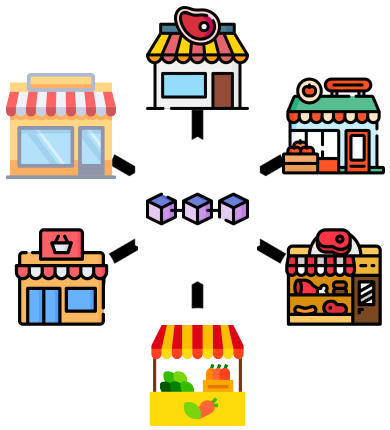

Fig. 1: Blockchain Miners.

This is illustrated in Figure 1. The consensus process is left to the insitution's discretion: this is part of the blockchain's and the local cryptocurrency's genericity. It can be any kind of consensus. However, since it is a permissioned blockchain, it would be more advantageous to use a BFT consensus such as Algorand's $BA\star$.

*Coins and Transactions:* When clients buy local cryptocurrency from the insitution in exchange of sovereign currency (whether in cash or digital format), the insitution keeps and safeguards the sovereign currency and issues a transaction on the blockchain to mint the corresponding amount of coins in the client's name (*i.e.*, his public key). The insitution effectively plays the role of an exchange platform. When shops want to buy back sovereign currency from the insitution, a fee could be applied to give the insitution working capital. When a buy back occurs, the corresponding coins on the blockchain are destroyed. Transactions are left in the format of unspent transaction output (UTXO): a transaction's output is used as input in a subsequent transaction, by signing it and binding it with the recipient's public key. We do not address privacy issues at this point in time. Transactions can have multiple inputs and one or two outputs. Each input is a separate coin. The first output is the beneficiary's coins, and the second is sender's the leftover change.

*Discussion:*

*a) Unrestricted Area:* In such a construction, transactions could occur between people who are not physically in the local currency's dedicated grographical sphere. Furthermore, nothing prevents unaffiliated shops (whether local or non-local) of setting up a public / private key pair and actively receiving payment in the local currency. However, they cannot buy back sovereign currrency from the insitution, since they are not affiliated. Though this is legal – as long as the shops pay their taxes (including the VAT) in sovereign currency – it goes against the local currency's raison d'être. However, despite its obvious issues, this does not fall behind local paper money for it suffers from the same vice. One way to restrict spending to a dedicated area is to only allow shops

as transaction recipients. Then clients cannot send money to each other. This seems as a major hindrance, and could be a major wall preventing adoption of the local currency.

*b) Trust in Shops:* It is true that clients have to trust associated shops, since their colluding could hinder the entire cryptocurrency. And trusting a finite set of entities would be a major flaw in any cryptocurrency. But comparing this to local paper currencies where clients trust that shops who adhered to the insitution will follow the charter they signed: both scenarios require trust in shops, albeit the local cryptocurrency version is much more detrimental to the clients if the shops turn out to be untrustworthy. This is still much more secure than a digital local currencyy (non cryptocurrency). This has no single point of failure, and it requires a majority of shops to be malicious and to collude in order to steel people's money. Whereas in conventional digital currency, one has to blindly trust the insitution in charge of all transactions.

### B. Generic Local Cryptocurrency II

This version of the local cryptocurrency builds on the previous one. We add a layer for limiting transactions to the geographical sphere. This is done by introducing a *Point of Attachment* and using distance bounding protocols to issue certificates of proximity.

Each coin has a *Point of Attachment* (PoA): this is the location of the coin at the current moment. When a coin is created, its PoA is the same as its creator, the insitution. Whenever a coin is spent, its new PoA is the recipient's location at the moment of transaction. The location of the recipient must be specified along with its public key. To determine the location of a recipient at the time of transaction, we use certificates delivered by Certificate Authorities (CAs). In our case, we limit ourselves to affiliated shops being the CAs, since local currency users inherently trust them for being part of the network, otherwise users would not use the local currency in the first place. Before issuing a certificate of proximity, CAs run a distance bounding protocol with the client to verify their proximity. The certificate of proximity comprises the public key of the client, along with the CA's location and the current time. If the recipient is an affiliated shop, then the shop just issues a certificate in its own name without running a distance bounding protocol. If the recipient is a client (peer-to-peer transfer), then the client must meet a CA and run a distance bounding protocol. The CA issues a certificate of proximity for the recipient which then sends it to the sender. The sender then has a set (unspecified at this point) amount of time to make the transaction. Let $\tau$ be the duration of time the certificate is valid for: miners do not accept a certificate older than $\tau$ to include in the blockchain. We suppose synchronicity between CAs.

*Discussion:* We can finally restrict monetary circulation to the dedicated geographical area. This is a wanted restriction in local currencies but that is unenforceable. We also trust shops as Certificate AUthorities. This trust is not problematic since we already trust the shops to mine the blockchain which is much more important. For the blockchain, we trust that most shops are not malicious and colluding, though for the certificates we trust that all shops do not collude with clients to issue false certificates of proximity.

### C. Generic Local Cryptocurrency III

Transactions on the blockchain incorporate geographical demurrage. Whenever a coin is spent, geographical demurrage is applied on it. The geographical demurrage is calculated based on the distance between the point where the coin was received by the sender, and the point where the sender is spending the coin.

Let $\delta(\cdot) : \mathbb{R}_{\geq 0} \rightarrow [0, 1]$ be a function that takes as input a distance, and outputs the corresponding geographical demurrage. $\delta(\cdot)$ must be a strictly increasing function with: $\delta(0) = 0$. Thanks to these properties, when a coin is spent exactly where it is, there is no demurrage; but when a coin is spent farther then the demurrage is bigger.

*Example:* Let $S$ be the sender and $R$ the receiver. Let $A$, $B$ and $C$ be three points. Suppose $S$ received $n$ coins when $S$ was at $A$. $S$ wants to send $m < n$ coins to $R$ at an ulterior moment in time where $S$ is at $B$ and $R$ is at $C$. Then the transaction is going to cost $S : \delta(||AC||)$.

To each coin corresponds a location. Shops are legally registered, and their location is available. As for clients' coins' location, it is the location of the client at the moment they acquired the coins. If the client buys coins from the insitution, the coins' location is the insitution's headquarters' location. Clients can receive coins from other clients, *i.e.*, they can buy coins from other clients. Whenever a coin is spent, demurrage is applied on the coin based on the distance between the coin's previous location and following location. Clients do not have a physical fixed location. In order to do that, they must prove their location at the time of receiving funds. To do that, they must go into a registered store and prove their location to that store with a distance bounding protocol. The store then issues a certificate that this person is indeed at that store at that time. This certificate is valid for a specific period of time. We do not specify optimal period in this paper.

*Example:* Let Alice buy coins from the insitution (whether online or in-person). These coins' location is set to be the insitution's headquarters' location. When Alice spends part of these coins at a shop, demurrage is computed based on the distance between the insitution's headquarters and the shop. When Alice sends money to Bob, Bob has to go into a registered shop (or the insitution's headquarters) and do a distance bounding protocol to prove he is in the close vicinity of this location. Then Alice sends Bob coins on which demurrage is applied based on the distance between the insitution's headquarters and the shop Bob went to.

*Transactions:* Transactions can have multiple inputs and multiple outputs. Each input is a separate coin. The first output is the beneficiary, and the rest of the outputs are the remainder of the coin, *i.e.*, the change. Thus, a sender can choose to pay some part of the transaction from coin $C_a$ at location $A$, another part of the transaction from coin $C_b$ from location $B$ *etc*. Figure 2 illustrates this. Equations 1 and 2 detail this. Let

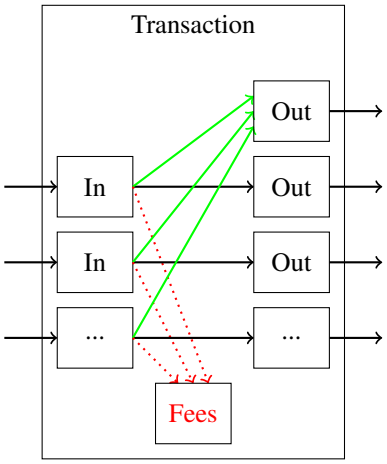


Fig. 2: Transaction Structure.

there be $n$ inputs, and $n+1$ outputs: $out_0$ corresponds to the recipient's sent coins, while $out_{j\neq 0}$ correspond to the change of coin $in_{j\neq 0}$. Let $\Delta_{i\neq 0}$ be the distance between input $in_i$ and the recipient's location. $d(\cdot)$ is the demurrage function: it takes a distance and outputs the corresponding demurrage rate. Let $out_{0,i}$ be the amount of coin $i$ that went into $out_0$. Equation 2 dictates that the amount from coin $i$ that went to the beneficiary is equal to or less than the amount sent $(in_i - out_i)$ on which geographical demurrage has been applied.

$$\sum_{i=1}^{n} out_{0,i} = out_0 \quad (1)$$

$$\forall i \in \{1, \cdots, n\}, (in_i - out_i) \cdot (1 - d(\Delta_i)) \geq out_{0,i} \quad (2)$$

The geographical demurrage can be seen as a fee to transact over distances. We propose two ways to handle fees: either the insitution benefits or the shops.

*a) Fees to the insitution:* In this option the fee in itself is destroyed: there is no beneficiary whom the fee goes to and can spend it. However, that does not entail money being destroyed. Since the insitution is compelled to have the equivalent of local currency safeguarded in sovereign currency, when the amount of local currency decreases, the insitution is no longer compelled to hold onto all of its sovereign currency reserve. The amount of local currency destroyed by geographical demurrage is gained by the insitution. The insitution can then use this money as working capital.

*b) Fees to the shops:* Another possibility we propose, is that the fees go to the miners – as happens in most cryptocurrencies. The miners here are the shops. They would be rewarded for taking part in the blockchain. Furthermore, they would be incentivized to be transparent and trusworthy, since maintaining the blockchain securely guarantees them income. This would also make up for their loss during reconversion of local currency to sovereign currency (where the insitution usually takes a reconversion fee). This way they would not necessarily be losing money by selling in the local currency instead of the sovereign currency.

### D. Universal Local Cryptocurrency: LCoin

In this final construction, we lift the geographic restriction that was imposed in the construction II and III (while keeping geographical demurrage as in construction III). Equivalent to this would be adding geographical demurrage to construction I. The transaction format remains the same as in construction III with Figure 2 and Equations 1 and 2 still applying. We call such a universal local cryptocurrency LCoin.

*Discussion:* In the universal local cryptocurrency, contrary to the generic local cryptocurrency, we deliberately let go of geographical restrictions. One could argue that this makes it a non local currrency for it is meant to be used in an unlimited area. However we do consider it a local currency in the sense of propelling local spending, since this new type of currency always encourages and incentivizes local spending. This universal type of local cryptocurrency has big scalable potential. Hence the recommendations of using a scalable consensus mechanism such as Algorand's $BA\star$ protocol.

In previous constructions, the insitution was responsible for setting the blockchain up, writing up the charter and creating coins. Everything was local. In this construction, a major obstacle is the non locality which we aimed for. It is an obstacle because we lose that centralized trusted format.

For the application of such a universal local cryptocurrency, different shops from different places and locations have to join the same network. It would be incumbent to have multiple exchange platforms to buy LCoins from, because if people do not have a nearby exchange platform they would see no benefit in paying enormous fees as geographical demurrage to spend money near them. Moreover, as the network grows geographically, trust becomes more difficult to maintain. It is easy to trust local shops since clients frequent them and know them. But when it comes to trusting a network made of shops whose majority is unkown to the client it becomes that much more difficult. We foresee that such a theoretical universal local cryptocurrency will inherently have borders such as state borders since it is easier to enforce laws within the judicial structure. And enforceable laws make for greater trust. Another downside of the universal local cryptocurrency is that if it grows to cover most of a sovereign state's area, the state could see it as a competition to its national currency, and thus halt the project.

## V. Conclusion

In this paper we have tackled the topic of local cryptocurrencies. We have introduced a generic cryptocurrency that mimics local paper money. Then we went a step further and restricted money circulation to the dedicated geographical sphere, which is desired but unachieved in current local currencies – digital or otherwise. We achieved this with the use of distance bounding protocols. The shops play the role of Certificate Authorities and issue certificates of proximity for clients who wish to receive funds. We also introduced the notion of geographical demurrage. And we used geographical demurrage on the local cryptocurrency to help maintain the system. Finally, by lifting the restrictions on local spending and keeping the geographical

demurrage, we obbtain a universal local cryptocurrency we name LCoin. This cryptocurrency incentivizes local spending and is not restricted to any area. Privacy was not a main focal point of our research. It requires deepening in distance bounding protocols' privacy. Furthermore, too much privacy would make it less likely for the local cryptocurrency to be accepted by the sovereign state. Hence, we leave privacy as a future work in this course of action.

## REFERENCES


[1] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Advances in Cryptology—CRYPTO'88: Proceedings 8*. Springer, 1990.

[2] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, 2014.

[3] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys (CSUR)*, 2020.

[4] C. Gritti, F. A. Hayek, and P. Lafourcade, "Generic blockchain on generic human behavior," in *SECRYPT 2023*, 2023.

[5] F. A. Hayek, M. Koscina, P. Lafourcade, and C. Olivier-Anclin, "Generic privacy preserving private permissioned blockchains," in *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 2023.

[6] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial innovation*, 2016.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.

[8] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," *July 7th*, 2013.

[9] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper*, August 2012.

[10] D. Boneh, B. Bünz, and B. Fisch, "A survey of two verifiable delay functions," Cryptology ePrint Archive, Paper 2018/712, 2018.

[11] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Annual international cryptology conference*. Springer, 2018.

[12] J. Long, "Nakamoto consensus with verifiable delay puzzle," *arXiv preprint arXiv:1908.06394*, 2019.

[13] M. Mahmoody, T. Moran, and S. Vadhan, "Publicly verifiable proofs of sequential work," in *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, 2013.

[14] B. Cohen and K. Pietrzak, "Simple proofs of sequential work," in *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II*. Springer, 2018.

[15] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, 2002.

[16] J. Chen and S. Micali, "Algorand," *arXiv preprint arXiv:1607.01341*, 2016.

[17] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th symposium on operating systems principles*, 2017.

[18] J. Chen and S. Micali, "Algorand: A secure and efficient distributed ledger," *Theoretical Computer Science*, 2019.

[19] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan *et al.*, "An empirical analysis of traceability in the monero blockchain," *arXiv preprint arXiv:1704.04299*, 2017.

[20] Y. Li, G. Yang, W. Susilo, Y. Yu, M. H. Au, and D. Liu, "Traceable monero: Anonymous cryptocurrency with enhanced accountability," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[21] N. Van Saberhagen, "Cryptonote v 2.0," 2013.

[22] Z. Yu, M. H. Au, J. Yu, R. Yang, Q. Xu, and W. F. Lau, "New empirical traceability analysis of cryptonote-style blockchains," in *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers*. Springer, 2019.

[23] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," *GitHub: San Francisco, CA, USA*, 2016.

[24] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in zcash," in *27th {USENIX} security symposium ({USENIX} security 18)*, 2018.

[25] Deeper, Monocolor, Nezero, Impressive, DogLover, Sean, D. Damian, and Airtorp, "Deeponion white paper," *self-published paper*, 2018.

[26] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[27] N. Khan and R. State, "Lightning network: A comparative review of transaction fees and data analysis," in *Blockchain and Applications: International Congress*. Springer, 2020.

[28] A. Kiayias and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols," *Cryptology ePrint Archive*, 2015.

[29] I. Takashima, "Litecoin: The ultimate guide to the world of litecoin, litecoin crypocurrency, litecoin investing, litecoin mining, litecoin guide, cryptocurrency," 2018.

[30] J. Liu and A. Serletis, "Volatility in the cryptocurrency market," *Open Economies Review*, 2019.

[31] J. Blanc *et al.*, "Classifying" ccs": Community, complementary and local currencies' types and generations," Tech. Rep., 2011.

[32] O. Groppa, "Complementary currency and its impact on the economy," 2013.

[33] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology—EUROCRYPT'93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings 12*. Springer, 1994.

[34] M. Fayngold, *Special Relativity and how it Works*. John Wiley & Sons, 2008.

[35] G. Avoine, M. A. Bingöl, I. Boureanu, S. Čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla *et al.*, "Security of distance-bounding: A survey," *ACM Computing Surveys (CSUR)*, 2018.

[36] A. Brelurut, D. Gerault, and P. Lafourcade, "Survey of distance bounding protocols and threats," in *Foundations and Practice of Security: 8th International Symposium, FPS 2015, Clermont-Ferrand, France, October 26-28, 2015, Revised Selected Papers 8*. Springer, 2016.

[37] F. Pinos, "How could blockchain be a key resource in the value creation process of a local currency? A case study centered on Eusko," *International Journal of Community Currency Research*, vol. Vol. 24 (Summer) Issue 2, pp. 1-13, 2020. [Online]. Available: https://hal.science/hal-03121151

[38] S. Seang, D. Torre *et al.*, "Proof of work and proof of stake consensus protocols: a blockchain application for local complementary currencies," *France: Universite Cote d'Azur-GREDEG-CNRS. Str*, 2018.

[39] A. Tichit, C. Elissée, F. Hayek, and P. Lafourcade, "La Blockchain, avenir des monnaies locales ?" Apr. 2022, working paper or preprint. [Online]. Available: https://hal.science/hal-03659241

[40] E. Barinaga, "The miracle of wörgl," 2020.

[41] A. P. Marshall and D. W. O'Neill, "The bristol pound: A tool for localisation?" *Ecological Economics*, 2018.

[42] C. Gelleri, "Chiemgauer regiomoney-theory and practice of a regional currency," *International Journal of Community Currency Research*, 2009.

[43] D. Edme-Sanjurjo, M. F. Duclerc, Y. Lung, J. Milanesi, and F. Pinos, "The eusko's trajectory. hypotheses to understand the success of the complementary local currency of the northern basque country," *International Journal of Community Currency Research*, 2020.

[44] J. . o. Blanc, "Free money for social progress: theory and practice of gesell's accelerated money," *American Journal of Economics and Sociology*, 1998.

[45] S. Gesell, *The natural economic order*. Owen London, 1958.

[46] J. Lansky, "Possible state approaches to cryptocurrencies," *Journal of Systems integration*, 2018.

[47] N. El Ioini and C. Pahl, "A review of distributed ledger technologies," in *On the Move to Meaningful Internet Systems. OTM 2018 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II*. Springer, 2018.

[48] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[49] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (nfc) technology," *Wireless personal communications*, 2013.

[50] A. Juels, "Rfid security and privacy: A research survey," *IEEE journal on selected areas in communications*, 2006.

[51] Y.-J. Tu and S. Piramuthu, "On addressing rfid/nfc-based relay attacks: An overview," *Decision Support Systems*, 2020.