# 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*—Blockchains are finding evermore applications. One underused application of blockchains is local currencies. Local currencies are currencies that float in a restricted area in purpose of growing the local economy by forcing local spending. We introduce the concept of geographical demurrage: money loses of its value the farther away it is spent. We construct four generic local cryptocurrencies: a regular one mimicking local paper money; a second that restricts spending to the dedicated geographical area; a third that utilizes geographical demurrage for maintaining the system, and a fourth that lifts the geographical restrictions and maintains geographical demurrage, thus creating 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. Blockchains made this possible with the introduction of Bitcoin [1]. The data written in the blocks must meet certain criteria and rules. In Bitcoin 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 [2]–[6].

A distinction is made between entities that maintain the blockchain and entities that create entries for the blockchain. Overlapping may occur. Maintainers of the blockchain are called *miners*, while those who create entries are called *users* or *clients*. 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.

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. There are many ways to do that [7].

### A. Local Currency

One form of currency is local currency [8]. 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. The goal of local currencies is to reinforce the local economy [9]. This is done by forcing local spending. Local currencies are governed by local institutions (usually associations). These institutions have a network of adherant shops. The local currency must be pegged to the sovereign currency, and no fractional reserve is permitted: the institution must hold 100% of the local currency's backing. Users can buy local currency from the institution. Only local shops are allowed to convert local currency back to sovereign currency by paying a fee to the institution. These conversion fees fuel the institution's working capital.

The local currencies who 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 and control. The local institutions are generally disinclined to the use of blockchains because of its reputation in illegal activities.

Wörgl's local currency implemented a concept of *temporal demurrage* [10] where there is a cost associated with owning or holding currency over a given period.

We introduce the concept of *geographical demurrage* where there is a cost associated with spending currency over a distance from where it was acquired.

### B. Distance Bounding

*Distance bounding* protocols [11] permit 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 [12]. 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 [13], [14].

### C. Contributions

We propose four generic constructions for local cryptocurrencies. The geniricity of the constructions resides in the modulable parameters of the blockchain, most prominently the consensus mechanism, but also block confirmation time, block

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

TABLE I: Four constructions properties.

size *etc*. The first construction emulates local paper money still 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 institution'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 far 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.

### D. Related Work

Blockchains for local currencies has been disregarded [15], [16], but is now on the rise [17]. We explore below the two most prominent examples: Colu and Léman.

*a) Colu:* Colu provides a link between the local economy and Ethereum's blockchain; Colu's smartphone application being the intermediary. 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 (also called *Lac Léman*). It lies between France and Switzerland. 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. The Léman Foundation created a specific blockchain to support the digital Léman, called Com'Chain. It is a clone of Ethereum's blockchain. Anybody can become a miner, 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.

## II. Local Cryptocurrency

### A. Generic Local Cryptocurrency I

The local currency institution 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 our constructions have the same type of blockchain. The blockchain needs to be permissioned, where the set of miners is a subset of associated local shops. The consensus process is left to the institution's discretion: this is part of the blockchain's genericity.

*Coins and Transactions:* When clients buy local cryptocurrency from the institution in exchange of sovereign currency, the institution safeguards the sovereign currency and issues a transaction on the blockchain to mint the corresponding amount of coins in the client's name. The institution effectively plays the role of an exchange platform. When shops want to buy back sovereign currency from the institution, a fee could be applied to give the institution 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.

*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 actively receiving payment in the local currency. However, they cannot buy back sovereign currrency from the institution, since they are not affiliated. Though this is legal, 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 a major hindrance, and could be a major wall preventing adoption of the local currency.

*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 institution 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 institution 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 institution. 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. 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 has a set 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.

*Restricted Area:* 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 coin's successive PoAs.

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 ni 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 $S : \delta(||AC||)$.

*Example:* Let Alice buy coins from the institution. These coins' PoA is set to be the institution's headquarters' location. When Alice spends part of these coins at a shop, demurrage is computed based on the distance between the institution's headquarters and the shop. When Alice sends money to Bob, Bob has to go into a registered shop (or the institution's headquarters) and do a distance bounding protocol to prove he is in the vicinity of this location. Alice sends Bob coins on which demurrage is applied based on the distance between the institution'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 coins, *i.e.*, the change. Thus, a sender can choose to pay some part of the transaction from coin $C_a$ from PoA $A$, another part of the transaction from coin $C_b$ from PoA $B$ *etc*. Figure 1 illustrates this. Equations 1 and 2 detail this. Let 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 institution benefits or the shops.

*Fees to the institution:* 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 institution is compelled to have the equivalent of local currency safeguarded in sovereign currency, when the amount of local currency decreases, the institution is no longer

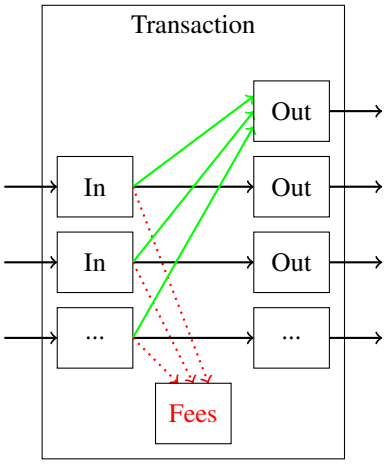


Fig. 1: Transaction Structure.

compelled to hold onto all of its sovereign currency reserve. The amount of local currency destroyed by geographical demurrage is gained by the institution. The institution can then use this money as working capital.

*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.

### D. Universal Local Cryptocurrency: LCoin

In this final construction, we lift the geographic restriction that was imposed in constructions II and III. Equivalently we could add geographical demurrage to construction I. The transaction format remains the same as in construction III with Figure 1 and Equations 1 and 2 still applying. We call such a universal local cryptocurrency LCoin.

*Discussion:* This cryptocurrency is by design geographically unrestricted. However it still 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 local cryptocurrency has big scalable potential.

For the application of such a universal local cryptocurrency, different shops from different areas have to join the same network. It would be incumbent to have multiple exchange platforms to buy LCoins from, so people can easily buy local currency. Moreover, as the network grows geographically, trust becomes more difficult to maintain: clients have to trust a network made of shops whose majority is unknown to the client. 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 same judicial structure. Another potential downside is that if it grows to cover most of a sovereign state's area, the state could consider it as a competition to its national currency and intervene.

## III. Conclusion

In this paper we have tackled the topic of local cryptocurrencies. We have introduced a generic blockchain that mimics local paper money. Then we 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 introduced the notion of geographical demurrage. 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.

## References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.
[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] C. Zhang, C. Wu, and X. Wang, "Overview of blockchain consensus mechanism," in *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, 2020.
[8] J. Blanc *et al.*, "Classifying" ccs": Community, complementary and local currencies' types and generations," Tech. Rep., 2011.
[9] O. Groppa, "Complementary currency and its impact on the economy," 2013.
[10] J. . o. Blanc, "Free money for social progress: theory and practice of gesell's accelerated money," *American Journal of Economics and Sociology*, 1998.
[11] 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.
[12] M. Fayngold, *Special Relativity and how it Works*. John Wiley & Sons, 2008.
[13] 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.
[14] 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.
[15] 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*, 2020.
[16] 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.
[17] 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