Which kind of blockchain application for local complementary currencies?

Sothearath Seang, Dominique Torre

Which kind of blockchain application for local complementary currencies?

Sothearath SEANG* Dominique TORRE*

May 2020

Abstract

This paper examines the application of the blockchain technology to local complementary currencies through two consensus protocols: the Proof of Work (PoW) and the Proof of Stake (PoS). Given the increasing digitisation of local currencies, and the challenges affecting their management and operation, we analyse the potential of a technological solution in addressing these issues. The case of local currencies with a blockchain is different from the case of crypto-currencies as there is no speculation possible due to the one-to-one fixed exchange rate with the legal tender, and the geographical limit of use for local currencies. In this context, the blockchain offers different services and has different properties. The choice of the right validation process matters in this case, but also incentives of miners and validators to participate in the process.

JEL Classification: E42, R5

Keywords: digitisation, community currency, Proof of Work, Proof of Stake, payment systems

*Université Côte d'Azur - GREDEG - CNRS, 250 rue Albert Einstein, 06560 Valbonne, France. E-mails: sothearath.seang@gredeg.cnrs.fr, dominique.torre@gredeg.cnrs.fr

1 Introduction

The blockchain technology has sparked much interest around the world in recent years, and its applications are being tested across many sectors such as finance, energy, public services and sharing platforms. Although the technology has not matured sufficiently to be operable in all domains, and is being subjected to numerous ongoing experiments, the potentially diverse benefits and opportunities deriving from its decentralised and open-to-innovation nature are attracting huge attention from researchers and investors. Its mainstream adoption will take time and will require a certain degree of novelty and a certain level of technological, social and regulatory effort to coordinate it (Iansiti and Lakhani, 2017). The first ever and most well-known application of the blockchain is the Bitcoin. Its advent has triggered the emergence of thousands of other crypto-currencies, each with different aims and properties. The controversial success of crypto-currencies has promoted the blockchain as one of the symbols of a globalised market without seat nor frontiers, which facilitates speculation and promotes anonymous mechanisms and irresponsible behaviours. As a counterpoint to this universe without distance and identity, have also emerged from the late 2010 decade new needs for authenticity, proximity, local anchoring, that echo with the rise of ecological attitudes and as a reaction against the scourge of standardisation. Local initiatives have emerged to allow local government and citizens to re-appropriate for themselves distribution channels, to develop traceability, to revitalise the commercial activities of their city centres,...*etc.* This paper wishes to point out the role of the blockchain in these local universes, where proximity makes actions less anonymous, and where sustainability is frequently a substitute for profitability. In these local circles, the blockchain should surely have its place, but we cannot imagine reproducing *stricto sensu* the same model that was adopted for crypto-currencies.

Local complementary currencies are payment systems that function alongside legal tenders in a geographical area. Given the increasing digitisation of local currencies, and the current challenges affecting their management and operation, we analyse the potential of a technological solution in addressing these issues. The objective of this paper is to analyse the application of two blockchain consensus protocols to manage a local currency or a network of local currencies. The case of local currencies with a blockchain is different from the case of crypto-currencies as there is no speculation possible due to the one-to-one fixed exchange rate with the legal tender, and the geographical limit of use for local currencies. These specificities, combined with those of the blockchain, allow for a relevant study of two models of blockchain-based solutions with heterogeneous agents who interact with each other and have different objectives and characteristics.

The paper is organised as follows. Section 2 describes the main features of a local currency and the motives behind its recent increasing digitisation. Section 3 provides an overview of the blockchain technology - its foundations, and its application in different sectors. Section 4 analyses the blockchain application in the context of local currencies by addressing the potentials of the technology, the two models of consensus protocols (Proof of Work and Proof of Stake), and the eventual concerns for such application. Section

5 exposes the alternative consensus protocols, opens the discussion and provides some suggestions for further research. Section 6 concludes the paper.

2 Local currencies and their digitisation

2.1 Objectives and management of local currencies

A local (or community) currency is a type of complementary currency,[1] *i.e.* a payment system which generally is restricted to a specific geographical area (*e.g.* a town, a city, an agglomeration). It functions alongside the legal tender and aims to promote sustainable development. Complementary currencies can contribute to the achievement of objectives such as revitalising local businesses (Renoir currency in Cagnes-sur-Mer, France), strengthening social relations and community welfare (Fureai Kippu currency in Japan), promoting and protecting a local identity (Eusko in Basque country, France), helping people in difficulty and alleviating poverty (Palma currency in Brazil), acting as an alternative payment method during financial crises (Tem currency in Greece), and fostering production and short distribution channels, promoting sustainable behaviors and helping unemployed people by providing with jobs paid in the local currency.

In general, businesses that accept a local currency must adhere to the community values and abide by specific rules which generally are defined by a charter (*e.g.* guarantee ethical and sustainable practices by its members, and high quality of products sold in the community (Blanc and Fare, 2016)). For instance, in the French Basque country, merchants who accept the local community currency (Eusko) as a payment must display product labelling in both French and Euskara since one the objectives of the association is to promote and protect use of the local language.[2]

The local currency issuer or project leader is usually a non-profit association but could be a local government or a merchants' federation or association. Management of the currency is ensured by the issuer, or can be delegated to an external financial agent. This management includes printing the notes if the chosen form is fiat money, providing conversion services through exchange offices (usually merchants who accept the local currency) and determining the properties of the local currency *i.e.* additional advantages to the users such as 10% benefit when converting from legal tender to local currency, or guaranteed access to higher quality products.

If the local currency takes the form of notes, security features such as specially watermarked paper and bubbles patterns protect them from counterfeiting and provide assurance of their authenticity. In general, there is a fixed one to one exchange rate between the local currency and the legal tender which reduces the possibility of specula-

[1] A local currency differs from other types of complementary currencies such as local exchange trading systems (LETS), time banks and virtual/crypto-currencies. See Tichit, Lafourcade and Mazenod (2017) for a list of the criteria used to distinguish different types of complementary currencies.

[2] http://www.euskalmoneta.org/statuts/

tion. To avoid local currency hoarding, several different methods may be employed. For instance, some local currencies are defined as melting currencies *i.e.* the local currency note loses $x\%$ of its value if it is not spent within a given period of time (usually a few months) so there is an incentive for currency holders to spend it as quickly as possible which increases the velocity of circulation of the currency.

The currency issuer generally deposits legal tender which are converted by users at a partner bank. Generally, One means of covering the operating expenses of the local currency is to charge a percentage to merchants reconverting the local currency. This could be perceived as a constraint to adoption of the local currency but is an additional incentive for merchants to find business partners or ways to re-inject the money back into the local community.

2.2 Digitisation of local currencies

Some local complementary currencies exist only in digital form, for instance the *So-Nantes* currency in the Loire Atlantique county in France. These digital currency forms usually are administered by one or a few central entities such as a bank or an information technology (IT) firm. Recent years provide many examples of local currencies originally introduced in the form of notes and transitioning to a digital version. The change to digital version is a crucial milestone on the path to an improved local currency; it especially alleviates the burden associated to traditional paper based business-to-business (B2B) transactions in local currencies (Blanc and Fare, 2018). Groppa (2013) finds also that the spending multiplier is greater in digital community currencies systems compared to the regular money market. Having a digital version of a local currency may also signify a better control of the money supply, and of the transactions' management, since most of the tasks and statistics are automated. Taking the example of the Eusko, which is the most important local currency in Europe, it is available in both in notes and digital form. Therefore, the motives behind digitisation of a complementary currency might be multiple: elimination of paper printing costs, facilitating B2B transactions, reducing administration costs and reliance on third-parties, and increasing the likelihood of attracting younger users, alongside all the potential benefits and opportunities that can be derived from use of a decentralised management solution such as blockchain.[3] Table 1 provides an overview of local currencies in Europe that have transitioned or are in the process of transitioning to a digital form, and those already in digital form. It is therefore reasonable to imagine decentralised solutions to managing these currencies that would not include banks or other financial agents (with a possible monetary motivation). Application of the blockchain via different consensus protocols could be relevant in this context.

[3] The alleged advantages of the blockchain are discussed briefly in section 2.

Currency name	City/Town/Area of use	Country	Form
Boniato	Madrid	Spain	Digital
Bristol Pound	Bristol	United Kingdom	Notes & Digital
Brixton Pound	Brixton	United Kingdom	Notes & Digital
Chiemgauer	Prien am Chiemsee	Germany	Notes & Digital
Eusko	Pays Basque	France	Notes & Digital
Gonette	Lyon	France	Notes & Digital
Grama	S. Coloma de Gramenet	Spain	Digital
Kingston Pound	Kingston	United Kingdom	Digital
Léman	Lake Geneva	France/Switzerland	Notes & Digital
Pive	Franche-Comté	France	Notes & Digitising*
Racine	Chevreuse Valley	France	Notes & Digitising
Renoir	Cagnes-sur-Mer	France	Notes & Digitising
Sol-Violette	Toulouse	France	Notes & Digitising
Sonantes	Loire-Atlantique	France	Digital
Stück	Strasbourg	France	Notes & Digitising
Trèfle	Périgueux	France	Digital
Turuta	Vilanova i la Gellrù	Spain	Digital
Vilawatt	Viladecans	Spain	Notes & Digitising

Table 1. List of digital local currencies in Europe as of December 2019 (non-exhaustive)

*In the process of or considering a digitisation according to the official website of each currency. The same applies to the Renoir, the Sol-Violette and the Stück currency.

3 The blockchain technology

3.1 Overview and applications of the technology

A blockchain is a general purpose technology and a type of distributed ledger technology (DLT) which is secured by cryptography.[4] Information is gathered into blocks that are linked to one another and constitute a chain of information that is immutable, therefore serving as a proof of existence of a transaction, or of any type of information at any given point in time. Because there is no central authority to regulate and control the system, consensus among users is paramount to guarantee the security and sustainability of the system.[5] Global agreement on the blockchain is facilitated by the implementation of a consensus protocol which dictates the rules by which users must play and abide.

[4] A DLT is a record-keeping system where all or some of its users possess a copy of the ledger. Cryptography is the science of mathematical codes and techniques to enable secure communication with unknown third parties (Pilkington, 2016). A blockchain is a cryptographic-based DLT.

[5] This is valid for a public or permission-less blockchain. For private, permissioned or consortium blockchains, one entity or a group of entities can control who sees, writes and modifies the data on it. The decentralisation aspect is essential and is the core value in the blockchain so in what follows we consider only the case of a public blockchain.

The blockchain technology is being studied and tested in many sectors including finance, energy, cybersecurity, healthcare, government services and e-residency. Fully functional blockchain applications include control of supply chain management using the Everledger blockchain which tracks diamonds (from their discovery to their final form) and guarantee of the authenticity of diplomas (at the École Supérieure d'Ingénieurs Léonard-de-Vinci in France). Wolfond (2017) explains how implementation of a decentralised and collaborative identity verification model based on the blockchain that possesses certain characteristics could allow for a substantial reduction in the healthcare and government services costs in Canada which would benefit businesses and citizens. Kshetri (2017) presents the example of a blockchain applied to the healthcare industry to point out the potential improvements in terms of security and privacy, and the possibilities for the technology to resolve certain major problems related to the current cloud-based Internet-of-things (IoT) systems. In the energy sector, blockchain applications via Ethereum-based smart contracts are being tested to understand distributed market coordination and data management architectures for decentralised energy systems (Hukkinen, Mattila, Ilomäki and Seppälä, 2017). Sullivan and Burger (2017) examine the legal, policy and technical implications of the development of e-residency in Estonia.[6] The system has minimal identity requirements and authentications and allows nationals from any country to engage in a range of economic activities in Estonia.

From an economic perspective, Catalini and Gans (2016) discuss how the reduced verification and networking costs allowed by the blockchain system change the types of transactions supported in the economy. They analyse the implications for intermediation and argue that although blockchain implementation would hugely reduce the market power of intermediaries, they would remain necessary for some offline tasks that still required human verification. Ølnes, Ubacht and Janssen (2017) conducted an assessment of the potential blockchain benefits identified in the literature, and classified them into different categories: strategic (transparency, fraud and manipulation avoidance, corruption reduction), organisational (increased trust, predictive capability and control, transparency and suitability, clear ownership), economic (reduced costs, spam resilience), informational (better data integrity and quality, reduced human error, access to information, privacy and reliability) and technological (resilience, security, persistence and irreversibility, reduced energy consumption). They found also that a robust governance model is a condition for blockchains to yield benefits.

In the banking industry, Guegan (2017) addressed various issues related to use of private blockchains to reduce costs, increase security and simplify bank operations. He emphasised that the current benefits to be derived from blockchains are more applicable to a public, and hence a decentralised model. The work of Guo and Liang (2016) explores the potential advantages related to clearing and credit information systems, and regulation, efficiency and security issues in the context of blockchain implementation in the Chinese banking industry. They conclude that those problems will be solved over time,

[6] According to the authors, Estonia is the most advanced country in the world in terms of government-backed programs for consumers' digital identity.

and the technology will be incorporated in the future. In the case of payment systems, Ripple is an interbank solution which allows high speed transactions (across the world in seconds), transparency and simplicity for users. It seeks to create a universal payment protocol and uses a digital currency called XRP for blockchain transactions (Schwartz, Youngs and Britto, 2014). Similarly, Jaag and Bach (2016) present the possibilities related to using blockchain for postal financial services to improve financial inclusion, and the creation of a postal crypto-currency to counter the high levels of volatility that plague most crypto-currencies. By backing coins with a national currency such as the US dollar, CryptoBucks and Tether (Conley, 2017) seek to overcome the market volatility of crypto-currencies, and induce consumer trust, and enhance ease of use and financial connections to the outside world. In the context of creating contracts and programs, the Ethereum blockchain allows its users to build, buy and sell smart-contracts based on the currency Ether which is the second largest crypto-currency in terms of market capitalisation.[7]

3.2 The proof of work and proof of stake consensus protocols

The first blockchain system application employed the PoW consensus protocol as its backbone and was introduced in the Bitcoin network in 2008 by Satoshi Nakamoto.[8]

In the PoW protocol, it is the combination of cryptography and computational power which creates the consensus and ensures the authenticity of the data recorded on the blockchain. Other features inherent to the system such as the size of the blocks, their generation rate and the money supply limit are defined in the protocol.[9] To show that a block is valid and that the necessary work has been completed, the network nodes (or miners) use their computational power to validate the transaction (*i.e.* verify that the sender has sufficient funds and is not double-spending), and most importantly, compete in the race to solve the cryptographic problems imposed by the protocol.[10] This process is called mining.

[7] According to https://coinmarketcap.com at the time of our writing.

[8] Collomb and Sok (2017) describe the Bitcoin system as a combination of past developments: Napster's 1999 peer-to-peer (P2P) protocol (a music exchanging platform), the 1970 cryptographic hash functions and encrypted block chaining mechanism, the 1993 PoW introduced to combat spamming, the 1979 Merkle tree compression mechanism to stock and manage big data and the concept of timestamp introduced in 1990 to ensure good IT security protocols. Since 2008 the Bitcoin blockchain has served as a reference for studies and applications of the technology.

[9] In the case of Bitcoin, block size is around 1 megabyte, generation rate is around 10 to 12 minutes, current bounty is 12.5 Bitcoin which is halved every 210,000 blocks or every 4 years, and the money supply limit is 21 million Bitcoins with the difficulty of the network readjusted every 2016 blocks or every two weeks. The PoW design varies greatly among crypto-currencies. For example, Litecoin has a money supply limit of 84 million Litecoins and a block generation rate of only 2.5 minutes. This frequency may be more appropriate for small transactions (such as coffee or bread purchases) which require only a few confirmations from the receiver (number of blocks (following the block containing the transaction) required to prove that the operation is authentic.

[10] Technically, miners need to find a hash value that is less than a certain number (the target or difficulty level), usually a number with leading zeros. To achieve this, random guesses are generated by adding and varying a nonce (an integer value) to the hash of the block.

The incentive for miners to join the race is twofold: the first miner to find a solution is rewarded with a bounty defined by the protocol and gets to collect all the fees associated to the transactions (borne by and varying among the users involved in the transactions) that they choose to include in the block. When a miner finds a solution, he / she creates a block X by including the hash of the previous block, the timestamp and the transactions. The miner broadcasts the newly created block X to the network and other miners verify the transactions and validate the block. The block is considered legitimate if other miners continue to work on extending the chain from block X. When a chain splits, miners will always choose the longest chain since this represents the most work. Miners can work on multiple chains but to the detriment of their computational power which is correspondingly reduced.

A miner's computational power plays a deterministic role in the PoW protocol since the greater the capacity to generate guesses (measured in hashes per second), the higher the probability of finding a solution. The computers run at full capacity 24 hours a day, thus the mining process consumes considerable amounts of electricity. That makes the PoW a extremely resource-intensive model, and the time and energy involved serve as proofs that the work has been done. In 2014, the total power consumed by the Bitcoin network was equal to the total electricity consumption of the island of Ireland (O'Dwyer and Malone, 2014). This protocol was approved by users and miners, and its wide adoption by other crypto-currencies has made it popular and recognised as a successful model. However, despite this, the future of the PoW remains unclear because it was not designed initially to manage a speculative asset which Bitcoin has become.

As Zhang (n.d.) puts it: "Like all distributed systems, blockchain systems are challenged with network latency, transmission errors, software bugs, security loopholes and black-hat hacker threats. Moreover, its decentralised nature suggests that no participant of the system cannot be trusted.[11] Malicious nodes may emerge, as does data difference due to conflicting interests." Problems inherent in distributed and decentralised systems continue to constitute a threat to their large scale implementation. In theory, the PoW system can be attacked if a lone miner or a group of miners control more than half of the network's total mining power. This is described as a 51% attack. In practice, attackers would create their own secret chain and once it exceeded the length of the honest chain broadcast it to the network in an attempt to double-spend or compromise the whole system. This new chain would be considered valid by other miners based on it being the longest chain, and these others would move on to work on subsequent blocks. At the start of 2014, the *G.HashIO* mining pool was near to reaching 51% then, fearing an attack several miners left the pool (CoinDesk, 2014).

The alternative to the PoW is the PoS protocol. It confers decision power on system stakeholders (minters or validators). Unlike the PoW where everyone can become a miner and participate in the process, not everyone can join the PoS protocol network.

[11] We believe the author made a typographical error and the phrase should be understood as "*no participant of the system can be trusted*".

Ownership of a currency or having a deposit in the network allows nodes (validators) to participate in the minting process (*i.e.* validating transactions and creating blocks.) Again, unlike the PoW system, no computational power is required to solve cryptographic puzzles. There are no rewards in the form of a money creation process:[12] validators collect fees from users and are paid by them as an intermediary. Since validators receive only transaction fees, the scenario in which validators create empty blocks is avoided[13] because they have an incentive to include the maximum number of transactions in order to maximise their gains. Because the money supply is based on what is issued originally (no money is created in this protocol), the problem arises of an initial fair coin distribution. If the PoS includes a selection process for validators (the greater the stake, the higher the probability of being selected as the creator of the next block), then additional balancing mechanisms are required to mitigate the risk of rich validators getting richer. PeerCoin is a crypto-currency which employs a PoW scheme for its initial mining phase and a PoS-based protocol to validate transactions and reward their validators (King and Nadal, 2012). It uses the *Coinage* concept and a stochastic PoS minting process.[14]

One of the problems related to PoS is the *nothing-at-stake* case which means that it costs a validator nothing to vote for more than one block. This problem could be solved by for instance allowing validators to vote only once or to penalise them heavily if they vote on more than one chain. In practice, it may be more complicated to solve this problem due to possible network delays and latency issues which might cause validators to receive offset chain information.

4 The blockchain application for local currencies

4.1 Potentials of the blockchain for local currencies

Removing intermediaries and improving management

One of the main ideas behind the Bitcoin is to allow individuals to transfer money between each other without the need of a bank, or to put it simply, a third-party who

[12] Many forms of PoS protocols exist and each version has its own set of rules and properties, the initial PoS form only rewards validators with transaction fees. The main differences between the PoW and the PoS are briefly summarised in Appendix 1 along with a list of crypto-currencies that use the PoW and pure form of the PoS.

[13] In the Bitcoin network miners can create empty blocks which contain only the coinbased transaction (their reward transaction), *e.g.* at block height 459713 (https://blockchain.info/block/000000000000000001bf525682830b4f77612eb36c2e73754345a7f91aebf7ea). One of the reasons for this behaviour is that miners prefer to conserve their hash power and time to work on subsequent blocks rather than including transactions in current blocks.

[14] In Peercoin, the duration of an unspent coin determines its *coinage e.g.* an individual who holds 4 coins for 10 days will have accumulated 40 coin-days and will have 4 times more chances to generate profit compared to someone with 10 coin-days. Once a miner is chosen to create a block, his/her coinage resets to zero and the individual must wait to accumulate coinage again. The minting process is designed to yield around 1% profit per year.

acts as a financial intermediary. As this is made possible thanks to the properties of the blockchain, in the same way, the technology can be used to free small communities from banks and third-party I.T. companies by respectively allowing transactions to occur without the need for confirmation from a bank and establishing a direct connection between the managers of the local currencies and the users for technical specificities.

As such, payments made by a user to a shop owner can occur instantly without asking for confirmation to a middle-man. Sending and requesting money can be done in the same way. In the traditional model, the technical team is distinct from the managerial one whereas for a blockchain-based local currency, the technical and managerial are regrouped under one entity that is the administrator. For the technical aspect, by not depending on a private I.T. solution, issues can be directly addressed between the users and the administrator of the local currency.

Becoming a cost-competitive alternative

Compared to other digital solutions in the complementary currencies marketplace nowadays, the blockchain may appear as a more cost-competitive alternative. A well-known solution to community currency management is online and mobile banking software *Cyclos*. The costs of using a private software such as Cyclos can amount to 8000 euros per year.[15] This could represent an extremely high investment for small communities. In addition to the cost, third-party centralised systems are vulnerable to cyber-attacks and most important, local currency communities are heavily dependent on them if they wish to add specific features (additional cost) or encounter technical issues.

Com'Chain,[16] a private blockchain-based solution operating on Ethereum, currently manages the e-Leman local currency in France and Switzerland. In the case of the Eusko, the company offers their service with a cost of up to 20 000 euros per month if the entire service is delegated to the company, according to Pinos (2019). This shows that the application of the blockchain has reached the local currency communities already although in the case of the e-Leman, the currency also exists in the form of QR-coded notes[17] and the digitisation is managed by a private entity in a lucrative way. However, as the blockchain is becoming more mainstream, and if it emerges from the local authority, or communities with non-lucrative objective to serve the public interest, we can expect the possibility of a much lower cost solution to implement a blockchain-based solution in the very near future since the open-source nature of the technology allows for greater flexibility, rules and system designs.

[15] https://www.cyclos.org/products/price-list/ Their price vary according to the size of the project (number of users and turnover) and there are additional fees for the installation, the licence and the yearly maintenance of the platform.

[16] https://com-chain.org//

[17] https://www.ripess.eu/e-leman-a-local-blockchain-currency-in-switzerland-and-beyond/

Increasing legitimacy and credibility for stakeholders

One of the many challenges that local currencies face is the lack of impact measurement tools to support their legitimacy amongst stakeholders and the public (Fare and Ahmed, 2017; Place and Bindewald, 2015). It has always been difficult to measure the efficacy, let alone the actual impact of a local currency initiative over the community due to several factors that are sometimes inherent to the ways the project is implemented. Digital tools help to automatise various tasks and ease the record-keeping work for many local currencies but it usually comes at the cost of third-party dependency and transparency issues. With a blockchain-based local currency, records of transactions are publicly accessible and because of its immutable property, stakeholders can fully trust what they see and act accordingly. The open access feature also implies open collaboration from potential stakeholders that may want to participate and improve the local currency community.

4.2 A model of blockchain-based local currency

A blockchain associated to a local currency is introduced in the usual interactions of the community's stakeholders: administrator/issuer of the currency, its users, and its member shops, with whom miners/validators interact. The incentives of this community are intrinsic for the most and have no reason to change radically with the introduction of the blockchain.[18] Only the validation of transactions and the nature of incentives and payments for miners/validators differ from the case where a centralised system is used. For transparency and traceability purposes, the blockchain-based solution for local currencies should be made public, and could employ a PoW or a PoS consensus protocol. It would interact with other members of the community as follows:

The administrator of the currency and its interaction with validators

Local currencies are usually administered by people who act as volunteers or through local governments. This form of governance could be maintained with the introduction of a blockchain. The administrator issues at a fixed exchange rate the local currency in counterpart of the legal tender. It also operates the retro-conversion of complementary currency into legal tender, for member shops (participants of the local currency network) who wish to. The administrator team is complemented by I.T. specialists who ensure the technical and technological aspects of the digitisation. In the same way, the administrator defines and modifies if necessary the conditions of admission for member shops in the community. The amount of rewards is also controlled by the administrator. For the reserve of legal tender, the administrator should be place it preferably in a mutual bank for ethical purposes. The management and technical teams constitute the administrator agent.

[18]For-profit local currencies also exist (such as the Renoir in Cagnes-sur-Mer in France) but they are infrequent as most initiatives are centred around societal and environmental objectives rather than economic ones.

Miners or validators

Miners or validators could be or not be members of the community associated to the local currency project. When they are members, they generally have intrinsic incentives like improving the security of the system. They are in this case comparable to the developers of Open Source communities: their contribution is motivated by signalling effects on job markets, or by their implication in other initiatives of the local government. They could also be physically distant from the local complementary currency ecosystem and operate simultaneously as miners or validators of other blockchains: in this case, their motivation would probably be more extrinsic and associated to the gain generated by the rewards they expect from mining or staking.

Users

Users are citizens who live in or near the geographical area in which the local currency is accepted. They may use the local currency in a regular or irregular manner according to their convictions in the values that the local currency conveys, promotes and protects. They are motivated by the objectives of the community which could be to develop short distribution channels, fair trade, organic productions, *...etc.* They cannot convert local currency into legal tender and have to pay a very small fee for each transaction. This fee is a part of the rewards served to miners and validators.

For users, the local currency is stored and managed in a digital wallet. A private and public key will be issued for each user, and the operation principles are the same as a crypto-currency wallet. Via the digital wallet application, users can convert legal tender into local currency via credit card and bank transfer, pay merchants, and transfer local currency from peer to peer.

Member shops

Member shops (grocers, mini-markets, clothing stores, pubs, restaurants, *etc*) are located in the area of circulation of the local currency and accept the local currency as a means of payment. They are authorised to convert the local currency into legal tender if they sign and adhere to a chart of values defined by the local currency community. This commitment provides the intrinsic motivation for users. For instance, they commit to be respectful of the environment, to sell local and/or organic products, to promote short distribution channels, to reduce and prevent waste, to improve their packaging design, *etc.* The conversion from local currency to legal tender entails a small fee percentage, which will complement transaction fees from users to fund validators' rewards. The idea behind the fee is to encourage B2B transactions so that the currency keeps circulating in the community.

Payments

When the motivations of miners/validators are intrinsic, rewards are only optional. On the contrary, when they are are extrinsic, they must be adapted to the type of con-

sensus protocol.[19] With the PoW or PoS protocol, a lottery or a contest, combined with another criterion (the performance of mining equipment or the validator's stake), determines which miner/validator will be paid. With this system, the total validation cost, *e.g.* the financial contribution of the community to the validation activity does not depend on the number of miners/validators but only on the number of transactions/blocks to validate. However, the expected payment for each miner/validator decreases as the total number of miners/validators increases since their probability to win the lottery or the contest depends on the number of total participants in the network.

Each time the rewards proposed by the administrator increase, there is an entry of participants in the network, and the opposite occurs when the rewards decrease. Given opportunity costs and other costs supported by miners/validators, the number of effective miners/validators then increases with the rewards. The blockchain network must be sufficiently active to be efficient and reliable: this creates a lower bound for a decrease of rewards and generates a trade-off for the administration between cost and reliability.

How does the model operate?

The administrator has the leadership and the authority to make decisions. It evaluates the reactions of other stakeholders to its possible choices: what kind of commitments are appreciated by users, which ones are enforceable, what terms for the trade-off between cost and reliability of the blockchain application? In time, given in particular the number of effective transactions but also the evolution of the technology, the administrator could adjust fees, reconversion penalties and the amount of rewards. This control has its specificities depending on the consensus protocol employed.

Proof of Work protocol

In the case of a PoW validation system, the computational power of miners is important both for validating transactions, and for determining the individual probability for each participant to win the rewards. Now, the computational power of each miner evolves in time with technological progress and costs of equipment. The number of potential miners also evolves because of different circumstances as the available existing of opportunities in other I.T. activities. These changes could modify in time the number of effective participants to a given blockchain. If this question is not so relevant for crypto-currencies where the number of miners is rather large, it could become critical for local currencies if they are not constituted in networks. It is then important to control that technological innovations do not create distortions such that the heterogeneity between the computational power of the most and the less efficient miners increases during time. All increase of the heterogeneity among miners could crowd out the less efficient participants, weaken the reliability of the system and increase the risk of attacks.

[19] In many situations, public blockchains would host miners/validators who have different motivations: this context requires to address the payment question in a more serious way.

It is inefficient for an individual miner to spend energy to create malicious blocks, since they can be verified by other miners and a block is considered valid only if there is a majority of miners who confirms it. However, if malicious miners pool their mining capacity together (which is the equivalent of voting power) sufficiently to obtain at least 51% of the total network power, they could agree to vote or validate on whatever they wish to. In the case of Bitcoin, the share of mining pools is publicly accessible via https://www.blockchain.com/pools. We could imagine the same situation for a single or a network of local currencies where miners have access to information about their blockchain network at all time. This is known as the 51% attack which remains an important threat in the PoW protocol. The income generated by those attacks may be limited to a single local complementary currency but if many local currencies are associated to form a network, it becomes much more interesting for malicious miners to conduct an attack as they can have access to a more important amount of local currency that can be spent or converted in legal tender.

To prevent this risk, the administrator first needs to maintain the rewards at a sufficiently high level. This control regulates the concentration of the miners' network. If this concentration increases, it is indeed easier for the most efficient participants to constitute a pool that can control 51% of the network power. The control could however be imperfect if it is limited to the adjustments of rewards. Each member of the blockchain network can contribute to the validation of the transactions of many local currencies and the administration of one single currency has only a limited influence on the global structure of the network. This fluidity of the miners' network must encourage administrators to cooperate in the determination of rewards and to coordinate their actions, including different forms of monitoring.

Proof of Stake protocol

In the PoS protocol, the validator must first convert in the local currency the revenue (in legal tender) it intends to transmit to the future. In this case, the heterogeneity of the participants is no longer determined by the computational power of their mining equipment but by their capacity to constitute deposits, and by their preference for the present which determines for most the cost of opportunity associated with those deposits. Wealth or liquidity and time preference then determine the decision of each potential participant to contribute and their probability to win the lottery and the rewards. All things equal, increasing the rewards also increases the size of the blockchain's network, and again, the smaller the size of a given local currency, the less efficient the adjustment of rewards.

However, this positive effect of rewards is less decisive in the PoS case than in the PoW one. Increasing the number of participants still increases the rapidity of the mechanism but it does not help radically to prevent attacks. In the PoS case, attacks are indeed not generated by pooling mechanisms buy are for the most individual initiatives. They are associated to the possibility of each validator to mint (bet on) several blocks (branches) simultaneously and consequently increase their probability of winning. When

a chain has forked for different reasons, each validator has indeed the possibility to mint several blocks at the same time, without increasing its deposit, and to increase its probability to be chosen by the lottery. It is reasonable to think that, in this case also, wealth or liquidity, and opportunity costs associated to the preference for the present, are also decisive in the propensity for a given participant to validate simultaneously many blocks and to increase the risk of success of a malicious attack. Only an adapted and costly monitoring of the system, associated with strong penalties for each deviating behaviour, could perfectly be a remedy to this risk.

Another difference between the risks of the two validation systems is that the *nothing at stake* case does not depend on the size of the network. This risk depends on the amount of rewards but also naturally on the number of transactions to validate. Mechanically, the reliability of the PoW then increases with the volume of circulation of the local currency or of the network of local currencies to which a given blockchain is associated. This remark seems to indicate that, all things equal, the smaller the local currency community, the greater the interest to adopt a PoS protocol.

4.3 Concerns for blockchain-based local currencies

Common misconceptions of the blockchain

The blockchain is often perceived as a disruptive technology, one that will radically change the ways we conduct business. In fact, it should be considered more as a foundational technology that would, in contrast to a disruptive one, not attack traditional business models but rather provide the foundations for our economic systems[20] (Iansiti and Lakhani, 2017). In this sense, the blockchain can be seen as a stepping stone for solving issues that traditional solutions fail to address, *e.g.* immutability, decentralisation...*etc.*

The second misconception and probably the most common one is the systematic association of the blockchain to high electricity consumption and environmental issues. This concern stems from one particular consensus protocol that is used by Bitcoin and a handful of other crypto-currencies: the PoW protocol. Because whenever the blockchain is mentioned, people tend to think about Bitcoin as well and every consequence derived from the latter. In reality, a blockchain can operate withtout the PoW protocol as there exist other consensus protocols can could ensure the same security and validation roles as the PoW such as the PoS and the Byzantine Fault Tolerance (BFT) protocol.

Objectives and development of local currencies

While blockchain is not the panacea to all the problems a local currency might face,

[20] It can be compared to the transmission control protocol/internet protocol (TCP/IP) (Iansiti and Lakhani, 2017).

it surely does alleviate some of them and provides a reflection room for complementary solutions. For instance, Pinos (2019) found that the blockchain is not suitable for the Eusko local currency for now since it does not create public value and the project itself does not require a technical solution to address its issues. In fact, the novelty of the technology constitutes one of the reasons that made the managers reject the technology, for now. This example provides insight on a local currency that does not need the blockchain to solve their issues even though it sparked some interest for the managers and the author of the study. In contrast, some local currencies have experienced or showed interest in a blockchain-based solution such as the Liverpool Pound, operated by Colu[21], the Monnaie Léman and Racine[22], run by Com'Chain. Because each local currency project has different objectives and develops at its own pace, the needs and size are important factors that will influence the consideration of a technical solution that is the blockchain.

5 Alternative consensus protocols

Operating a blockchain with a hybrid consensus protocol could also be a possibility and should be explored further in the context of local complementary currencies (*e.g.* some crypto-currencies such as Peercoin and Dash have a hybrid protocol). Issues inherent to the current PoW and PoS protocols call for further research on consensus models. The literature includes studies of alternative forms of the PoS protocol *s*uch as the Casper protocol (Buterin and Griffith 2017) and the proof of activity or PoA (Bentov, Gabizon and Mizrahi 2014).

5.1 Casper protocol

The Casper protocol proposed by Buterin and Griffith (2017) is a consensus model designed to allow upgrading of an existing and operating PoW chain through implementation of a PoS-based system. The Casper protocol was proposed to replace the current PoW system in the Ethereum blockchain. It includes some interesting new features which fill some of the gaps in existing consensus models such as accountability (imposing a penalty equal to the whole of the malicious validator's deposit, with two slashing conditions), setting dynamic validators set and more effective protection against reversion attacks. The notion of accountability implies that the size of the deposits determines the security of the protocol not the number of validators. In Casper, the concepts of finalised and justified checkpoints are introduced: every block which is a multiple of 100 from the original block can become a checkpoint, and the guiding rule is always to follow the chain with justified checkpoint at the highest block height. For validators who that go offline intentionally or unintentionally, the protocol proposes implementation of an

[21] The project stopped in 2019.

[22] The Racine has announced on their website that an electronic version of the currency running on the blockchain will be available soon. Com'Chain included on their website the Racine as one of their clients.

inactivity leaks system. It works by draining a proportion $d = D$ x p - where D is the deposit amount and $0 < p < 1$ - of the offline validators until the online ones take them over and become a supermajority, with the right to make decisions and keep the system functioning. The question of whether to burn the drained funds or return them to the validators needs more discussion and economic justification. However, Casper does not resolve the 51% attack problems.

5.2 Proof of Activity (PoA)

Bentov, Gabizon and Mizrahi (2014) focus on the problem of depletion of a physical scarce resource posed by the PoW system to maintain its security and operability. They propose the idea of a chains of activity (CoA) concept which is an extension of the proof of activity (PoA) protocol (Bentov, Lee, Mizrahi and Rosenfeld, 2014) and employs a hybrid PoW / PoS system which ultimately employs the follow-the-satoshi method to achieve consensus.[23] Although it employs the PoW system to generate coins during the early stages of the currency to solve the fair initial coin distribution problem posed by the PoS system, the protocol stops the PoW system once a defined number of blocks has been mined. The differences between the CoA and Bitcoin mining are unproblematic readjustment so the block generation interval is not constant but requires definition of a minimum time gap (*e.g.* at least one minute gap between two blocks), fixed coin production costs (electricity and equipment) independent of overall network mining power, a number of blocks after the mined coins that can be spent that is greater than 100 to avoid an inflationary early phase, and a coin value pegged to its production costs. In the case of the PoS part of the CoA system, stakeholders are not allowed to double sign (those that do have their coins confiscated) which is an important difference compared to the PeerCoin system. The authors claim that the CoA protocol is more secure and has a more detailed design which makes it more resistant to bribe attacks, dishonest collusion and majority takeovers than the Bitcoin and Peercoin systems.

6 Conclusion and discussion

The study of blockchain applications in local complementary currency systems is an emerging field which is attracting the interest of researchers and practitioners around the world. Since complementary currency systems are being digitised, blockchains could provide communities with substantial benefits including the absence of intervention from a bank or financial intermediary. In this paper, we analysed two blockchain consensus protocols. They could be implemented in an isolated local complementary currency system or used to manage a number of local currency systems with the collaboration of the administrators of each currency. The need for reliability and trust on such systems with

[23] The *follow-the-satoshi* method derives from the PoA protocol and consists mainly of a lottery which determines that the creator of the next block is the owner of a randomly selected smallest unit of the currency. The selection process is described in detail in their article.

complex interactions calls for a variation in the design of the consensus protocol, where the administrator adjusts the amount of rewards and the miners and validators are still the sole ensurers of the validation process for the network.

Each of the consensus protocols examined has a different set of properties. The PoS protocol does not involve high costs and encourages validators to hold local currencies thereby fostering their adoption. Attacks on this system are possible but are to some extent limited and are relatively easy to control or tolerate. A sufficiently severe sanction would deter attackers. The system seems to be adapted to small sized experiences. Future work could also consider other derivations of the PoS protocol like the delegated PoS [24] (dPoS).

In the PoW, the variation in the mining capacity distribution has an effect on the number of end users. If their number is limited, the PoW protocol presents more risks with 51% attacks more likely to be launched by - fairly small sized - pools of miners. An increased number of users also augments the risk for attacks, but the effect is countered by an increase in the number of miners, which strengthens the network security and dampens malicious behaviours. Controlling the amount of rewards produces the same effect. The PoW seems to be more adapted for large sized experiences. Therefore, besides the environmental concerns caused by the energy-intensive validation process of the PoW, risks of attacks and collusions could be other reasons to consider and to seek for alternative consensus protocols such as for example.

[24] Used by other crypto-currencies such as Ark, Bitshares, EOS, Lisk and Peercoin. See appendix 2 for a list of other protocols employed by crypto-currencies.

Appendices

Appendix 1

Proof of Work	Pure Proof of Stake
Auroracoin	NavCoin
Bitcoin	Neblio
Bitcoin Cash	Nxt
Bitcoin SV	Okcash
DigiByte	Qtum
Dogecoin	
Ether	
Litecoin	
Mazacoin	
Monero	
Namecoin	
Primecoin	
Tether	
Verge	
Vertcoin	
Zcash	

Table 2. List of some of the crypto-currencies that use the proof of work and the pure form of proof of stake protocols

	PoW	**PoS**
Security ensured by	Miners	Minters / validators / forgers
Block creation	By capacity of mining equipment	Deterministic: by amount of deposit
Type of rewards	Block bounty + *transactions fees*	Transactions fees
Units creation	Degressive	None

Table 3. Main differences between a PoW and PoS protocol

Appendix 2

Crypto-currency	**Protocol**
Ark	Delegated POS (DPoS)
Bitshares	DPoS
Dash	PoW & Proof of Service
EOS	DPoS
Gridcoin	PoS & Proof of Research
Lisk	DPoS
NEM	Proof of Importance
NEO	Delegated Byzantine Fault Tolerance (dBFT)
Peercoin	DPoS
Reddcoin	PoS-Velocity (PoSV)
Ripple	Ripple Protocol
Stellar	Stellar Consensus Protocol (SCP)

Table 4. List of crypto-currencies that use other consensus protocols (non-exhaustive)

References

Bentov, I., Gabizon, A., and Mizrahi, A. (2016, February). *Cryptocurrencies without proof of work*. Paper presented at the International Conference on Financial Cryptography and Data Security (pp. 142-157). Springer, Berlin, Heidelberg.

Bentov, I., Lee, C., Mizrahi, A., and Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract] y. *ACM SIGMETRICS Performance Evaluation Review, 42*(3), 34-37.

Blanc, J., and Fare, M. (2018). Pathways to Improvement. Successes and Difficulties of Local Currency Schemes in France since 2010. *International Journal of Community Currency Research, 22*(Winter), 60-73.

Blanc, J., and Fare, M. (2016). Turning values concrete: the role and ways of business selection in local currency schemes. *Review of Social Economy, 74*(3), 298-319.

Buterin, V., and Griffith, V. (2017). Casper the Friendly Finality Gadget. *arXiv preprint*.

Catalini, C., and Gans, J. S. (2016). *Some simple economics of the blockchain* (No. w22952). National Bureau of Economic Research.

Collomb, A., and Sok, K. (2017, July). "Blockchain" : une révolution monétaire et financière ?. *Alternatives Economiques, 75*.

Conley, J. P. (2017). *Blockchain Cryptocurrency Backed with Full Faith and Credit* (No. 17-00007). Vanderbilt University Department of Economics.

Fare, M., and Ahmed, P. O. (2017). Why Are Complementary Currency Systems Difficult to Grasp within Conventional Economics? *Interventions Économiques, 59*.

Groppa, O. (2013). Complementary currency and its impact on the economy. *International Journal of Community Currency Research, 17*(A), 45-57.

Guegan, D. (2017). Public Blockchain versus Private blockhain. *Centre of Economics of the Sorbonne*.

Guo, Y., and Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation, 2*(1), 24.

Hajdarbegovic, N. (2014). Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack. *CoinDesk*.

Hukkinen, T., Mattila, J., Ilomäki, J., and Seppälä, T. (2017). *A Blockchain Application in Energy* (No. 71). Retrieved from the Research Institute of the Finnish Economy.

Iansiti, M., and Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118-127.

Iwasaki, A., Ueda, S., Hashimoto, N., and Yokoo, M. (2015). Finding core for coalition structure utilizing dual solution. *Artificial Intelligence*, 222, 49-66.

Jaag, C., and Bach, C. (2017). Blockchain technology and cryptocurrencies Opportunities for postal financial services. *In The Changing Postal and Delivery Sector* (pp. 205-221). Springer, Cham.

King, S., and Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-published paper.*

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027-1038.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*

O'Dwyer, K. J., and Malone, D. (2014, June 26-27). *Bitcoin mining and its energy footprint.* Paper presented at the 25th IET Irish Signals & Systems and China-Ireland International Conference on Information & Communities Technologies (ISSC/CIICT), Limerick.

Ølnes, S., Ubacht, J., and Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355-364.

Pilkington, M. (2016). Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.

Pinos, F. (2019). How could blockchain be a key resource in the value creation process of a local currency? A case study centered on Eusko, presented at the 5th Biennial RAMICS International Congress, Hida-Takayama, 11th-15th September 2019.

Place, C., and Bindewald, L. (2015). Validating and improving the impact of complementary currency systems through impact assessment frameworks. *International Journal of Community Currency Research, 19*, 152-164.

Schwartz, D., Youngs, N., and Britto, A. (2014). The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper, 5.*

Sullivan, C., and Burger, E. (2017). E-residency and blockchain. *Computer Law and Security Review, 33*(4), 470-481.

Tichit, A., Lafourcade, P., and Mazenod, V. (2017). Les monnaies virtuelles décentralisées sont-elles des outils d'avenir. *HAL-SHS Archives.*

Wolfond, G. (2017). A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review, 7*(10), 35-40.

Zhang, E. (n.d.) A Byzantine Fault Tolerance Algorithm for Blockchain. *NEO Documentation.*