Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies

Sothearath SEANG* Dominique TORRE*

January 2919

Abstract

This paper examines with the help of a theoretical setting the properties of two Blockchain consensus protocols namely the Proof of Work (PoW) and the Proof of Stake (PoS) in the management of a local (or networks of local) complementary currency(ies). The model includes the control by the issuer of the currency of the advantages derived from the use of local complementary currencies by heterogeneous consumers and the determination of rewards for heterogeneous validators and miners. It also considers the resilience of the protocols to malicious attacks conducted by an individual or pools of validators/miners. Results exhibit an interest in the PoS protocol for small communities of local complementary currency, whereas the PoW appears to be more advantageous when the size of the communities increases.

JEL Classification: E42, D91, L86, O31

Keywords: payment systems, heterogeneous agents, Proof of Work, Proof of Stake, blockchain, local complementary currencies

*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

In recent years, the blockchain technology has sparked a lot of interest around the world and its applications are being tested across many sectors such as finance, energy, public services and sharing platforms. Although the technology is still in its immature state and therefore going through numerous experiments, the potentially diverse benefits and opportunities derived from its decentralised and open-to-innovation nature have drawn much attention from researchers and investors. As a foundational technology[1], its mainstream adoption would take a lot of time and require the degree of novelty and the amount of technological, social and regulatory complexity efforts needed to coordinate it, to reach a sufficiently high level (Iansiti and Lankhani, 2017). Furthermore, systems with complex interactions also call for stronger control and reliability. Local payment systems are no different than that and it is of our interest to study the implementation of the blockchain technology to these systems.

The objective of this paper is to study the properties of two blockchain protocols, the Proof of Work and the Proof of Stake protocol. Their primary function would be to validate and clear transactions in (or among) local systems of digital complementary currencies. The Proof of Work is the pioneering one and still the most popular given its application in Bitcoin and other crypto-currencies. So far it appears as the most reliable and could be adopted in the case of the management of a local complementary currency. What about the properties of the Proof of Stake consensus protocol with heterogeneous agents, both on the sides of users and validators? The simplified theoretical setting presented in this paper attempts to answer this question. The model that we develop integrates three types of agents. (i) End users of local complementary currencies, who are motivated by the advantages associated to the use of the currency. (ii) The issuer/administrator of the local complementary currency, who determines the nature and amount of the advantages, and in charge of the conversion of official money into local currency. Finally, (iii) validators or miners, who confirm that a given payment is valid and clear the accounts of users. Because no system is perfect, it would appear relevant to also study the case in which malicious validators and miners decide to conduct an attack on the two protocols.

The theoretical results of the model point out the contrasting interest of the two protocols. The Proof of Work entails the creation of additional units of complementary currency which add up to the previous units held by users. The costs of these additional units are borne by the issuer of the currency. Attacks are more likely to occur when the size of the community of users is small. The Proof of Stake has opposite properties. It does not involve the creation of new units of money and attacks are less likely to occur when the size of the community is small. Its adoption seems more appropriate in the case of local complementary currencies.

[1] As opposed to a disruptive technology, the blockchain will not attack traditional business models and but instead, it would lay new groundwork for our economic systems. It can be compared to the transmission control protocol/internet protocol (TCP/IP) (Iansiti and Lankhani, 2017).

The paper is organised as follow. The next section presents the objectives of local complementary currencies and highlight the motives behind their digitisation. Section 3 provides an overview of the Blockchain technology by exposing its basic concept, applications in different sectors and how consensus protocols constitute the backbone of the system and ensure its operability. Section 4 introduces a local currency benchmark model via a Blockchain technology. Section 5 and 6 analyse respectively models of local currency with a Proof of Work and a Proof of Stake protocol. Section 7 concludes, opens the discussion and provides directions for further research.

2 Local currencies and digitisation

Objectives and management of local currencies

A local complementary currency is a payment system specific to a particular area of a country *e.g.* a town, a city, an agglomeration, a department. They are designed to help achieve local economic and/or social objectives such as revitalising local businesses in the city centre, strengthening social relations, promoting of local identity, production and short channels of distribution, fostering sustainable behaviours and helping unemployed people with a parallel activity paid in local currency. For instance, through their multiplier effect, local complementary currencies can reduce unemployment and increase social well-being of consumers (Della Peruta and Torre, 2015). In general, merchants that accept the local currency must adhere to a charter that contains the code of conduct of the local currency association which usually guarantees ethical and sustainable practices from its members as well as the quality of products sold in the community to end users (Blanc and Fare, 2016). In the French Basque country, merchants that accept the Eusko local currency (which is the most important local currency in Europe in terms of money supply and number of users) as a payment must display their products in both French and Basque language because one the missions of association is to promote the use of its local language[2].

The issuer of a local currency is not limited to a non-profit association but can also be a local government, a corporation of traders[3] or and the management of the currency is done by this issuer or delegated to a financial agent. The management includes printing the notes when the chosen form is fiat money, providing conversion services through exchange offices (usually merchants that accept the local currency) and determining the properties of the local currency *i.e.* additional advantages provide to the users such as
10

When a local currency is in the form of notes, security features such as special watermarked papers and bubbles patterns make them difficult to be counterfeited and therefore, ensure their authenticity. In general, there is a fixed exchange rate between the local and the official currency but different methods can be implemented in order to avoid its

[2] http://www.euskalmoneta.org/statuts/
[3] In the case of Europe.

hoarding.[4].

The association generally deposits the official currency converted by users at a partner bank. One way to cover the operating expenses of the local currency is to charge a percentage fee for merchants when they convert the local currency back to official money. This could be perceived as a constraint to the adoption of the local currency, but it is also another incentive for merchants to find business partners or ways to re-inject the money back into the local circuit.

Although it is a type of *complementary* currencies, meaning that it is used in parallel with the official currency of a country, a local currency is different from other types of complementary currencies such as Local Exchange Trading Systems (LETS), Time Banks and virtual/crypto-currencies[5].

Digitisation of local currencies

Some local complementary currencies only exist in digital form, for instance the *SoNantes* currency in the Loire Atlantique county in France and the *Colu* in Liverpool in the United Kingdom. It is more challenging to manage accounts, make settlements and provide a sufficient level of trust of such currencies. They are usually administered by one or a few central entities like a bank or an I.T. firm: SoNantes is managed by the *Crédit Municipal bank* of Nantes and *Colu* by the firm that goes by the same name as the currency. Another well-known solution for community currency management is the online and mobile banking software *Cyclos*. The costs of using a private software like Cyclos can amount up to 6000 euros annually[6] and could represent an extremely high expense for associations, especially smaller onces. Beyond the issue of cost, third-party centralised systems are also highly vulnerable to cyber-attacks and most importantly, local currency communities are heavily dependent on them.

Therefore, the motives behind the digitisation of a complementary currency could be multiple: elimination of paper printing costs, reduction of administration costs and reliance on third-parties, increased likelihood of attracting younger users and all the potential benefits and opportunities that can be derived from the use of a decentralised management solution like the blockchain[7]. In recent years, we observe that a considerable number of local currencies originally introduced in fiduciary form are now transitioning to a digital version like the *Renoir* in Cagnes-sur-Mer. Table 1 provides an overview of local currencies transitioning or in the process of transitioning to a digital form and those who are already in digital form in Europe. It is reasonable to imagine decentralised solutions

[4] Some local currencies are melting currencies *i.e.* a note will lose x% of its value if it is not spent in a given period of time (a few months usually) so there is an incentive for the holder of the notes to spend them as fast as possible, which in turn increases the velocity of circulation of the currency and helps to reach its objectives.

[5] See Tichit, Lafourcade and Mazenod (2017) for a description of criteria distinguishing the different types of complementary currencies.

[6] https://www.cyclos.org

[7] The claimed advantages of the blockchain are briefly exposed in Section 2.

to manage such currencies. Banks or other financial agents could be involved in these solutions (with a possible monetary motivation) but will not play the role of a central authority. The application of the Blockchain through different consensus protocols could prove relevant for this purpose.

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 & Digitising*
Grama	S. Coloma de Gramenet	Spain	Digital
Kingston Pound	Kingston	United Kingdom	Digital
Léman	Lake Geneva	France/Switzerland	Notes & Digital
Liverpool Pound	Liverpool	United Kingdom	Digital
Pive	Franche-Comté	France	Notes & Digitising
Renoir	Cagnes-sur-Mer	France	Notes & Digitising
RES	Girona	Spain	Digital
Sol-Violette	Toulouse	France	Notes & Digitising
Sonantes	Loire-Atlantique	France	Digital
Stück	Strasbourg	France	Notes & Digitising
Totnes Pound	Totnes	United Kingdom	Notes & Digital
Trèfle	Périgueux	France	Digital
Turuta	Vilanova i la Gellrù	Spain	Digital

Table 1. Non-exhaustive list of local complementary currencies in digital form

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

3 The Blockchain technology

Overview and applications of the technology

A blockchain is a General-Purpose Technology (GPT) and a type of Distributed Ledger Technology (DLT) that is highly secured by cryptography[8]. 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 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

[8] A DLT is a record-keeping system in which all or some of its users possess a copy of the ledger. Cryptography is the science that encompasses mathematical codes and techniques to create secured communication with unknown third parties (Pilkington, 2016). A blockchain is a cryptographic-based DLT.

and the sustainability of the system[9]. Reaching a global agreement on the blockchain is made possible by the implementation of a consensus protocol that dictates the rules by which the users should play and abide.

The blockchain technology is being studied and tested in many sectors including finance, energy, cybersecurity, healthcare, government services and e-residency. Wolfond (2017) explained how the implementation of a decentralised and collaborative identity verification model based on the blockchain that possesses certain characteristics could allow for a substantial reduction of costs and benefit businesses and citizens in healthcare and government services in Canada. Kshetri (2017) also took the example of application of the blockchain to the healthcare industry to illustrate the potential improvements in terms of security and privacy and additionally presented the possibilities of the technology to address some key challenges with 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 architecture for decentralised energy systems (Hukkinen, Mattila, Ilomäki and Seppälä, 2017). Sullivan and Burger (2017) examined the legal, policy and technical implications of the development of e-Residency in Estonia[10] that allows for minimal identity requirement and authentication for anyone in the world to engage in a range of economic activities in the country.

From an economic perspective, Catalini and Gans (2016) discussed how the reduction of verification and networking costs by the blockchain system change the types of transactions that are supported in the economy. They also analysed the implications for intermediation and argued that although the market power of intermediaries will be drastically diminished with the implementation of the blockchain, they would remain necessary for some offline tasks that still require human verification. Ølnes, Ubacht and Janssen (2017) conducted an assessment of the potential blockchain benefits found in the literature and classified them in different categories: strategic (transparency, fraud and manipulation avoidance, corruption reduction), organizational (increase of trust, predictive capability and control, transparency and suitability, clear ownerships), economical (costs reduction, spam resilience), informational (integrity and higher quality of data, human errors reduction, access to information, privacy and reliability) and technological (resilience, security, persistence and irreversibility, energy consumption reduction). They also found that having robust governance models is a condition for the blockchain to yield benefits.

In the banking industry, Guegan (2017) addressed some questions concerning the use of private blockchains to reduce costs, increase security and simplify bank operations. He

[9] 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 the core value in the blockchain so we will only consider the case of a public blockchain for the rest of the paper.

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

emphasises the fact that the current benefits of the blockchain are more applicable to a public model, hence a decentralised one. Guo and Liang (2016) explored the potential advantages that the blockchain can offer in clearing and credit information systems as well as the regulation, efficiency and security challenges for implementing the blockchain in the Chinese banking industry. They concluded that those problems will be solved over time and the technology will be somehow incorporated in the future. For payment systems, Ripple is an interbank solution that provides high speed transactions (across the world in seconds), transparency and simplicity for users. It seeks to create a universal payment protocol and has a digital currency for transactions on the blockchain called XRP (Schwartz, Youngs and Britto, 2014). Similarly, Jaag and Bach (2016) presented the possibilities of using the blockchain for postal financial services to improve financial inclusion and the creation of a postal crypto-currency to counter the high volatility that plague most crypto-currencies. By backing coins with a national currency like the US dollars, CryptoBucks and Tether (Conley, 2017) seek to combat the high market volatility of crypto-currencies and establish faith, ease of use and financial connections to the outside world for consumers. In terms of creating contracts and programs on the blockchain, the Ethereum blockchain allows its users to build, buy and sell smart-contracts and its currency Ether, is the second largest crypto-currency in terms of market capitalisation[11].

The Proof of Work and Proof of Stake consensus protocols

The first blockchain application employs the Proof of Work (PoW) consensus protocol as the backbone of the system and was introduced in 2008 by Satoshi Nakamoto to the Bitcoin network[12].

In the PoW protocol, it is the combination of cryptography and computational power that creates consensus and ensures the authenticity of 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[13]. To prove that a block is valid and that work has been done, the nodes in the network (called miners) use their computational power to validate transactions (*i.e.* verify that a sender has enough funds and is not double-spending) and most importantly compete with each other in a race to

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

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

[13] For Bitcoin, the block size is around 1 megabyte and its generation rate is around 10 to 12 minutes, the current bounty is 12.5 bitcoin and halves every 210,000 blocks or 4 years, the money supply is capped at 21 million Bitcoins and the difficulty of the network is readjusted every 2016 blocks or a fortnight. The PoW design can greatly vary among crypto-currencies. Litecoin for example, has a limited money supply of 84 million Litecoins and has a block generation rate of around only 2.5 minutes. This frequency may be more suitable for small transactions (like buying coffee or bread) that require only a few confirmations from the receiver (the number of blocks following the one containing the transaction to prove that the operation is authentic.

solve cryptographic problems imposed by the protocol[14]. This process is called mining. 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 vary among the users that make the transactions) that he / she chooses 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 as legitimate when other miners continue working on extending the chain from block X. When a chain splits, miners should always choose the longest chain since it has the most work done. Miners can work on multiple chains if they wish to but to the detriment of dividing their computational power.

Although it resembles a lottery, the computational power that a miner possesses plays a deterministic role in the PoW protocol as the bigger the capacity to generate guesses (measured in hash per second), the higher the probability to find a solution. The computers run at full capacity all day long, therefore the mining process consumes a considerable amount of electricity. That makes the PoW a extremely resource-intensive model: in here time and energy serve as proofs that work has been done. In 2014, the total power consumed by the Bitcoin network was equal to Ireland's electricity consumption (O'Dwyer and Malone, 2014). This protocol was approved by users and miners and widely adopted by other crypto-currencies by which it became popular and seen as a successful model. However despite its success, the future of the PoW remains unclear, particularly because it was not initially designed to manage a speculative asset that Bitcoin has become.

Like any digital system, blockchain consensus protocols present vulnerabilities. In theory, the PoW system can be attacked if a miner alone or a collusion of miners who possess more than half of the network total mining power. This is also known as the 51% attack. In practice, attackers would create their own secret chain and broadcast it to the network once it gets longer than the honest chain (other miners would consider this chain valid as it is the longest and move on to work on subsequent blocks) in an attempt to double-spend or compromise the whole system. At the start of 2014, the *G.HashIO* mining pool was about to reach 51% but miners left the pool over fears of the attack (CoinDesk, 2014).

An alternative to the PoW is the Proof of Stake (PoS) protocol. It confers the decision power to stakeholders (also called minters or validators) of the system. Unlike the PoW in which everyone can become a miner and participate in the process, not everyone can join the network in a PoS protocol. Ownership of a currency or having a deposit in the network allows the nodes (validators) to participate in the minting process (*i.e.* validating transactions and creating blocks.) No computational power is required to solve

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

cryptographic puzzles like in the PoW scheme. There are no rewards under the form of a money creation process: validators collect fees from users and are paid from them like a usual intermediary.
Since validators only get transaction fees, the scenario in which validators create empty blocks could be avoided[15] as they are incentivised to include the maximum number of transactions in order to maximise their gains. Because the money supply must be issued since the beginning (no money will be created in this protocol), the problem of an initial fair coin distribution arises. If the PoS includes a selection process for validators (the greater the stake, the higher the probability of being selected as a creator of the next block), then additional balancing mechanisms are necessary to mitigate the risk of rich validators getting richer. PeerCoin is a crypto-currency that employs a PoW scheme for its initial mining phase and a PoS-based protocol for validating transactions and rewarding its validators (King and Nadal, 2012). It uses the *Coinage* concept and a stochastic PoS minting process[16].

One of the problems that the PoS faces is the *nothing-at-stake* case where it costs nothing for a validator to vote for more than one block. This problem can be solved by allowing validators to vote only once and heavily penalise them if they vote on more than one chain. In practice, it is more complicated to implement due to possible network delay that might make the validators receive offset chain information.

4 Local currency model with a consensus protocol

In this model of local currency, a decentralised solution via the blockchain is introduced to manage the clearing and validation of transactions and to eradicate the need for a financial partner. Banks or other financial agents could be involved in these solutions (with a possible monetary motivation) but will not play the role of a central authority.

4.1 A non-technical presentation of the model

We present a model that initially includes two types of agents: (pure) consumers who are short-sighted and sophisticated consumers equipped with computers who are able to provide validation services. We deduce present and future consumption of these agents. We then extend the model by introducing a third agent, labelled as the administration,

[15] Miners in the Bitcoin network can create empty blocks that contain only the coinbase transaction (his/her own reward transaction), e.g. at block height 459713 (https://blockchain.info/block/00000000000000001bf525682830b4f77612eb36c2e73754345a7f91aebf7ea). One of the reasons behind this behaviour stems from the fact that miners prefer saving their hash power and time to work on the next blocks rather than include transactions into the current ones.

[16] In Peercoin, the duration of an unspent coin determines its *coinage* e.g. a person who holds 4 coins for 10 days will have accumulated 40 coin-days and will have 4 times more chance to generate profit than a person who has 10 coin-days. Once a miner is chosen to create a block, his/her coinage resets to zero and he must wait again to accumulate coinage. The minting process is designed to yield around one percent profit per year.

who issues the digital complementary currency with an exchange rate of one to one. Consumers seek to obtain bonuses or discounts when they use the currency. For the issuer (who is a corporation of traders or a local government), it is of their interest to foster expenses and increase the profits. The blockchain is chosen to validate transactions done with the complementary currency. Sophisticated agents are able to provide these services. The PoS and PoW consensus protocols are then compared. With the PoS protocol, the validators with the highest amount of deposit in complementary currency are chosen and are paid with fees from consumers. In the PoW protocol, the mining capacity of each sophisticated agent depends on the power of their computer equipment. Miners are then paid with the creation of new units of complementary currency, proportional to the number of transactions they validate. In both cases, the equilibrium number of final users and validators/miners are made endogenous. Additionally in the PoW case, the level of miners' rewards (*i.e.* of endogenous money creation) is also determined.

The possibility of malicious attacks is then considered. In the case of the PoS protocol, the attacks reflect the possibility of validators to mint many transactions simultaneously. This behaviour increases their chance of increasing their revenue associated to their initial deposit of complementary currency. But there is a probability to be detected that can entail costs for them. Validators with the highest initial deposit of complementary currency choose to deviate. The administration can control the level of the advantages provided to end users and the control of malicious validators. Costs associated to control the two aforementioned aspects help determine the optimal choice for the administration, the number of end users at equilibrium and the number of active and malicious validators. In the PoW case, malicious miners conduct the 51% attacks. Given the transaction costs, only efficient miners are able to create a pool. The possibility to control malicious attacks by the administration is also considered in this case.

4.2 The benchmark model

The blockchain can be used to manage digital local currencies. In contrast with crypto-currencies, complementary currencies have only a limited area of circulation and a specific objective for its administrators and users. They can for instance help to promote local productions, short distribution channels or contribute to mutual services exchange inside LETS. There is no possible speculation with this kind of currency: it has fixed exchange rate with the official currency and all incentives converge towards helping users to spend the money they are holding as fast as possible (programmed depreciation of idle balances, limited possibilities of re-conversion, etc).

Initially, the benchmark model integrates three types of agents; consumers and potential validators. There are n short-sighted pure users that has one unit of official currency to spend each, providing them the present utility u. There are also l more sophisticated agents that are called validators (although they do not perform any validation for the moment). They have also one single unit of revenue for the current and the future period each one. They can reallocate it freely as in a financial market. The intertemporal utility

function of validator j ($j = 1, 2, \ldots l$) is given by the following expression:

$$v_j = \ln \left[x_j^{1-\alpha_j} (1 - x_j)^{\alpha_j} \right]$$

where x_j and $(1 - x_j)$ represent respectively the present and future consumption of validator j, and $(1-\alpha_j)$, his/her preference for the present, with $\alpha_j = j/2l$. Thus validators are heterogeneous and they differ according to their rate of preference for the present. Given that, however they would prefer the present than the future.

Validators maximise v_j with x_j to determine the level of their present and future consumption $x_j^* = 1 - \alpha_j$ and $1 - x_j^* = \alpha_j$ respectively. As expected, the smaller the preference for the present for validator j, the bigger the tendency to transfer purchasing power to the future.

This benchmark will be now used to test the effect of the PoW and PoS consensus protocols.

5 Local complementary currency with a Proof of Work protocol

5.1 Characteristics of the model

Units of a complementary currency are issued now. The administration is ensured by third-party agent, external to the pure users and validators. This administrator could be a local government, a private corporation or a non-profit association. Consumers can convert one unit of official currency into one unit of complementary currency. There is no secondary market for the complementary currency in which it could be converted back in official currency, therefore it can only be spent. Pure users can choose to convert or not their unit of official currency before spending it. Converting and using the complementary currency entail costs (essentially transaction costs) and provide advantages such as discounts, rebates, access to retailers who are committed to the respect of environmental or ethical charts and the possibility to have exclusive access to some categories of goods and/or services. These costs and advantages are different for all pure users.

The n consumers are ranked according to these costs and advantages or, similarly, according to their capacity to accept and use the complementary currency. They choose between a reservation utility u, without the use of the complementary currency and a current utility $u_i (i = 1, 2, \ldots n)$ associated with the use of the complementary currency, expressed as:

$$u_i = u - c + ia \tag{1}$$

where c is the psychological or opportunity cost associated to the use and $ia (a > 0)$ the advantages provided by the use of the complementary currency. The additional advan-

tage a is diversely evaluated by consumers, which explains why its value depends on i, and varies across users.

Transaction costs are low than in the PoW protocol, given that miners are paid by the creation of new units of complementary currency. To simplify and without having any consequences on the results, transaction costs are then omitted in expression (**??** given that the revenue of validators comes from the block rewards.

The performance of miners' equipment now determines the capacity of these agents to mine. The higher the performance, the lower the cost to mine and the higher the profit. It is then necessary to rank miners according to the decreasing performance of their equipment. Utility of miner j now writes now as equation (**??**):

$$v_j = \ln \left[x_j^{1-\alpha_j} (1 - x_j + \delta y_j)^{\alpha_j} \right] - \gamma_j y_j \tag{2}$$

where δ represents the unit reward obtained after the creation of a block, y_j the number of validated blocks and $\gamma_j = j\bar{\gamma}, (\bar{\gamma} > 0)$, the unit cost to create a block given the capacity of the equipment of miner j. Note that there is no reason to suppose that the ranking of parameters γ_j is the same than the ranking of parameters α_j. In addition to these private utility and costs, each block generates a social cost e in term of global warming. The miner j then generates negative externalities evaluated to ey_j.

Rewards are spent by miners and finally correspond to a cost for the administrator. Its utility function then changes from expression (**??**) to expression (**??**):

$$U = (\beta - a - \delta)n^* \tag{3}$$

5.2 Basic properties

There is no rationing scheme in this protocol: all potential miners are allowed to participate in the network. The equipment capacity is limited and as the costs of mining increase faster than the utility provided by the validation of transactions, the offer of mining services varies in the same direction as δ (see the proof of lemma **??** for a more detailed study of these variations). Given its objective given by expression (**??**), the administrator chooses the level of rewards δ that maximizes its utility given by expression (**??**) given that the first term of the expression decreases with δ and the second increases with it. The number of "effective" miners adapt to the amount of δ proposed by the administrator and then define the number of transactions able to be validated and the effective number of pure users of the complementary currency. A Nash equilibrium of this economy corresponds then to set of values $\{n^*, l^*, a^*, \delta^*\}$ such that n^* and l^* represent respectively the number of pure users and the number of active miners, a^* the optimal discount offered by the administration and δ^* the unit reward. This is a Nash equilibrium since in this state, each agent (pure users, miners and administrator) make their best decision given the other agents' actions. We begin by exploring the existence of this equilibrium in lemma (**??**):

Lemma 1. *There exists a unique equilibrium set* $\{n^*, l^*, a^*, \delta^*\}$ *that is a solution of the PoW model. This solution does not depend on the relations between the power of mining equipment and the preference for the present of potential miners.*

Proof: From the consumer utility definition, the number of optimal users is now $n^* = n - i^* = n - \frac{c}{a}$. Equation (**??**) is maximised with x_j and y_j for a given value of δ in order to find the individual offer of mining services of miner j if it chooses to participate. The solution is $\left\{x_j = (1-\alpha_j)\frac{\delta}{\gamma_j}, y_j = \max\{\frac{\delta-\gamma_j}{\delta\gamma_j}, 0\}\right\}$ from which is deduced the expression of v_j in equation (**??**), $v_j = (1-\alpha_j)\ln(1-\alpha_j) + \alpha_j \ln \alpha_j + 2\ln\delta + 2\ln\gamma - \frac{\delta-\gamma_j}{\delta}$. This expression must be compared with the benchmark expression of v_j to provide the participation constraint which is then $2\ln\delta - \frac{\delta-\gamma_j}{\delta} \geq 0$. This last expression also writes as $\delta \geq e^{\frac{\delta-\gamma_j}{2\delta}}$. This condition is satisfied for all values of δ and γ_j inside their definition subsets, which makes this participation constraint always validated. The only restriction to the participation of potential miners is then $y_j \geq 0$, *i.e.* $j \leq \delta/\bar{\gamma}$, from which derives $l^* = l\delta/\bar{\gamma}$. Given the expression of γ_j, the total supply of mining services expresses as $\int_1^{l\delta/\bar{\gamma}} \frac{\delta - j\bar{\gamma}}{\delta j \bar{\gamma}} dj = \left[\left(\frac{l\ln j}{\bar{\gamma}} - \frac{lj}{\delta}\right)\right]_1^{\delta/\bar{\gamma}}$, i.e. $\frac{l(\ln\delta - \ln\bar{\gamma})}{\bar{\gamma}} - \frac{l}{\bar{\gamma}} + \frac{l}{\delta}$ which is equalised to $n - \frac{c}{a}$. This equality allows to express δ in function of a. This expression is substituted in equation (**??**) to provide an objective including a single variable. This expression is continuous and has a single maximum in δ^*. From this value, are deduced l^* and a^*, which ends up the proof.

Note[17] that the individual offer of services by miners does not depend on α_j, *i.e.* but rather on the correlation between γ_j and α_j. The same remark can be made for the participation constraint.[18]. Finally, the equilibrium reward δ^* and the number of active miners depend only on the efficiency of the equipment given by $\bar{\gamma}$ and not on the correlation between the preference for the present of miners and the efficiency of their equipment. From Lemma **??** is derived Proposition **??**.

Proposition 1. *The number of miners and the rewards decrease when the efficiency of mining equipment increases.*

Proof: From the determination of δ^* derived from the equation $\frac{l(\ln\delta - \ln\bar{\gamma})}{\bar{\gamma}} - \frac{l}{\bar{\gamma}} + \frac{l}{\delta} = n^*$ and after deriving the left part by $\bar{\gamma}$, it comes that for a given value of δ^*, n^* and $\bar{\gamma}$ vary in the same direction. As a consequence, δ^*, $\bar{\gamma}$ and l^* vary in the same direction at equilibrium.

5.3 Malicious attacks on the Proof of Work model

In this case, it is inefficient for an individual miner to spend energy to create dishonest blocks, since they can be verified by other miners and a block is considered as valid only if there is a majority of miners who confirm it. However, given that the mining capacity is not observable by the administrator, some of the miners can join in their mining power

[17] See Proof of lemma (**??**).
[18] *Ibid.*

to form a single macro-miner that possesses the majority of the total network capacity. This is known as the 51% attack which remains a theoretically important threat in the PoW protocol.

Pooling the mining capacity generates transaction costs (in the sense of Coase): dishonest miners must interact, coordinate and exchange information to maintain mutual trust. These costs increase with the size of the network. However, this activity generates additional revenue in the same proportion τ than in the PoS case and the cost to be detected is expressed similarly. The utility of miner j is now given by expression (**??**) if it decides to participate in an attack:

$$v_j = \ln\left[x_j^{1-\alpha_j}(1 - x_j + (\delta + \tau)y_j)^{\alpha_j}\right] - \gamma_j y_j - \gamma' c - ps \tag{4}$$

where c is the number of single miners that form the malicious macro-miner and γ' a positive parameter. The composition of the pool is set to minimise transaction costs for each member, under the constraint that the pool will be able to provide at least half of the total network mining power. In this scenario, the following proposition is derived:

Proposition 2. *If there are malicious attacks, they are conducted by the most efficient miners. Their relevance decreases when the number of pure users of the complementary currency network increases.*

Proof: A miner for whom collusion is the best choice, considers that the pool that minimises the costs is the one that is composed of itself and other miners that possess the highest mining power. Therefore, only the most efficient miners would pool together. If the miner l^{**} is the least efficient in the pool, the value of l^{**} is obtained as a solution of the equation $\int_1^{j^{**}} \frac{\delta - \bar{\gamma} j}{\delta \bar{\gamma} j} dj = \frac{n^*}{2}$ which gives the solution $l^{**} = -l\frac{\delta}{\bar{\gamma}} W\left(-\frac{\bar{\gamma}}{\delta} e^{\frac{\bar{\gamma} n^*}{2} + \bar{\gamma}}\right)$ where $W(.)$ is the Lambert (or ProductLog) function. Given the non-injective form of $W(.)$, the variation of l^{**} in function of n^* is challenging to study. Its value is however obtained as $\frac{2 \ln l^{**}}{\bar{\gamma}} - l^{**} + 1$ the derivative of which $\frac{2}{b l^{**}} - 1$ decreases, proving that the efficiency of the threshold malicious miner decreases when the number of users increases, or that the pool increases with the number of users. An analysis of the same expression shows that l^{**} decreases slower than n^* increases, which proves the second part of the proposition.

The intuition of this result is simple: when the number of users increases, resources required for mining also increase. If the capacity of the miners' equipment remains unchanged, less efficient computers will also be required to validate an increased number of blocks. Similarly, as 51% of the network power now represents a higher number of miners, the marginal miner inside the new pool is less efficient than before. If the population of users continues to grow, the potential marginal miner in the 51% pool will be unable to cover its costs, given that it has a decreased efficiency and that transaction costs increase. This optimistic conclusion is however challenged by the improvements in mining equipment that are probably faster than the potential growth rate of the population of users.

5.4 The control of malicious attacks

There exist several possibilities to control malicious attacks for the administrator of the complementary currency. The first possibility is to improve the mechanism of detecting attackers. The trade-off is the same as in the PoS model. Costs dramatically increase when the administrator wishes for zero failure. Moreover, as the mining power of malicious miners is associated to the efficiency of their equipment, the most efficient miners tend to resist to relatively efficient systems of detection. Another way to control attacks is to use the amount of rewards. The intuition is simple: an increase of rewards encourage additional miners (the not so efficient ones) to participate in the mining process. Not only the distribution of rewards is changed by this scenario but in overall, the pool size required to cover the 51% total capacity becomes significantly larger. The additional gain from attacks decreases for malicious miners and transaction costs increase. Without any improvement of the mining equipment, the possibilities of malicious pooling could disappear for some levels of rewards. Unfortunately, rewards are also expenses for the administration and since they can be spent by miners or converted into official currency, the choice is then no trivial and should be discussed.

6 Local complementary currency with a Proof of Stake protocol

6.1 Characteristics of the model

Consumers are unchanged, except that, given there is no creation of complementary currency generated by the validation of blocks, transaction costs are paid by consumers to validators for each transaction made in complementary currency. The new utility function is given by equation (**??**):

$$u_i = u - t - c + ia \tag{5}$$

where t is the transaction cost associated to the use of the complementary currency.

In a PoS, the amount of deposit of complementary currency units determines the possibility to mint. In order to mint, a validator must first convert the revenue it intends to transmit to the future in complementary currency. If a validator is chosen to mint at the present period, it will obtain an additional revenue generated by the transaction costs available in the future, with the possibility of spending it or converting it into official currency without cost. If it is not chosen to mint, it can also convert its initial deposit into national currency in the future without cost. Therefore, two periods are considered in this model: the first period in which consumers spend complementary currency and validators validate transactions and the second one in which they spend the cuurency saved in period 1.[19].

[19]For now, in this simplified version of the model, it is supposed that validators have no specific advantages or costs to use complementary currency themselves.

The utility function of validator j now writes as (**??**):

$$v_j = \ln \left[x_j^{1-\alpha_j} ((1 - x_j)(1 + t))^{\alpha_j} \right] \tag{6}$$

where t figures the expected reward (the transaction fee) for one unit of minted complementary currency.

6.2 Basic properties

The benchmark can be solved with a, t and c taken as constants. In application of the PoS protocol in a deterministic way, only potential validators with the highest amount of deposit are selected. Each validator has the possibility to mint an amount of complementary currency equal to its previous idle balance of complementary currency. It is reasonable to suppose that potential validators are rationed but it is not the case for end users (all transactions are minted). Although it could seem unrealistic, the reverse assumption will be discussed below.

If l^* figures the number of effective or active validators, the following lemma is derived:

Lemma 2. *There exists a unique equilibrium pair $\{n^*, l^*\}$ of pure consumers and active validators satisfying the conditions of the PoS model.*

Proof: From equation (**??**), the threshold consumer i^* is such that $i^* = \frac{c+t}{a}$ and the number of users among consumers is $n^* = n - i^* = n - \frac{c+t}{a}$. From the maximisation of equation (**??**) in x_j, the idle balance of complementary currency is obtained for each potential validator as $1 - x_j^* = j/2l$. Given the typical rationing rule of the PoS protocol, the threshold validator j^* is determined as the solution of the equation $\int_{j^*}^{l} (j/2l)dj = n^*$, *i.e.* $j^* = [l(l - 4n^*)]^{1/2}$. Note that $l \geq 4n^*$ is the formal expression of the condition according to which validators and not end users are rationed. From j^* is deduced $l^* = l - j^* = l - [l(l - 4n^*)]^{1/2}$.

Note that with the PoS protocol, the transaction costs t is a way to control the availability of a sufficient number of validators. From lemma (**??**), the condition $l \geq 4(n - \frac{t+c}{a})$ indicates that with low transaction costs, the number of effective validators becomes too small compared to the number of transactions to validate. Similarly, increasing the value of advantages for end users given the transaction costs could have the same effect: this situation is however less likely to occur given that these advantages have generally a cost for the administration of the complementary currency.

From lemma **??**, is derived Proposition **??**:

Proposition 3. *The number of complementary currency users and the number of validators both increase with the advantages provided by the administrator. An increase of the rewards would increase the utility of selected validators, but would also decrease both the number of pure users and active validators.*

Proof: From the proof of lemma **??**, n^* and l^* both increase with a, and n^* decreases when c increases. Given that x_j^* does not depend on t, v_j^* increases with t for active validators and is independent of it for initially inactive validators. However, given that the value of j^* is obtained in the proof of lemma (**??**), the number of validators decreases when c increases, which corresponds also to an increase of t.

6.3 Malicious attacks on the Proof of Stake model

Each validator now has the possibility, if it is chosen, to mint many transactions at the same time. With this extra activity, it can increase its expected revenue, proportionally to the number of transactions it can mint. The probability to get caught and be disclosed is p: in this case, a penalty fine of s is applied immediately. The new utility then expresses as (**??**):

$$v_j = \ln \left[x_j^{1-\alpha_j} ((1 - x_j)(1 + t + \tau))^{\alpha_j} \right] - ps \tag{7}$$

where τ represents the unit increase of future revenue associated to the minting of additional transactions.

The following result derives from the aforementioned assumptions:

Proposition 4. *If there are malicious attacks, they are conducted by the most active validators, which have also the lowest rate of preference for the present.*

Proof: Potential validators have now three possibilities: (i) reservation, (ii) supplying validation services, with a utility given by equation (**??**) or (ii) supplying validation services and validating additional transactions, with a utility given by equation (**??**). Possibility (i) is still dominated by possibility (ii). The comparison between expression (ii) and (iii) determines the threshold malicious validator $j^{**} = \frac{2psl}{ln(1+t+\tau)-ln(1+t)}$.

Intuitively, the number of potential validators who are able to conduct malicious attacks $l - j^{**}$ increases with the expected revenue of the attacks and decreases with the probability to be detected and with the penalty fine. This setting is however not perfectly correct. When there are attacks, extra transaction costs are paid to validators. These extra transaction costs paid to validators imply new unexpected conversions that the administration of the local currency (local government, association of retailers, associations promoting sustainability or short circuits) must bear. The effect is the same if these extra units of complementary currency are converted into goods or services. It is then necessary to explicit the profit function of malicious validators in order to control the attacks.

6.4 Controlling malicious attacks

When the possibility of malicious attacks is not considered, the administration of the local currency has its own benefit or utility function U given by equation (**??**). This

utility depends positively on the number n^* of transactions in complementary currency, and negatively on the advantages a provided to consumers.

$$U = (\beta - a)n^* \tag{8}$$

where $\beta > 0$ is the gross profit obtained by the administrator on each transaction when it is done in complementary currency.

The level of advantage a can be controlled by the administration in order to maximise its gain: the administrator has the position of the principal in an principal-agent relation with pure consumers. With the benchmark specifications and given that $n^* = n - \frac{c+t}{a}$, the optimal amount of the gain a^* can be easily expressed as $a^* = (\frac{\beta(c+t)}{n})^{1/2}$. It increases with the costs of using the complementary currency and decreases with the number of people interested in its use. When there are malicious attacks, wrong transactions generate a cost for the administrator when the additional revenue is converted into official currency or spent in goods or services. The administrator can however invest to increase the probability to detect the attacers. This cost increases at an important rate when p is close to 1 and could for instance be approximated by $\beta' \tanh p$ with $\beta' > 0$. The utility function of the administrator now writes as (**??**):

$$U = (\beta - a)n^* - \beta' \tanh p - \tau \int_{j^{**}}^{l} \frac{j}{2l} dj \tag{9}$$

From this expression is derived the following result:

Proposition 5. *The optimal rate of control of the administrator on malicious activities can prevent any attack on the system only if the sanction is sufficiently severe.*

Proof: Without considering any upper bound of j^{**}, the optimal rate of control p^* is the solution of the equation $\tanh p = (\frac{\beta - \tau l + Ap^2}{\beta})^{1/2}$ with $A = \frac{4\tau s^2 l}{(ln(1+t+\tau) - ln(1+t))^2}$. This equation has a unique solution in p^* that is strictly superior to 0 but strictly inferior to 1. Given the upper bound l of j^{**}, this optimal level of control can prevent any attack ($j^{**}(p^*) \geq l$) or not ($j^{**}(p^*) < l$).

Note that the optimal value of a^* does not depend on τ, e.g. on the aptitude of validators to conduct malicious attacks.

6.5 Externalities

The negative externalities generated by miners have a negative social cost that we neglected in the previous subsections. Their total amount is $\int_1^{l\delta/\bar{\gamma}} e\bar{\gamma} j dj$. These negative externalities are distributed to all agents, including consumers who do not adopt the local currency. Therefore, it is rather arbitrary to introduce the externalities in the private utility function of the administrator and consumers. The loop that generates externalities also entails more complexity to the resolution of the model. It could be easier and not less relevant to consider that these externalities apply to the economy as a whole, without

being exactly evaluated by each agent. In this case, the Nash equilibrium determined in the PoW case does not correspond to the maximisation of welfare. As in similar cases, adapted measures must be defined to limit the activity of miners and the size of the network of local currency users.

7 Conclusion and discussion

Blockchain applications have not yet been addressed to local complementary currency systems. Somehow, the *Colu* local network (CLN) in Liverpool is transitioning onto the blockchain. As these currencies are devoted to get digitised, using the blockchain could free them from the intervention of banks or a financial intermediary. Two blockchain consensus protocols are compared in this paper. They could be implemented in an isolated complementary currency system or used to manage an important number of complementary currency systems in which there would be a collaboration from the administrators of the currency. Each consensus protocol has a different set of properties. The PoS protocol that is still at a preliminary stage, does not involve high costs and encourages validators to hold complementary currencies that would foster its adoption. Attacks on the system are possible but somehow limited to some extent and relatively easy to control or even to tolerate. The system seems to be adapted for small size experiences. When the number of users is limited, the PoW protocol presents more risks as the 51% attacks are more likely to be conducted by pools of miners of rather small size. At this stage, it is difficult to increase the rewards at a level sufficiently high to increase at the same time the number of effective miners and the size of the malicious pools. When the size of the network of local currencies managed in the same blockchain increases, the PoW model becomes less risky as it is the case currently for Bitcoin: malicious attacks are more difficult to be conducted and rewards could be maintained at a relatively low level without risks of generating attacks.

Issues inherent to the current PoW and PoS protocols call for better designs of consensus models. Various alternate forms of PoS protocols are being studied *e.g* the Casper protocol presented by Buterin and Griffith (2017)that is designed to give the possibility for an upgrade on an existing and operating PoW chain with a PoS-based system and the Proof of Activity (PoA) by Bentov, Gabizon and Mizrahi (2014) that aims to solve the problem of depletion of physical scarce resource posed by the PoW system. Future work should encompass these new forms of consensus protocols as well as other forms like the Zero-Knowledge Protocol (ZKP), or the Proof of Space. Even among these new consensus protocols, the specific size and nature of local complementary currencies will determine the choice of the adapted blockchain that follows different objectives than those of crypto-currencies.

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. (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.

Della Peruta, M. and Torre, D., (2015). Virtual social currencies for unemployed people: social networks and job market access. *International Journal of Community Currency Research, 19*(Summer), 31-41.

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

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.

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.