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

Sothearath SEANG* Dominique TORRE*

February 2018

Abstract

This paper examines with the help of a theoretical setting the properties of two blockchains' consensus protocols (Proof of Work and Proof of Stake) in the management of a local (or networks of local) complementary currency(ies). The model includes the control by the issuer of advantages of the use of the currency by heterogeneous consumers, and the determination of rewards of also heterogeneous validators (or miners). It considers also the resilience of the validation protocols to malicious attacks conducted by an individual or pools of validators. Results exhibit the interest of the Proof of Stake protocol for small communities of users of the complementary currency, despite the Proof of Work Bitcoin like system could have advantages when the size of the community increases.

JEL Classification: E42, L86

Keywords: payment systems, heterogeneous agents, Proof of Work, Proof of Stake, blockchains, complementary currencies.

1 Introduction

In recent years, the blockchain technology (BCT) has sparked a lot of interest around the world and its applications are being tested across many sectors such as

*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

finance, energy, public services and sharing platforms. Although the technology is still immature and 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. A blockchain is a type of distributed ledger technology (DLT) that is highly secured by cryptography[1]. 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 types of information at any given point in time. Because the blockchain has no central authority of regulation and control, consensus among users is paramount to guarantee the security and the sustainability of the system[2]. 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.

Like any systems that have complex interactions and require reliability and control, local payment systems would be a relevant case for the adoption and use of the BCT. Local complementary currencies are payment systems that have proved to help achieving economic and/or social objectives such as revitalisation of local businesses, reinforcement of social links, promotion of short circuits and valorisation of territorial resources. They are different from Local Exchange Trading Systems (LETS) and virtual/crypto-currencies[3]. Through their multiplier effect, complementary currencies can also reduce unemployment and increase social well-being of consumers (Della Peruta and Torre, 2015). In their fiduciary version which is also the most frequently adopted, complementary currencies are made reliable by the insertion in each note of a digital device difficult to counterfeit. Some complementary currencies exist only in digital form, for instance the *SoNantes* in the Loire Atlantique district in France and the *Colu* in Liverpool in the United Kingdom. It becomes more challenging to manage accounts, make settlements and provide a sufficient level of trust of such currencies. They are usually admin-

[1] A DLT is 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.

[2] 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 BCT so we will only consider the case of a public blockchain for the rest of the paper.

[3] See Tichit, Lafourcade and Mazenod (2017) for a description of criteria distinguishing complementary currencies, LETS and crypto-currencies.

istered by one or a few central entities like a bank or an I.T. firm[4]. The motives for the digitisation of a complementary currency could be multiple: elimination of paper printing costs, reduction of administration costs by a third-party, increased likelihood of attracting more young users and all the potential benefits and opportunities that can be derived from the use of the BCT[5]. Some complementary currencies originally introduced under fiduciary forms are now moving to a digital version like the *Renoir* in Cagnes-sur-Mer in while others are directly introduced in the latter form like the *SoNantes*. It is therefore reasonable to imagine decentralised solutions to manage such currencies, in which banks or other financial agents could be involved (with a possible monetary motivation) but will not play the role of a central authority. The BCT could be useful for this objective and different consensus protocols are to be confronted.

The first BCT application was introduced in 2008 by Satoshi Nakamoto to the Bitcoin network and employs the Proof of Work (PoW) consensus model as the backbone of the system [6]. PoW protocol needs the adoption of diverse conventions, relative for instance to the size of each "block" which bother transactions waiting for validation, the bounty reward of validators (called "miners") which consists in the Bitcoin case in the monetary creation, the reward amount adjustment in time, and the money supply limit[7].

In a PoW protocol, it is the combination of cryptography and computational power that creates consensus and ensures the authenticity of data recorded on the

[4] SoNantes is managed by the *Crédit Municipal bank* of Nantes (see https:sonantes.fr) and *Colu* by the firm that goes by the same name as the currency (see https:colu.com)

[5] The claimed advantages of the BCT are briefly exposed in the literature section.

[6] 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.

[7] 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.

blockchain. 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 solve cryptographic problems imposed by the protocol[8]. 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 transaction fees associated to the transactions (borne by and vary among users that make the transactions) that he / she included 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 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 mining process requires computers to run at maximum capacity, therefore consuming a considerable amount of electricity which makes by nature the PoW a resource-intensive consensus protocol; time and energy serve as proofs that work has been done. In 2014, the power consumed by the Bitcoin network was equal to Ireland's electricity consumption (O'Dwyer and Malone, 2014). Users and validators accepted this protocol which became popular and contributed to the success of the crypto-currencies that adopted it. However, despite this success, the future of this protocol remains unclear, particularly because it was not imagined to manage the speculative asset that became Bitcoin.

Like any digital devices, 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

[8] 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.

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 decision power to minters that actually have a stake in the system. Unlike the PoW in which everyone can become a miner, not everyone can join the network in a PoS system. Ownership of a currency or having a deposit in the network allows the nodes to participate in the minting process i.e. to validate transactions and create blocks. No computational power is required to solve cryptographic puzzles like in the PoW scheme. There are no rewards under the form of a money creation: validators collect fees from users and are paid from them as an ususal intermediary. Since validators only get transaction fees, the scenario in which validators create empty blocks can be avoided[9] as they are incentivised to include a maximum number of transactions to maximize their gains. Because no new coins will be created in a pure form of PoS and the money supply must be issued since the beginning, the problem of an initial fair coin distribution arises. If the PoS includes a selection of 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[10].

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

[9] 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 might be because miners prefer saving their hash power and time to work on the next blocks rather than include transactions into the current ones.

[10] 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.

be solved by allowing validators to vote only once and heavily penalize them if they vote on more than one chain. In practice, this is more complicated to implement due to network delay that might make the validators receive offset chain information. Two other types of PoW/PoS-improved consensus protocols (Casper and Chain of Activity) are briefly presented in the literature section.

The objective of this paper is to study the properties of the two blockchain protocols when they are applied to validate and clear the transactions inside (or among) local systems of digital complementary currencies. The PoW consensus is the pioneering one and still the most popular given its use in Bitcoin. So far it remains the most reliable and the most commonly adopted in the case of the management of a local complementary currency. What about the challenging properties of the Proof of Stake (PoS) consensus protocol with heterogeneous agents, both on the users' and validators' side? The simplified theoretical setting presented in this paper tries to contribute to answer this question. It integrates three types of agents. Final users of complementary currencies are motivated by an advantage associated to transitions made using this money. The issuer/administrator of the complementary currency determines the nature and amount of this advantage, and organises the conversion of official money in complementary currency. Lastly, validators / miners confirm that a given payment is valid and clear users' accounts. It would also be interesting to know whether it is beneficial for malicious validators / miners to conduct attacks or not.

The theoretical results of the model point out the contrasting interest of the two protocols. The PoW generates the creation of additional units of complementary currency which add to the previous ones held by the users. The costs of these additional units are borne by the issuer. Attacks are more likely to occur when the size of the users' community is small. The PoS 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.

2 Blockchain applications in different sectors

The blockchain is a General-Purpose Technology (GPT) that is being studied and tested in many sectors including finance, energy, cybersecurity, healthcare, government services and e-residency. Wolfond (2017) explained how the imple-

mentation 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 BCT to the healthcare industry to illustrate potential improvements in terms of security and privacy and additionally showed 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[11] 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 require human verification. Ølnes, Ubacht and Janssen (2017) conducted an assessment of the potential BCT benefits found in the literature and classified by 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 BCT to yield benefits.

In the banking industry, Guegan (2017) addressed questions concerning the use of private blockchains to reduce costs, increase security and simplify bank operations. He stressed on the fact that the current benefits of the BCT are more applicable to a public and hence decentralized system rather than a centralized

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

one. Guo and Liang (2016) explored the potential advantages that the BCT can offer in clearing and credit information systems as well as the regulation, efficiency and security challenges for implementing the BCT in the Chinese banking industry. They came to conclude that those problems will be solved over time and the technology will be somehow incorporated in the future. Ripple is an inter-bank payment solution that provides extremely fast transactions speed (across the world in seconds), transparency and simplicity for users. It seeks to create a universal payment protocol and has a digital token for transactions on the blockchain called XRP (Schwartz, Youngs and Britto, 2014). Similarly, Jaag and Bach (2016) presented the possibilities of using the BCT for postal financial services to improve financial inclusion and the creation of a postal cryptocurrency to counter the high volatility that plague most cryptocurrencies. By backing coins with a national currency like the US dollars, CryptoBucks and Tether (Conley, 2017) seek to combat the high market volatility of cryptocurrencies and establish faith, ease of use and financial connections to the outside world for consumers. The Ethereum blockchain allows users to create, buy and sell smart-contracts on the blockchain and its currency Ether, is the second largest crypto-currency in terms of market capitalisation[12].

3 The benchmark model

Blockchains can be used to manage digital complementary currencies. In contrast with the international crypto-currencies, complementary currencies have only a limited area of circulation, and a specific objective for administration and users. They can for instance help to promote local productions, short distribution channels, or contribute to exchange of mutual services inside LETS. There is no possible speculation with this kind of currency: t a fixed exchange rate with the official currency and all incentives converge to help users spending rapidly their holdings (programmed depreciation of idle balances, limited possibilities of re-conversion, etc).

The benchmark model integrates initially three types of agents; (pure) users, the administration of the complementary currency and potential validators. There are n short-sighted pure users. Each one has one unit of official currency to spend,

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

providing it the present utility u. There are also l more sophisticated agents labeled validators (despite they do not validate anything for the moment). They have also one single unit of revenue for the current and the future period. They can reallocate it freely by a prefect 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 $\alpha_j = j/2l$. Validators are then heterogeneous and differ according their rate of preference for the present, given that all however prefer present to future.

Validators maximise v_j in 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 proof of work and proof of stake consensus methods.

4 Complementary currency with a proof of stake protocol

Complementary currency is now issued. It is administrated by a third agent, external to pure users and validators. This administrator could be a local government, a professional corporation or a non profit association. Consumers can convert one unit of national currency into one unit of complementary currency. There is no secondary market for complementary currency where it could be converted back in official currency: it can only be spent. Pure users can convert or not their unit of official currency before spendings. Converting and using complementary currency entail costs (essentially transaction costs) and advantages (discounts, possibility to access to some category of goods or services). These costs and advantages are not the same for all pure users.

The n consumers are ranked according to these costs and advantages or, simi-

larly, according to their capacity to accept and use complementary currency. They choose between a reservation utility u, without the use of complementary currency and a current utility associated with the use of complementary currency $u_i (i = 1, 2, \dots n)$, expressed as:

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

where t is the transaction cost associated to the use of the complementary currency, c other psychological or opportunity costs associated to the same use, and $a (a > 0)$ the advantage generated by the use of complementary currency. This advantage (access to specific additional services, to rebates, to retailers specially committed to the respect of environmental or ethical charts) is diversely evaluated by consumers, which explains why its value vary across potential users.

In a proof of stake consensus method, the amount of complementary currency deposit determines the possibility to mint. In order to mint, a validator must then convert first the revenue it intends to transmit to the future in complementary currency. If it is chosen to mint at the present period, it obtains an additional revenue generated by transaction costs available in the future, with the possibility to convert its to without cost or to spend it. If it is not chosen to mint, it can also convert back its initial holding in the future without cost.[13]

The utility function of validator j writes now as (2):

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

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

4.1 Basic properties

The benchmark can be solved with a, t and c taken as a constant. In application of the proof of stake rule in a deterministic way, only potential validators with the highest offer of validation are selected, each one having the possibility to forge an amount of complementary currency equal to the amount of its previous idle balance converted in complementary currency. It is reasonable to suppose

[13] In this simple version of the model, it is thus supposed that validators have no specific advantage or cost to use themselves complementary currency.

that potential validators are rationed but not final users (all transaction is always forged). 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 1. *There exists a unique equilibrium pair $\{n^*, l^*\}$ of pure consumers and active validators satisfying the conditions of the proof of stake model.*

Proof: From equation (1), 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 maximization of equation (2) in x_j, the idle balance of complementary currency is obtained for each potential validator, as $1 - x_j^* = j/2l$. Given the rationing rule typical of the proof of stake system, 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 which validators and not final users are rationed. From j^* is deduced $l^* = l - j^* = l - [l(l - 4n^*)]^{1/2}$ ■

Note that with the proof of stake system, the amount of transaction costs t is a way to control the availability of a sufficient number of validators. From lemma (1), the condition $l \geq 4(n - \frac{t+c}{a})$ indicates that with tiny 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 final users for given transaction costs could have the same effect: this situation is however less likely to appear given that these advantages have generally a cost for the administration of the complementary currency.

From lemma 1, is derived Proposition 1:

Proposition 1. *The number of complementary currency users and the number of validators both increase with the advantage to use complementary currency provided by the administrator. All increase of the rewards increases the utility of selected validators, but decreases both the number of pure users and of active validators.*

Proof: From proof of lemma 1, 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 on it for initially inactive ones. However, given the value of j^* obtained in the proof of lemma (1), the number of validators decreases

when c increases, which corresponds also to an increase of t ■

4.2 Malicious attacks

Now, each validator has the possibility, if it is chosen, to forge and validate many transactions at the same time. With this extra activity, it can increase its expected revenue, in proportion of the number of transactions it can forge. The probability to be disclosed is p: in this case, a penalty s applies immediately. Its new utility then expresses as (3):

$$v_j = \ln \left[x_j^{1-\alpha_j} ((1 - x_j)(1 + t + \tau))^{\alpha_j} \right] - ps \tag{3}$$

where τ figures the unit increase of future revenue associated to forging additional bad blocks.

The following result derives from these assumptions :

Proposition 2. *If there are, malicious attacks are conducted by the most active validators, which have also the smallest 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 (2) or (ii) supplying validation services and validating bad blocks, with a utility given by equation (3). The possibility (i) is still dominated by the possibility (ii). The comparisons between expressions (ii) and (iii) determines the threshold malicious validator $j^{**} = \frac{2psl}{ln(1+t+\tau)-ln(1+t)}$ ■

As suggested by intuition, the number of potential validators able to conduct malicious attacks $l - j^{**}$ increases with the expected payment of these attacks, and decreases with the probability to be detected and the amount of the penalty when detected. This setting is however not perfectly correct. When there are attacks, extra transactions costs are payed to validators. Even if wring validations correspond only to additional wrong empty blocks, extra transaction costs payed to validators involve new unexpected conversions that the administration of the local currency (local government, corporation of retailers, association promoting sustainability or short circuits, etc.) has at its charge. The effect is the same if these extra units of complementary currency are converted in goods or services proposed by the administration in exchange of them. It is then necessary to make

explicit validators' function of gain to consider actions they could select to control malicious attacks.

4.3 Controlling malicious attacks

When the possibility of malicious attacks is not considered, the administration of the local currency has its own gain or utility function U given by equation (4). This utility depends positively on the number n^* of transactions in complementary currency, and negatively on the advantages a provided to consumers.

$$U = (\beta - a)n^* \tag{4}$$

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

The level of advantage a can be controlled by the administration in order to maximize its gain: the administrator has the position of the principal in an agency relation with agents/pure consumers. With the benchmark specifications, given that $n^* = n - \frac{c+t}{a}$, the optimal amount of the gain a^* is easily found as $a^* = (\frac{\beta(c+t)}{n})^{1/2}$. It increases with the cost of using the complementary currency and decreases with the population interested in its use. When there are malicious attacks, wrong blocks generate a cost for the administrator when the revenue they create is converted in official currency or spent in goods or services. The administrator can however invest to increase the probability to observe the authors of malicious attacks. This cost increases at an increasing 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 (5):

$$U = (\beta - a)n^* - \beta' \tanh p - \tau \int_{j^{**}}^{l} \frac{j}{2l} dj \tag{5}$$

From this expression, is derived the following result:

Proposition 3. *The optimal rate of control of the administrator on the malicious activity can prevent any attack of 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^* 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 nor depend of τ, e.g. on the aptitudes of validators to conduct malicious attacks.

5 The proof of work version

There is no fundamental change for consumers in this version except that transaction costs are lower than in the PoS protocol, given that miners are paid by the creation of new units of complementary currency. For the sake of simplicity and without any consequences on the results, transaction costs are ignored given that validators revenue have for the most another origin. Consumer i utility is now given by equation (6):

$$u_i = u - c + ia \tag{6}$$

The performance of miners' equipment now determines the capacity of these agents to mine. The higher the performance, the smaller the cost to mine and the bigger the gain. It is then necessary to rank miners in a new way, according to the decreasing performance of their equipment. Utility of miner j now writes now as equation (7):

$$v_j = \ln \left[x_j^{1-\alpha_j} (1 - x_j + \delta y_j)^{\alpha_j} \right] - \gamma_j y_j \tag{7}$$

where δ represents the unit reward obtained after the validation of one transaction, y the number of forged transactions, and $\gamma_j = j\bar{\gamma}, (\bar{\gamma} > 0$, the unit cost to forge one transaction given the capacity of miner j's equipement . Note that is no reason to suppose that the ranking of parameters γ_j is the same than the ranking of parameters α_j.

5.1 Basic properties of the Proof of Work system

There is no rationing schema in this protocol: all potential miners wishing to forge are allowed to participate. The rewards could be considered as social costs for the administrators of the complementary currency (they can be converted back at least partially in the official currency, which involves a cost for the administrator).

At the same time, as the equipment capacity is limited and as the costs to mine increase faster than the utility generated by the validation of transactions, the offer of mining services varies in the same direction than δ (see the proof of lemma 2 for a more detailed study of these variations). For the administrator, there is a tendency to make δ as small as possible, until the optimal reward δ^* the offered capacity to forge is just sufficient for the number of transactions to forge. A Nash equilibrium of this economy corresponds then to a triplet $\{n^*, l^*, \delta^*\}$ such that n^* and l^* represent respectively the number of pure users and the number of active miners corresponding to the unit reward δ^*. 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 (2):

Lemma 2. *There exists a unique equilibrium triplet $\{n^*, l^*, \delta^*\}$ solution of the proof of work model. This solution does not depend on the relation between the power of computers and the preference for present of potential validators.*

Proof: From consumer utility definition, the number of users among consumers is now $n^* = n - i^* = n - \frac{c}{a}$. Equation (7) is maximised in x_j and y_j for a given value of δ 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 (7), $v_j = (1-\alpha_j)\ln(1-\alpha_j) + \alpha_j \ln \alpha_j + 2\ln\delta + 2\ln\gamma - \frac{\delta-\gamma_j}{\delta}$. 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 expresses also 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., $j \leq \delta/\bar{\gamma}$. Hence, given the expression of γ_j, the total supply of mining services expresses as $\int_1^{\delta/\bar{\gamma}} \frac{\delta - j\bar{\gamma}}{\delta j \bar{\gamma}} dj = \left[\left(\frac{\ln j}{\bar{\gamma}} - \frac{j}{\delta}\right)\right]_1^{\delta/\bar{\gamma}}$, i.e. $\frac{\ln\delta - \ln\bar{\gamma}}{\bar{\gamma}} - \frac{1}{\bar{\gamma}} + \frac{1}{\delta}$ which equalised to $n - \frac{c}{a}$ determines the reward δ^*. The solution is unique given the variation of $\frac{\ln\delta - \ln\bar{\gamma}}{\bar{\gamma}} - \frac{1}{\bar{\gamma}} + \frac{1}{\delta}$ inside the interval of definition of δ. From δ^*, is derived $l^* = \delta^*/\bar{\gamma}$. Namely, the variation of this expression when δ increases is given by the sign of its derivative $\frac{1}{\bar{\gamma}\delta} - \frac{1}{\delta^2}$. Given the definition of y_j, this expression is always positive, indicating that n^* and δ^* increase together, proving the uniqueness of δ^*. Last, from δ^*, is derived $l^* = \delta^*/\bar{\gamma}$ which is also unique and decreases when n^* increases ■

Note[14] that the individual offer of services by miners does not depend on α_j, e.g. on the correlation between γ_j and α_j. the same remark can be made for the participation constraint.[15]. Finally, the equilibrium reward δ^* and the number of active miners depend only on the computers' efficiency, given by $\bar{\gamma}$ and not on the correlation between the preference for the present of validators and the efficiency of their computers. From Lemma 2, is derived Proposition 4.

Proposition 4. *The number of pure consumers and miners increase and the rewards decrease with the advantage to use complementary currency provided by the administrators. The number of miners and the rewards decrease when the efficiency of mining equipment increases.*

Proof: The derivative of n^* according a is positive. As the threshold miner is $l^* = \delta^*/\bar{\gamma}$, and given Lemma 2, δ^* increases with n^* which increases itself with a, l^* finally increases itself with a. Also, given Lemma 2, the rewards decrease with a. From the determination of δ^* derived from the equation $\frac{\ln\delta - \ln\bar{\gamma}}{\bar{\gamma}} - \frac{1}{\bar{\gamma}} + \frac{1}{\delta} = n^*$ and after derivation of the left part in $\bar{\gamma}$, its comes that for a given value of δ^*, n^* and $\bar{\gamma}$ vary in the same direction. As a consequence, δ^* and $\bar{\gamma}$, then l^* vary in the same direction at equilibrium ■

5.2 Malicious attacks of the Proof of Work system

In this case, it is inefficient for an individual miner to spend energy to create bad blocks, since they will 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 their mining power and form a single macro-miner that possesses the majority of the total network capacity. This is the 51% rule which provides the most efficient threat of failure in the PoW protocol.

Pooling the mining capacity generates transaction costs (in the sense of Coase): dishonest miners must interact, coordinate and exchange signs to maintain mutual trust. These costs increase with the size of the network. However, this activity generates for additional revenue in the same proportion τ than in the PoS case

[14] See Proof of lemma (2).
[15] *Ibid.*

and the cost to be disclose is expressed in the same way. The utility of miner j is now given by expression (8) if it decides to participate in an attack:

$$v_j = \ln\left[x_j^{1-\alpha_j}(1 - x_j + (\delta + \tau)y_j)^{\alpha_j}\right] - \gamma_j y_j - \gamma' c - ps \tag{8}$$

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 5. *If there are, malicious attacks are conducted by the most efficient miners. Their relevance decrease when the number of pure users of the complementary currency increases.*

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

The intuition of the result is simple: when the number of users increases, resources necessary for the validation also increase. If the capacity of the miners' equipment remains unchanged, less efficient computers are also reacquired 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 validator 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 probably

more rapid than the potential grow of a population of users.

5.3 The control of malicious attacks

There exist several possibilities to control malicious attacks for the administrator of the complementary currency. The first is to improve the mechanism of disclosure of the authors of the attacks. The trade off is the same than with the PoS model. Costs dramatically increase when the administrator plans 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 observation. Another way to control attacks is to use the amount of rewards. The intuition is simple: all increase of the rewards makes additional miners, not so efficient, able to participate to the validation process. Not only, the distribution of rewards is changed by this entry but overall it the pools necessary to cover 51% of the votes is larger. The additional gain from attacks decreases for malicious miners and transaction costs increase. Without any improvement in the computers' memory, the possibility to pool could disappear from some level of rewards. Unfortunately, rewards are also expenses from the administration, since they can be spent by miners or convert near the administrators in official currency. The choice is then no trivial and could be discussed.

6 Conclusion

Blockchain applications have not yet been addressed to local complementary currency systems. Somehow, the *Colu* currency in Liverpool is transitioning onto the blockchain. As these currencies are devoted to get digitised, using the BCT could free them from the intervention of secondary banks or a financial intermediary. Different blockchain protocols are compared in this paper. They could be implemented in an isolated complementary currency system or used to activate an important number of complementary currency systems the administration of which would have decided to collaborate at this level. Each consensus protocol has a different set of properties. The PoS protocol, still at a preliminary stage to secure crypto-currencies, does not involve large costs, and it also encourage validators to hold complementary currencies, which would help its adoption. Attacks are possible, but limited to some extent and relatively easy to control or even to tolerate. The system seems to be adapted to small size experiences. When the number of users is limited, the PoW protocol presents more risks as 51% attacks

are more likely to be conducted by pools of miners of very limited size. At this stage it is difficult to increase the rewards at a level high enough to increase the number of effective miners and the size of the pools of malicious ones. When the size of the network of local currencies managed by the same blockchain increases, the PoW system 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 but not yet e.g the Casper protocol presented by Buterin and Griffith (2017) designed to give the possibility to upgrade 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 at solving 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 others like the Zero-Knowledge Protocol (ZKP), or the Proof of Space. Even among these new consensus protocols, the specific size and nature of each complementary currencies will define the choice of the most adapted blockchain.

References

Bentov, I., Gabizon, A., and Mizrahi, A. (2016). *Cryptocurrencies without proof of work.* Paper presented at the International Conference on Financial Cryptography and Data Security (pp. 142-157). Springer, Berlin, Heidelberg, February. DOI:10.1007/978-3-662-53357-4_10

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. DOI:10.1145/2695533.2695545

Buterin, V., and Griffith, V. (2017). Casper the Friendly Finality Gadget. *arXiv preprint.* arXiv:1710.09437

Catalini, C., and Gans, J. S. (2016). *Some simple economics of the blockchain* (No. w22952). Retrieved from the National Bureau of Economic Research. http://www.nber.org/papers/w22952.pdf

Collomb, A., and Sok, K. (2017). "Blockchain" : une révolution monétaire et financière ?. *Alternatives Economiques, 75, July.* Retrieved from https://www.alternatives-economiques.fr/blockchain-une-revolution-monetaire-financiere/00079793

Conley, J. P. (2017). *Blockchain Cryptocurrency Backed with Full Faith and Credit* (No. 17-00007). Retrieved from the Vanderbilt University Department of Economics. http://www.accessecon.com/Pubs/VUECON/VUECON-17-00007.pdf

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. DOI:10.15133/j.ijccr.2015.004

Guegan, D. (2017). Public Blockchain versus Private blockhain. Retrieved from the Centre of Economics of the Sorbonne. https://halshs.archives-ouvertes.fr/halshs-01524440/

Guo, Y., and Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation, 2*(1), 24. DOI:10.1186/s40854-016-0034-9

Hajdarbegovic, N. (2014). Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack. *CoinDesk.* Retrieved from https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

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. https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-71.pdf

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. DOI:10.1007/978-3-319-46046-8_13

King, S., and Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-published paper.* Retrieved from http://peerco.in/assets/paper/peercoin-paper.pdf

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027-1038. DOI:10.1016/j.telpol.2017.09.003

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

O'Dwyer, K. J., and Malone, D. (2014). *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, June 26-27. DOI:10.1049/cp.2014.0699

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. DOI:10.1016/j.giq.2017.09.007

Pilkington, M. (2016). Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225. Retrieved from https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660

Schwartz, D., Youngs, N., and Britto, A. (2014). The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper, 5*. Retrieved from https://prod.coss.io/documents/white-papers/ripple.pdf

Sullivan, C., and Burger, E. (2017). E-residency and blockchain. *Computer Law and Security Review, 33*(4), 470-481. DOI:10.1016/j.clsr.2017.03.016

Tichit, A., Lafourcade, P., and Mazenod, V. (2017). Les monnaies virtuelles décentralisées sont-elles des outils d'avenir. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01467329/

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. DOI:10.22215/timreview/1112