The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework

Olivier Hueber

The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework

Olivier Hueber

University Côte d'Azur (UCA) – GREDEG CNRS (UMR 7321), 250 Rue Albert Einstein, 06560 Valbonne – Sophia Antipolis, France

Abstract: After a description of the blockchain that underpins the Bitcoins, this paper provides a new mechanism to reinforce the credibility of online transactions blockchain technology based. It then becomes possible to explore the future of the blockchain technology in other online electronic markets of goods and services. We assert that the blockchain technology, still linked with the bitcoins, could become in a near future the keystone of many electronic markets and could considerably increase online transactions. A cryptocurrency regime based on sidechain is modeled and a public blockchain controlled by a Central is proposed.

Keywords: Blockchain, Sidechain, Bitcoin, Crypto-currency, memory, payment system, online market

Reference: Hueber O., (2017) 'The Blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework', *Int. J* Transitions and Innovation Systems *xxxxxxxxxxx xxxxxxxxxxx*,

Biographical notes: *Dr*. Olivier Hueber is associate professor in the University Côte d'Azur (UCA), France. He is currently Director of UnicePro, a University Centre for the lifelong learning programs. As a full member of the public Research Institute GREDEG (UMR 7321, CNRS) in Sophia Antipolis, his topics of research include electronic money and entrepreneurship. He is also the author of a textbook in General Economic Theory devoted to undergraduate students

1 Introduction

In the economic literature, the question of the coexistence of different currencies is very old. Such a question is already present in the debate initiated by Adam Smith (1776, Book II, chapter II) on free banking in Scotland. According to Smith, banks can be left free in their paper-money policies because convertibility between different private currencies is enough to prevent excessive issuance (White, 1984). Conversely, Stanley Jevons (1850) advocated for a monopole of money creation held by a Central Bank.

Olivier Hueber,

Although never really disappearing from the literature, the debate was strongly revived from the nineties concomitantly with the explosion of new private currencies conveyed by the Internet network. Many economists, following the example of Benjamin Friedman (1999), argued that a private electronic money (e-money) might render central banks obsolete and threaten the publics regulated interbank systems. Beyond the ongoing theoretical debates, the reality principle forces us to admit that private electronic currencies are now at the core of the electronic commerce. This fact considered, it becomes essential to find a solution able to coordinate the numerous electronic private currencies altogether and a solution able to link them to central banks.

As far as we know, no one have already find an economic lasting solution to create reliable footbridges between the numerous private and public electronic currencies. Many website propose an exchange rate service for converting different private e-currencies. Such websites are in any way connected neither to the official interbank systems nor with a "supraweb" currency acting like a unit of account within a multilateral clearing system in the worldwide web[1]. One solution to create gateways between the public monetary regimes (with legal tender currencies) and the private monetary regimes (with private cryptocurrencies or local currencies) could lie in the creation of an Automated Clearing House (ACH). Such an institution could give to any private crypto money issuer some special drawing rights based on a standard of measure like the gold standard. This proposal comes to partially reinvent sixty years after, the "bancor" of Keynes (1980 ed.). The solution on creating an international ACH online has been investigated but it is hard to implement because of the difficulty to find a common standard measurement of value (Heller 2017). The invention of the blockchain technology, almost ten years ago, has completely revolutionized the way of conceiving the coordination between private electronic currencies and their links with central banks.

The Blockchain is the ledger of past transactions which allows asset control in a network without a central authority[2]. This concept of sharing a common ledger between parties increases the transparency of all markets and can make these markets more accessible to a broad range of economic agents. With the now well-known cryptocurrency Bitcoin, the

[1] We use the word "supraweb" by analogy to the supranational currency conceptualized by Keynes and called Bancor. According to Keynes, international trade would gain to be valued and cleared in bancor.

[2] A blockchain is a chain of blocks confirming taken transactions to the entire network.

blockchain technology has proven its robustness and its efficiency[3]. A blockchain is powered by blocks issued from a mining process and from blocks describing changes in asset control. Most of the blockchains are designed to register transaction of digital coins but a blockchain can also register any asset and is not confined solely currencies. A coin is a specific asset and in the cryptographic vocabulary an asset is a digital property whose controller can be cryptographically ascertained. Blockchain is both an asset registry and an identity framework based on cryptographic signatures. So anywhere where this is helpful, the blockchain technology can be implemented. Therefore, a blockchain can register and validate diploma, a virtual share, a copyright, a proof of membership, land registry or anything else.

It's a safe bet that in a very near future many online transactions will be validated by blockchains. The theoretical challenge that must be overcome is so how to coordinate the different blockchains with each other's and how, at the monetary level, link the monetary blockchains to central banks.

This paper assert that the sidechain technology is the solution enable to coordinate and to efficiently organize the huge world of online private crypto currencies[4]. After a technical overview of the blockchain technology (II), a new solution devoted to reinforce the reliability of online transactions using blockchains is proposed (III). It then becomes possible to model how sidechains pegged to blockchains car play a coordination and a security role in the expansion of electronic transactions done with private electronic tokens (IV).

2. Technical overview and theoretical issues

The creation of a new block added to the blockchain relies on a hash-based proof-of-work. A hash function is an algorithm that transforms (hashes) an arbitrary set of data elements, such as a text file, into a single fixed length value (the hash). The hashcash proof-of-work function (h) used by miners comes from Adam Back works (1997). This function is built on a security property of cryptographic hashes, that they are designed to

[3] The Bitcoin is fiduciary money launched in 2009. Nobody really knows the genesis of the Bitcoin. We just have a nickname namely Satoshi Nakamoto which wrote a paper in 2009 presenting a system for peer-to-peer electronic transactions.

[4] A sidechain is a blockchain "pegged" to the main blockchain allowing transfers of key information from one chain to the other. The sidechain validates data from other blockchains.

be hard to invert. With y=H(x), it is easy to compute y from x. Conversely, it is harder to find x given only y. The difficulty of the proof-of-work is determined by the value of y (ie. the nonce). With the hascash algorithm SHA-256 used by miners of the Bitcoin community, a full hash inversion is mathematically infeasible[5]. The only way to find the value of x given only y is based on numerical simulations. These simulations - commonly called proof-of-work - are time consuming and are costly in energy. Miners are profitable when their hardware and electricity costs to mine one bitcoin are lower than the price of one bitcoin.

The Bitcoin mining process pointlessly wastes huge quantity of real energetic resources. By analogy, we can refer to the gold and the silver money much maligned by Adam Smith (Wealth of Nations II.ii.86). Smith pointed out the wastefulness of using precious metal as a currency[6]. According to Smith, gold and silver serve only a symbolic function and their production absorbs real resources. For this reason, Smith recommends to replace metal money with paper currency. Smith shows how bank issued paper money saves real resources. Admittedly, both mining process - either Bitcoin or precious metal - absorb real resources but the comparison cannot be carried too far. First, the real resources expended in mining Bitcoin are much less than the real resources expended in mining gold of silver. Second, the Bitcoin mining process, based on numerical simulations, is not necessarily pointless. The proof-of-work can be harnessed to improve knowledge in mathematics. For instance, the cryptocurrency Primecoin implements a proof-of-work based on searching for prime number. There is a Scientific Value behind Primecoin's Work.

The hashcash function is given by the bitcoin protocol without any central authority. Among the community of miners, each miner tries to find the value of x by doing numerical simulations. The first miner able to calculate x earns 25 bitcoins. The value of y given by the Bitcoin protocol is estimated in order to assume that the necessary period to find x is approximately 10 minutes[7]. If during the same period of roughly 10 minutes several miners find the value of x, a random process chooses a miner as a winner. Thereby, the Bitcoin protocol is built to create 25 Bitcoins about each 10 minutes and for

[5] The SHA-256 encryption of the name "Adam Smith" is "3db67c85ce1a968e7a45873dfe6faf102c957631ea65118c9715068a0877fee1".
[6] "The gold and silver money which circulates in any country may very properly be compared to a highway, which, while it circulates and carries to market all the grass and corn of the country, produces itself not a single pile of either." (Smith, 1776, II, ii, 86)
[7] In year 2015, each 10-12 minutes, 25 Bitcoins were issued.

giving these 25 Bitcoins to a selected miner who was able to solve the proof-of-work function (h) by using numerical simulations[8].

The selected miner who receives 25 "new" Bitcoins adds a new block to the blockchain[9]. This new block asserts that all the transactions done, since the previously created page (approx. 10 minutes ago), are valid. Such a validation is essential. During a transaction, the computer of the seller of a good or a service connected to the network consults the Blockchain which is a common file to the entire community. In this way, the computer verifies on the blockchain that the Bitcoins sent by the buyer for its purchase have not been already spent by him for another transaction. Because of the possibility of a simultaneous double spending, a transaction is considered valid only if it appears in the Blockchain. To be assured of irreversibility (eg before sending the book you have sold you want to be sure that the buyer has sent to you the payment in Bitcoin), the seller has to wait ten minutes for seeing the transaction validated on the new block[10].

Once a new block created on the blockchain, the Bitcoin protocol gives a new contextual element (k) to the hashcash function. This element triggers to the miner community a new round of roughly 10 minutes.

The Bitcoin protocol plans to divide by two every four year the amount of Bitcoins distributed to miners (nodes). In 2009, the prof-of-work was rewarded with 50 bitcoins. The reward decreased at the level of 25 in 2002 and the decrease will be continued until it tends towards zero. In this way, in year 2140, the total amount created of bitcoin will be equivalent to 21 million of Bitcoins. After year 2140 no more Bitcoin will be created for rewarding the creation of a new block. To preserve the incentive for miner to build the blockchain, a commission for adding a new block to the blockchain is planned by the Bitcoin protocol (Delahaye, 2014). Accordingly, the supply of Bitcoins follows a predictable and finite steady state. Like Gold, the total number of bitcoin is capped. However, unlike gold the mining process of bitcoin is not subject to the hazard of new discoveries. The mining of gold does not follow a steady pace. The predetermined path of the Bitcoins creation process is at time, a strength and a weakness. It is a strength because Bitcoin is not subject to monetary supply shocks. It is a weakness because this

[8] In the founder paper of the Bitcoin protocol published on the Internet under the name of Satoshi Nakamoto, miners are called nodes.
[9] For privacy bitcoin expect the miner to use a different reward address (Public Key) on each successful block.
[10] Bitcoin rate of work is called the network hashrate in GH/sec.

cryptocurrency is not suited to adjust shocks on money demand. A Currency is useful inasmuch as it can be used to buy goods or services. In this intention, the supply of money has to rise and fall in order to maintain the vector of relative prices stable even as people's demand for money varies. In other words a currency needs to be elastic.

The theoretical literature on "memory" is particularly suitable to study the role of the blockchain both on the supply of Bitcoins and on monetary transactions in Bitcoins. In this literature, Memory is a publicly observable record of past transactions that buyers and sellers can consult prior to transacting (Kocherlakota, 1998a)[11]. Money is not essential when agents have access to memory. Luther and Olson (2015) demonstrated that the blockchain technology by providing a public record of past transactions is able to facilitate exchange in much the same way as traditional hand-to-hand currencies. The blockchain is simply a form of memory and to be aware of such a memory character of this cryptocurrency, we have to describe succinctly how a transaction in a block is technically done.

Assume a payment of N Bitcoin (BT) from a buyer (B) of a good or a service to a seller (S). The buyer holds 2 cryptographic keys namely one public key (Bpub) and one private key (Bpriv). The private key is a password that allows someone to spend bitcoins in his online wallet (the public key). The buyer uses his private key with a writing function (W) and sends the message N' to the seller (see graph 1). N' is the codification of the amount of N Bitcoin paid to the seller. All the community of Bitcoin can check that the seller is the writer of the message because only this seller can sign this specific message with his private key.

$$W(Bpriv, N) = N' \qquad (1)$$

In the aim of decoding the message N', the seller uses a reading function (R) with the public key of the buyer (Bpub). He can so accredit the payment transfer from the Bpub to his public key (Spub) for the price of N Bitcoins. Public keys are actually electronic purses. In traditional interbank systems, this corresponds to account numbers. Bitcoin users must pay a fee when sending a transaction on the network.

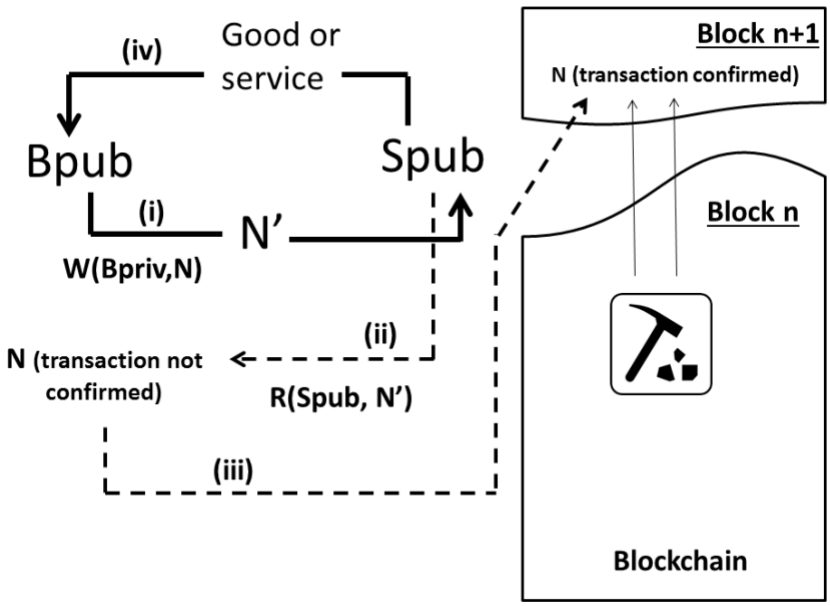
$$R(Bpub, N') = N \qquad (2)$$

[11] "Memory is defined as knowledge on the part of an agent of the full histories of all agents with whom he has had direct or indirect contact in the past" (Kocherlakota, 1998a)

The reading function allows the buyer to read the message (N) of the seller without knowing the private key of the seller.

Approximatively 10 minutes later, the transaction appears in a new block of the blockchain, like described above. A block certifies on average roughly between 1500 and 2000 transactions[12].

Figure 1: Confirmation of a transaction in a new block



In graph 1, steps (i), (ii), (iii) and (iv) describe the ordering of operations from the writing of the initial message to the delivery of the good or the service sold.

The blockchain technology allows quasi-anonymous transactions. The public key - i.e. the electronic purse - does not contain any personal and traceable information concerning its owner[13]. A paper banknote owns the same features. Accordingly, the Bitcoin is literally a fiduciary money based on trust. Confidence is especially as important as the BlockChain recounts transactions and their value in Bitcoins but it is impossible to know the nature of the goods or services paid for such transactions. Consequently, it is very

[12] https://blockchain.info/fr/stats
[13] Here is an example of a public key: 1GMwXuiCcKpRUo3psJCFaLHDCMpA52q8Ee

hard to estimate the internal value of the Bitcoin. Moreover, most of the transactions are used to exchange goods or services in the Dark Web which makes impossible the calculus of the relative price vector. Assuming that the Bitcoins users adopt a rational behaviour and that such users cannot estimate the inflation rate in Bitcoin, the only way to estimate the price of what they buy or sell in Bitcoin is to reason in their own public currency. They have in mind the relative price vector in their own public currency and they simply convert in Bitcoin price by using the exchange rate.

3. Modelling for reinforce the reliability of online transactions

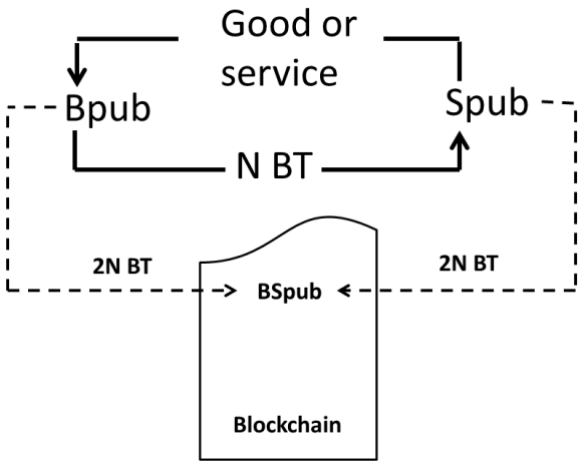
The blockchain allows economic agents who have no particular confidence in each other and who do not know each other to collaborate apart from a central authority. In other words, the blockchain with times creates trust. Cryptocurrencies used for online transactions Blockchain based, are *de facto* fiduciary monies. This characteristic, much more marked for the Bitcoin than for the traditional paper money, is exacerbated in the online market. Literally, the word "fiduciary" is derived from the Latin word *fides* which means trust. Even recorded and validated in a Blockchain, most on the transactions on the Internet still suffer from lack of trust between sellers and buyers. Trade between individuals on the Internet is hindered by the inability to establish a trusting relationship with a stranger. The seller may send a good to the buyer and never receive the payment for it. Alternatively, the buyer may send the money and never receive the good in exchange. Such a problem is not trivial and the main aim here is to model a solution for reinforcing the credibility of online transactions based on the blockchain technology and prove the robustness of such a solution by using game theory. Many merchant websites recommend direct exchange by meeting face-to-face. Sending against repayment is a solution but does not work well.

Some websites offer three solutions to limit the risks:
- blocking the money sent before the reception of the product,
- Proposing a rating system that indicates whether the people were correct in their previous transactions ("reputation system"),
- offering an insurance.

There is a much better solution thanks to the timestamp server in the core of the Blockchain. The model proposed here is derived from Delahaye (2015) work and could usefully be implemented by the Bitcoin Community. Let's consider an online transaction for a specific product paid for the price of n Bitcoins. The buyer (B) and the seller (S) cannot exchange face-to-face. A trust question must be solved. The buyer before sending n BT to the seller wants to be sure to receive its purchase and the seller wants to be sure to receive the money before sending by post its sale.

A common public key to the buyer and to the seller is created, like a common wallet[14]. Such a common public key (BSpub) is added to the blockchain and locked for a specific period. The buyer transfers the amount of 2n BT from his public key (Bpub) to common public key and the seller does the same operation with his own public key (Spub). Like this, a total amount of 4n BT is credited to the common public key (see graph 2).

Figure 2: Temporary common wallet in the Blockckain



This amount of 4N BT is held captive until the transaction is solved. Neither the buyer nor the seller can recover the amount of 4N BT with their own signature. The seller sends the product to the buyer and the buyer sends the amount of n BT to the seller. If money is not unlocked in time (Let's say less than 10 minutes), either party can destroy all the

[14] A public key corresponds to a specific Bitcoin address.

money in the common public key. Once the product received by the buyer and the money received by the seller done, both parties sign each the common public key and can each recover their 2N BT of deposit. It is impossible for one co-contracting party to recover his security deposit of 2N BT without the signature of the other co-contracting party.

Locking money on a specific joint wallet for a fixed period of time is a solution able to solve a Nash equilibrium strategy called mutually assured destruction (or MAD)[15]. The threat of Mutually Assured Destruction (MAD) means that neither the buyer nor the seller has any incentive to not unlock the deposit in Bitcoins by signing the common public key, because that would inevitably lead to a loss of the amount receivership. According to Nowak and Highfield (2011), "Cooperation doesn't emerge in the Prisoner's Dilemma unless you have some mechanism in place. The simplest mechanism that allows this is called direct reciprocity." The creation of a common public key between two co-contractors in Bitcoins introduces a mechanism of direct reciprocity. The defining feature of a direct reciprocity game is that strategies will depend on the past history of behaviors. The common public key created for the joint deposit appears in the public BlockChain viewable by the entire community of Bitcoins users. If any kind of scam appears the buyer and/or the seller would suffer of a reputational damage among the community.
The following MAD game model described here includes a guaranteed deposit (D) for each player (seller or Buyer) for a traded good with a value in BT of n. The payment and the unlocking of D are made simultaneously. Similarly, the receivership takes effect when the two contractors have agreed for it to happen. Everyone sees what the other commits so it is not possible that one contractor makes a deposit on the common wallet and the other not.

Case 1: The seller does not send the sold good to the buyer

Losses of each player appear in brackets i.e (loose of the Buyer, losse of the Seller).

Seller Buyer	Sign to unlock	Not sign to unlock

[15] The strategy of Mutually Assured Destruction and the acronym MAD are due to John von Neumann

Sign to unlock	(0,0)	(-D, -D)
Not sign to unlock	(-D, -D)	(-D,- D)

If 0>-D ⇔ D>0, signing to unlock D is the dominant strategy for the 2 players.

Case 2: The seller sends the good to the buyer

Seller Buyer	Sign to unlock	Not sign to unlock
Sign to unlock	(0,0)	(-D+n, -D-n)
Not sign to unlock	(-D+n, -D-n)	(-D+n, -D-n)

If the buyer never sends back the money after the retrieving of the good, the buyer loses D and gains the value of the good (-D+n) and the seller loses D and n (-D+N).
-D +n <0 ⇔D>n
If D>n, signing to unlock D is the dominant strategy for the 2 players.

The amount receivership by the two players must be higher than the value of the shared object. Otherwise the first player receiving the sending of another has no interest to send what he promised to send, even if he loses the amount sequestered. However, the sum receivership must not be too important because the small risk that the amount is not recovered would be too great compared to the price of the exchanged item. The main blockchain interest is precisely to allow secured and trusted operations without requiring a trusted third party. Anonymity is preserved which is the main characteristic of fiduciary money like the Bitcoin.

Beyond the single case of Bitcoins, the Blockchain is the third necessary required for many operation based on trust. It is the universal sheet used to know and verify who holds various digital rights. A blockchain is the engine that provides the basis of bitcoin which requires consensus to execute transactions and other operations securely and controlled without central oversight authority. This is possible because transactions and

all others operations are validated by the entire network. The validation by the community of Bitcoin users reinforces the trust in the system. Messages can be added to a blockchain in clear or encrypted. For instance, one acknowledgment of debt can appears encrypted in the blockchain. If the debtor respects his commitment, the acknowledgment of debt stays encrypted. If not, the owner of the account payable publishes the key decryption and anyone can be aware of the failure of the debtor.

4. Modelling sidechains pegged to the main blockchain technology

The blockchain is the key innovation that has made Bitcoin possible. By tracking each coin for each transaction, the blockchain protects against fraud and serves to prevent a buyer from spending the same bitcoin more than once. The robustness of the Bitcoin's blockchain from its creation in year 2009 allows to the blockchain technology to be generalized to any type of contract or document that would usually require a third party.

For example, thanks to the blockchain technology, it becomes possible to make cheap tamper-proof public databases for land registries. Documents can be notarized by embedding information about them into a public blockchain. A notary dedicated to vouch for them is no longer needed. The blockchain is in this case a record of who owns what instead of having a series of internal ledgers in numerous notary offices. Let's say Mr. Smith buys a castle in Kirkcaldy, Scotland, to Mr Hume for the price of N (N Bitcoins or any N units of private or public currency). Mr Smith sends to Mr Hume an encrypted message N' by using his private key (Bpriv). Mr Hume decodes the Message N' with his reading function and the public key of Mr Smith (Bpub). The purchase of the castle is broadcast to all nodes and each of them collects it into a block. When a node finds a proof-of-work, it broadcasts the block to all nodes. The proof-of-work is devoted to check if the Castle is really owned by Mr Hume and that he is allowed to sell it. Nodes accept the blocks only if the transaction is validated by the proof-of-work. Nodes express their acceptance of the block by working on creating the next block in the chain. The first node able to find the proof-of-work is allowed to add the new block to the blockchain. Mr Smith, for his part, sends transaction fee to the node "winner" by using his public key (Bpub). All nodes can anytime check the history of each block therefore the blockchain

of land registry can be much more reliable than a large number of notarial offices. By using both his private and public keys an owner can always prove his property.

The per-transactions fees are for the nodes the only motivation to permanently check, certificate and validate the blockchain. At this point, the question of the currency used by the blockchains is crucial. There are two possibilities.

- Transaction fees are paid in a private cryptocurrency already based on the blockchain technology. Also in this case gateways have to be created from the blockchain of the cryptocurrency (for instance the Bitcoin) to the blockchain of the land registry.

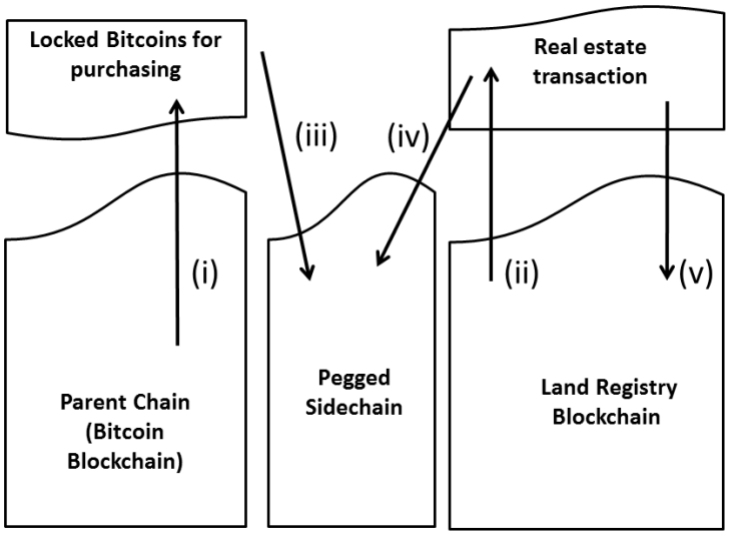
- Transaction fees are paid in a public currency like the Euro or the US dollar. In this case, a gateway has to be created to introduce legal money in a public key (an encrypted wallet).

In both cases, a sidechain model can be effectively implemented. A sidechain is a blockchain “pegged” to the main blockchain so as to allow transfers of key information from one chain to the other. The sidechain validates data from other blockchains. The sidechain technology creates gateways between blockchains. Let's examine how the two possibilities could be implemented.

With a private cryptocurrency like the bitcoin, the sidechain can be a pegged sidechain of the parent chain that is the Bitcoin's Blockchain. According to Adam Back and alii (2014), a pegged sidechain is "a sidechain whose assets can be imported from and returned to other chains; that is, a sidechain that supports two-way pegged assets." More precisely, the two-way peg mechanism freezes Bitcoins so they can only be released according to a decision by some other blockchain. The transfer process is demonstrated in graph 3.

Figure 3: Recording a real estate transaction payable in Bitcoins in the land registry's blockchain

Olivier Hueber,



(i) An amount of as-yet unspent Bitcoins are locked by the buyer. The locked Bitcoins holder publishes its public key (Bpub) and proves its property by signing with its private key (Bpriv). The locked Bitcoins are sent to a specially formed Bitcoin address designed so that the coins are now out of control of their holder and out of the control of anybody else either. The locked bitcoins can only be unlocked only if somebody can prove they're no longer being used elsewhere in the network.

(ii) The land registry blockchain temporarily encrypts the ongoing non confirmed transaction in a specific block.

(iii) The buyer sends the encrypted message (N') corresponding to the amount paid in Bitcoin (N) for the transaction by using his writing function (W) and his public key (Bpub).

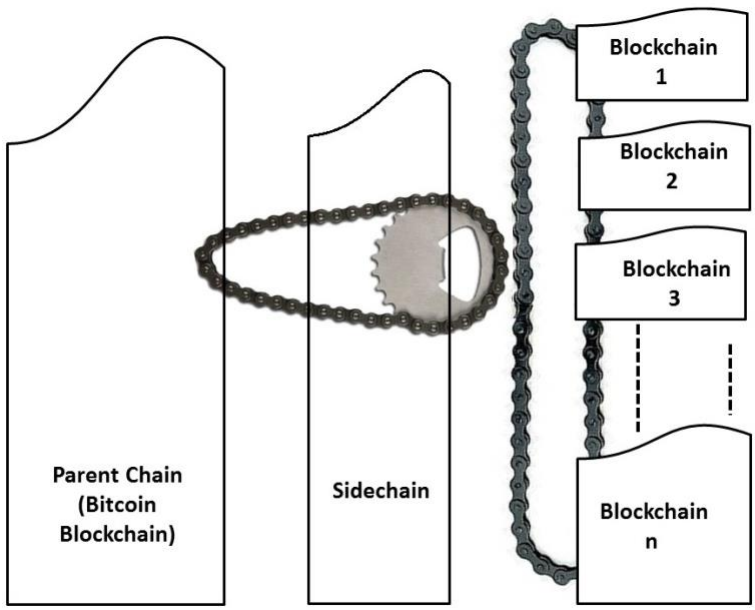
(iv) The seller sends to the sidechain a cryptographic message containing firstly the proof of his property and secondly his agreement to trade with the buyer for the amount of N Bitcoin. A new block is created in the sidechain and a contest period starts between nodes in the aim of proving the veracity of the

transaction. The organization of the contest period based on a proof-of-work can be connected with a proper mining process inside the sidechain.

(v) Once the transaction validated by the sidechain, a new block containing the certified transaction is added to the blockchain of land registry.

Beyond the example of the land registry blockchain, the sidechain can be used by many blockchains. A pegged sidechain can be conceived as an "open blockchain" linking any kind of blockchains. It is not necessary to multiply sidechains. Like for a bicycle, the pegged sidechain modeled here is the transmission chain between blockchains (see graph 4). A sidechain allows for the creation of multi-block chain ecosystems in which assets can be exchanged and transferred.

Figure 4: Multi-block sidechain ecosystem with the Bitcoin blockchain as a Parent Chain



Olivier Hueber,

The Blockchains number 1, 2...to number n can be linked all together by the sidechain. For instance the blockchain number 2 could be a blockchain devoted to register and validate diplomas and the blockchain number 1, could be the land registry blockchain. The sidechain can check if an owner of a specific diploma (let's say a Doctorate in Dentistry), is allowed to buy a specific property (let's say a Dental clinic). If not, the sidechain does not validate the transaction and no block is added on the blockchain 1.

The implementation of the sidechain ecosystem providing gateways between different blockchains is harder to conceive if the parent chain is not a cryptocurrency based on a blockchain, such as is the Bitcoin. Yet the stake is high. Due to both the multiplicity of the blockchains and the development of private cryptocurrencies (i.e. Bitcoins and others), Central Banks cannot have an effective control on many online transactions. One effect of private e-monies, like the Bitcoin, is a permanent decrease in Public money demand and consequently in the Central Banks reserves (Fullenkamp, Nsouli, 2004). We are not yet there of course; the total amount of private currencies in circulation (online or not) is insignificant compared to the value of the aggregate stock of public money. It is nevertheless true that Central Banks need to be vigilant on that point. Inside a public monetary regime, the Central bank influences agents' decision-making, through their policies of interest rate, exchange rate, asset prices or credit facilities.

The scientific approach adopted here for use of the concept of monetary regime in the aim of studying the blockchains of cryptocurrencies is enlightening because "*a primary concern in monetary economics is whether a purely private monetary regime is consistent with macroeconomic stability*" (Sanches, 2016). According to Heymann and Leijonhufvud (1995), a monetary regime means, "on the one hand, a system of expectations on the part of the public that governs their decision and, on the other, that pattern of behaviour on the part of the policy-making authorities that sustains these expectations. The monetary regimes forms a crucial part of the environment in which both the public and the authorities have to make their decisions" [16]. In the strictest sense of the definition, the monetary regime is a pure equilibrium concept with perfect symmetric information. Such a definition is suitable for the study of the emerging world of blockchains. All the transactions confirmed by new blocks on blockchains are available for the entire community and can be anytime checked by it. The information is symmetric and perfect. The only unknown variables are the real identities of public key's

owners but these hidden identities are apart from the blockchain protocol. The success of Central bank monetary policies requires positive demand on government money because a Central Bank can influence real economy mainly through interest rates. If the government's money demand decreases as a consequence of the spread of private cryptocurrencies the real effect of the public monetary policy weakens. Living in an economy where different monies coexist, forces people to adapt every aspect of their economic activities to this new environment. The most routine daily transactions must be organized differently. As explained by Heymann and Leijonhufvud (1995), "Money is not a refrigerator. The picture of money as a service-producing asset is incomplete without a look at transactions practices". The monetary regime tends to be parceled out by different communities of payment. Any economy operating with different currencies destroys the public character of the money. Different categories of economic agents may be excluded from specific markets. A private cryptocurrency creates injustice toward those for practical, legal or financial reasons cannot access it. A Central Bank must supply all the markets (online or not) with its public money. Any economy operating with different currencies destroys the public character of the money. Different categories of economic agents may be excluded from specific markets. It is well-known from Aristotle's writings that money (*nomisma*) must supply all the markets[17]. For the moment, no reliable footbridge between various communities of e-payment exists. Admittedly, many website propose an exchange rate service for converting different private e-currencies. Such websites are in any way connected neither to the official interbank systems nor with a "supraweb" currency acting like a unit of account within a multilateral clearing system in the worldwide web.

The public monetary regimes (for instance the Euro zone) have no grip on what we could qualify as private cryptocurrency regimes. The public currencies - like the Us Dollar or the Euro - as well as their interbank systems are not linked to a blockchain. One solution to link reliably the public money and the private cryptocurrencies would lie in the creation by Central banks of a "supraweb" currency. All the transactions negotiated in private electronic monies would gain to be valued and cleared with a "supraweb" currency linked, recognized and accepted by the official interbank system. Such a solution which requires a centralized organization (a clearing house) akin to a traditional bank does not fit to the decentralized aspect of the cryptocurrencies based on the

---

[16] D. Heymann, A. Leijonhufvud 1995, p.39

Olivier Hueber,

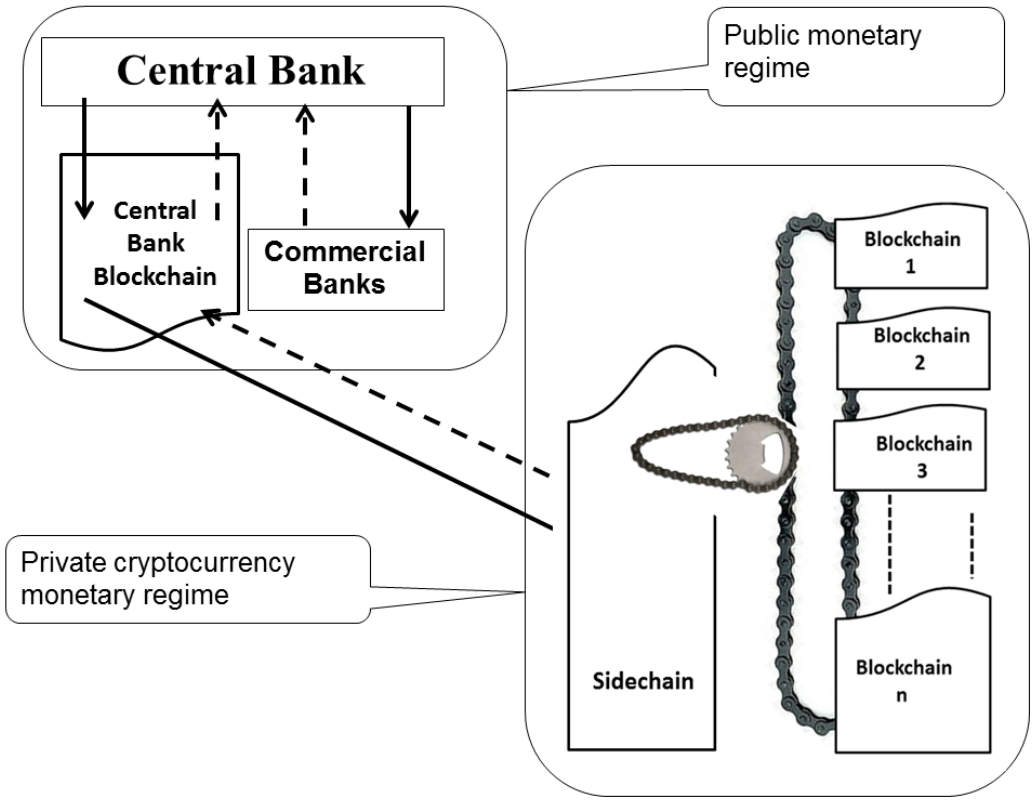
Blockchain technology. A research has to be done in order to peg official monetary regimes with the currently shaping private monetary regime around the Bitcoin blockchain. The issue of creating a blockchain by one or more central banks is posed. Such a public blockchain could create a crypto-currency (for instance BitUs Dollar or BitEuro) and could peg this legal tender token to a sidechain. In this way, the sidechain could act as a gateway between public and private monetary regimes (Graph 5).

A public Blockchain could be at a time decentralized and subject to a cryptographic protocol written by a Central Bank. Two solutions are available. The first solution is to trade the Bitcoins (BT) for obtaining US Dollars (USD) in a private exchange platform. These platforms already exist and are numerous on the Internet[18]. There is no security with these cryptocurrency exchange offices. Using these platforms is at the risk of their users. The second solution would be to use the public blockchain of the US Federal Reserve - assuming this blockchain exists.

The central Bank by using a mining process similar to the Bitcoin's one could give a contextual element to a hashcash function in the aim of creating blocks at roughly the same pace than the evolution of demand of USD for BT. In other words, the pace of the public cryptocurrency creation could fit with its demand coming from the private cryptocurrency regime. Of course, the value of the exchange rate USD/BT is subjected to arbitration by the Bitcoin holder looking for US Dollar. This holder of Bitcoin compares the exchange rate USD/BT given by the cryptocurrency exchange offices, with the price of the USD for BT written in the latest block of the public blockchain. Eventually, a convergence of exchange rates between the two monetary regimes emerges.

Figure 5: Central Bank Blockchain

[17] The word 'Money' (*nomisma* in the Ancient Greek Language), doesn't come from its intrinsic nature but from the law (*nomos*).
[18] www.coinbase.com, https://paxful.com/



With a cryptocurrency monetary regime pegged on sidechains, each blockchain (monetized or not) can issue their own tokens and enable these tokens to be transferred to other blockchain or traded for other assets and for other currencies (public or private). All this is made possible without a trusting central authority like an official last resort lender (for instance a Central Bank). The traditional public interbank system driven by the Central Bank is not modified in its own operating rules. The refinancing relationships between the Central Bank and the Commercial Banks persist. The novelty here lies on the possibility for commercial Banks to access to the private cryptocurrency monetary regime by means of the Central Bank's blockchain.

5. Conclusion

Olivier Hueber,

The sidechain technology offers a possibility to connect publics monetary regime with private monetary regimes. This connection is reliable because the public aspect of money is preserved. Moreover, the confidence in online transactions can be reinforced by adopting new protocols in the blockchain like the mechanism of the common wallet described here. Creating sidechains allows Central Banks to regain the control on the proliferation of cryptocurrencies. Admittedly, the cryptographic protocol enabling the creation of new blocks inside the Central Bank's Blockchain must be subject to a forthcoming analysis. Nobody can determine today if the Bitcoin will become unavoidable in the years to come and if the Bitcoin will be the keystone of a private cryptocurrency regime rooted on the sidechain technology. Whether the Bitcoin become the parent-chain or not, the blockchain technology allows in a bottom-up process the emergence of a reliable monetary regime able to trade with many different private tokens or assets. The intrinsic decentralized character of a cryptocurrency based on the blockchain technology fits very well with the peer-to-peer online transactions. Such a character must be preserved without a strict control of any public central bank. Implementing a control by public monetary authorities would be pointless and inefficient. The official interbank systems are part of a top-down mechanism while the Blockchains are guided by a bottom-up principle. Monetary authorities must establish many institutional arrangements in society to ensure the reliability of interactions between communities of e-money holders. The Sidechains hooked to numerous blockchains shape a reliable private cryptocurrency regime. Such a regime can be in turn hooked to the public monetary regime through the creation of public blockchains whose protocol is decided by Central Banks. Implementing public blockchains can make reliable a decentralized private monetary regime in coordination and in conformity with the public monetary regime driven by central banks. The coordination mechanisms and the gateways described here have to be deepened and be subject of subsequent analysis. More particularly, a research on contributions and limits of a demurring process linked to the sidechains has to be done. The tokens locked before transiting to another blockchain thanks to a sidechain could have a demurrage fee. The concept of demurrage fee is not new. It was proposed initially by Silvio Gesell (1929). In the

complementary and the cryptocurrency currencies field, demurrage is a cost associated with owning or holding an electronic token. Demurrage keeps the currency supply stable while still rewarding miners of electronic tokens. Thereby, sidechains can become the cornerstones of an effective coordination of uncountable electronic private currencies operating under the blockchain principle. In addition to the many economic benefits of this solution, it is possible to solidify it by introducing a demurrage mechanism. It is this aspect that needs to be deepened.

Olivier Hueber,

References

Aristote, Éthique à Nicomaque, Livre V, 1132 b 21-30, pp. 246 et s.

Back A., (2002) "Hashcash - A Denial of Service Counter-Measure", technical report, August

Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timon J., Wuille P. (2014), Enabling Blockchain Innovations with Pegged Sidechains, commit 5620e43, 2014-10-22

Cukierman A., (1992) "Central Bank Strategy, Credibility and Independence: Theory and Evidence." *The MIT Press*, Cambridge, Massachusetts.

Delahaye, J.P. 2014, Le Bitcoin, première cryptomonnaie "1024" *Bulletin de la Société Informatique de France*, n°4, pp. 67-104, octobre 2014.

Delahaye J.P., (2015) "Les blockchains, clefs d'un nouveau monde », Pour la science, n°449, pp. 80-85, mars.

Friedman B., (1999), "The Future of Monetary Policy", *International Finance*, November

Gesell S., (1929) "The Natural Economic Order: a Plan to Secure an Uninterrupted Exchange of the Products of Labour", Trans. Philip P. (1916), Berlin Neo-Verlag ed.

Heller D., (2017), "Do Digital Currencies Pose a Threat to Sovereign Currencies and Central Banks?", Policy Brief, Peterson Institute for International Economics, April

Jevons W.S. (1850), *Money and the Mechanism of Exchange*, Kegan Paul, London 1975.

Keynes J.M. (1980), The Collected Writings, Volume XXV: Activities, 1940-44 - Shaping the Post-war World: The Clearing Union., Basingstoke

Kocherlakota N.R. (1998a) "Money is memory", Journal of Economic Theory, 81(2):232-51

Nsouli S, Fullenkamp C, (2004) "The Regulatory Framework for E-Banking", Banking, Payments, and ICT conference, Beirut, Lebanon, June 6–8.

Luther, William J., Olson Josiah (2015), Bitcoin is Memory, *Journal of Prices & Markets*, 3(3), pp.22-33.

Nakamoto S., (2009) "Bitcoin: A peer-to-peer electronic cash system", https://www.bitcoin.org/bitcoin.pdf

Sanches D., (2016) On the inherent instability of private money, Review of Economic Dynamics, Vol 20, April 2016, Pages 198-214

Smith, Adam. 1981 [1776]. An Inquiry into the Nature and Causes of the Wealth of Nations. The Glasgow Edition of the Works and Correspondence of Adam Smith. Edited by R.H. Campbell and A.S. Skinner. Textual Editor W.B. Todd. Oxford: Clarendon Press. Reprinted, Indianapolis: Liberty Classics.

White L.H., (1984) Free banking in Britain, Theory, experience and debate, 1800-1845, Cambridge University Press, Cambridge.