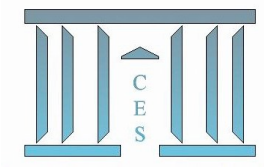
The Digital World: II – Alternatives to the Bitcoin Blockchain?

Dominique Guegan

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Documents de Travail du
Centre d'Economie de la Sorbonne

CES Working Papers



The Digital World: II – Alternatives to the Bitcoin Blockchain?

Dominique GUEGAN

2018.16

Maison des Sciences Économiques, 106-112 boulevard de L'Hôpital, 75647 Paris Cedex 13
https://centredeconomiesorbonne.univ-paris1.fr/
ISSN : 1955-611X

The digital world : II - Alternatives to the Bitcoin Blockchain?

Dominique GUEGAN

University Paris1 Panthéon Sorbonne, LabEx ReFi

Ca'Foscari University in Venezia, IPAG Business school

Abstract

In a previous paper (Guégan, 2018 b), we explain some limits and interests of the Bitcoin system and why the central bankers and regulators need to take some decision on its existence. In this article we develop some alternatives to the Bitcoin blockchain which are considered by the banking system and industries.

I - What is a blockchain ?

A blockchain runs on a set of nodes, each of which may be under the control of a separate company or organization. These nodes connect to each other in a dense peer-to-peer network, so that no individual node acts as a central point of control or failure. Each node can generate and digitally sign transactions which represent operations in some kind of ledger or database, and these transactions rapidly propagate to other nodes across the network. Thus, blockchain is a technology of storage and transmission of information, transparent, secure, and functioning without a central control party. By extension, a blockchain is a database that contains the history of all the exchanges made between its users since its creation. This distributed database is shared by its different users, without intermediaries, which allows everyone to check the validity of the chain.The blockchain gets its name from the fact that it constitutes a record of all transactions grouped into blocks that form a chain. The creation of this chain of blocks occurs through consensus algorithms that diverge depending on the blockchain at issue. The ledger's integrity is maintained through consensus reached by the participants. Thus, blockchains are complex systems, enabled by the combination of a distributed computer networks, cryptography and game theory.

The blockchain first emerged as the technology enabling the peer-to-peer digital cash Bitcoin, which explains why blockchains and cryptocurrency are often taken as synonymous whereas they are not. While the blockchain has rendered Bitcoin possible it has since been relied on by innovators to enable manifold other applications, the list of which is expected to significantly increase in the future. More generally, information and assets stored on a blockchain can be securely and accurately maintained cryptographically through keys and signatures that determine who can do what with the shared ledger.

Blockchain is based on different kinds of sofware architectures ideally including some properties as immutability, integrity, fair access, transparency, non-repudiation of transactions, equal rights. Some limitations can exist : data privacy (anonymity on one hand, open source system on another hand : everyone knows who makes exchange on the blockchain), scalability. There are scalability limits on (i) the size of the data on blockchain, (ii) the transaction processing rate, and (iii) the latency of data transmission. The number of transactions included in each block is also limited by the bandwidth of nodes participating in leader election (for Bitcoin Cash the current bandwidth per block is 1MB).

We can distinguish different generations of blockchains : it concerns the storage of data, the mining (different kinds of Proofs). It exists also a differentiation between permissionless blockchain (or public

blockchain), and permissioned blockchains (or private blockchain). These categories are specified in the next sections.

II - What are the different classes of blockchains ?

We can distinguish three kinds of concepts concerning the blockchain status : public blockchain, private blockchain and consortium blockchain. Their uses and objectives are not the same.

Bitcoin Blockchain as Ethereum Blockchain are public blockchains mainly based on Proof-of-Work, opensource sofware and consensus protocol. In a consensus protocol such as Proof-of-Work, the transactions cannot be tampered as long as no single miner controls more than 50% of the network's hash power. For these public blockchains all records are visible to the public and everyone can take part in the consensus process.

Private blockchain necessitates a right to enter in the network. In this latter case they develop a private ledger which can be scalable, increasing centralization, decreasing in a certain sense the transparency and is likely used for business exchange regarding database management, settlement delivery activities and auditing. The private blockchain is fully controlled by one organization, with a closed group of known participants, which implies a centralized rather than a decentralized network.

Lastly a consortium blockchain is partially decentralized, where transactions are validated by a selected set of nodes. Private and consortium blockchains may permission other users to read records in the blockchain. Transactions in private or consortium blockchains are editable as long as the major participants have reached an agreement, and hence a strong consensus protocol such as Proof-of-Work is not required.

III - Evolution of the Blockchain Protocol

Looking at the rise of blockchain technology and the highly topical and relevant social debate on sustainability, some researches investigated the developments in hardware and software for bitcoin mining and what that means for energy consumption, outlining a number of alternatives which lead to less energy consumption and thus smaller burden on the environment.

The first generation of Blockchains : the Bitcoin Blockchain

The most relevant feature of Bitcoin is the concept of decentalization which provides a total independence from any central autority. Bitcoin is a peer-to-peer network where every node participates in the realization of a distributed ledger. From a technical approach it is based on a distributed consensus protocol. The result is a distributed ledger containing the list of transactions which is constantly broadcasted in the network and that grows with new transactions. The main question is to verify that only valid transactions appear in the blockchain and this is done thanks to cryptography. The other question is to avoid double spending attempt, this cannot be done by cryptography, and as soon as we are on a peer-to-peer network synchronisation, this is not easy to be reached, because the timestamp cannot determine which was the first spending. To face this problem, the Bitcoin blockchain has created a mechanism to incentive miners' honest behavior. This honest behavior consists in giving a block reward to the nodes that manage to place their blocks first on the blockchain and stays in the long term blockchain, (such block reaches the consensus and it will not be discarded anymore. A block containing invalid transactions will not stay in the chain).

On July 14, 2010, Satoshi Nakamoto set a limit of 1 MB for each block created. At that time, the transactions were free and the developers were concerned that attackers could not "spam" the network

by creating huge blocks containing fake transactions and permanently inflating the chain of blocks that everyone must keep. This limit was intended to prevent this kind of attack until a better solution could be put in place. Since 2016, 1 MB limit is reached and a long controversy and a discussion on how to increase the number of possible transactions have arised. Indeed, when the number of transactions has finally reached the block size limit, the pool of pending transactions is saturated. The only way to integrate a given transaction into the blockchain faster for a user was to increase transaction fees (to, for instance, almost $ 25 in January 2018, compared with less than $ 1 before 2016).

Several proposals were made to increase the number of possible transactions, a first step called "segwit" was implemented in August 2017. A next step, Segwit2x, doubling the size of the blocks, was to be implemented in November 2017, but was abandoned due to lack of consensus. Nevertheless a fork arises August 1st, 2017 and a new Bitcoin is created based on a protocol which permits to create blocks whose size is 2MB. Thus currently, it exists two Bitcoin systems creating two Bitcoins currencies: the historical Bitcoin (BC) and the Bitcoin unlimited (BU).

Although independence represents one of the most important aspects of bitcoin, on the other hand it creates an intrinsic rigidity. If a procedure changes without user approval (e.g., from Bitcoin core-BC, to Bitcoin unlimited-BU), a different cryptocurrency is de facto created. In this condition, the logic of market competition between alternative solutions becomes the only possibility and the government of the original protocol is abandoned. It seems that real independence of the bitcoin system is not achievable, because its anarchism is compromised by the way that the system operates in practice: it favors the most powerful producers of the currency to become even more powerful creating monopolistic practices. Thus two main points have been considered, how to decrease the energy costs from one hand, and in another hand how to extend the possibility of the protocol, not to restrict it to create cryptocurrency.

As we recall in Guégan (2018) the Bitcoin blockchain is based on Proof of Work (PoW) necessitating to solve a mathematical problem permitting valid transactions and avoiding double spending. Other cryptocurrencies mineable coins using Proof-of-Work consensus algorithm generating new blocks on the blockchain, for instance Ethereum, litecoin, etc. For all these currencies the blockchain protocol is not the same as for Bitcoin and does not use as much energy, nevertheless new protocols are considering for mining.

The second generation of Blockchains

Dealing with the criticism that Proof-of-Work as applied in Bitcoin wastes energy, some thoughs try to replace the computation of hashes by more meaningful tasks. This second generation of blockchains wants to make the system more sustainable and is mainly based on Proof-of-Stake (PoS) which does not use computational power but part held in tokens into the technology in a deteministic manner. The more one invests in the blockchain, the more has a chance of winning and having the reward. But it exist also other protocols to solve the question of energy's consumption.

In Proof-of-Stake, users are required to prove the ownership of their amount of coins. Users create ' coinstake' transactions in which they send the coins in their possession to themselves and add a predefined percentage as reward. In the mining process of PoS, still the hash of a block has to be computed that is smaller than a target value. A block however does not include a nonce value that can be modified by the miner, but a time-stamp that changes every second. Hence, miners cannot rely on computational power, but they can only compute one hash every second. The miner that wins the block, receives the transaction reward. The difficulty is determined individually for every user: it is inversely proportional to the coin age, which is the amount of coins times the time period that the user

held these coins. Hence, users with a large coin age have a higher chance to mine a block. When a block is mined that includes a coinstake transaction, the coin age of the winner is reset. Users with the highest stakes in the system have the most interest to maintain a secure network, as they will suffer the most if the reputation and price of the cryptocurrency would diminish because of the attacks. In the proof of stake system, miners are replaced by validators. In order to become a certified validator, one must invest a part of his wealth in a stake node. Finally, depending on the value of the stake, the validator will then be able to validate a given percentage of pending transaction blocks. Economical punishments are then used if the validator does not do his certifying work properly. Thus, with proof of stake, instead of mining power, the probability to create a block and receive the associated reward is proportional to a user's ownership stake in the system. An individual stakeholder who has *p* fraction of the total number of coins in circulation creates a new block with probability *p*. The altcoins which use Proof of Stake are for instance Peercoin, (peercoin.net), Nxt (nxt.org), BlackCoin (blackcoin.co), or Novacoin (novacoin.org).)

Delegated proof of stake (DPoS) protocols are a subcategory of the basic Proof of Stake consensus. In these protocols, blocks are minted by a predetermined set of users of the system called delegates, who are rewarded for their duty and are punished for malicious behaviour (such as participation in double-spending attacks). Delegated proof of stake is a generic term describing an evolution of the basic Proof of Stake consensus protocols. In DPoS algorithms, delegates participate in two separate processes: (i) building a block of transactions, (ii) verifying the validity of the generated block by digitally signing it. While a block is created by a single user, to be considered valid, it typically needs to be signed by more than one delegate. The list of users eligible for signing blocks is changed periodically using certain rules. DPoS is utilized in BitShares, as well as proposed in algorithms such as Slasher, Casper or Tendermint. For example, in Slasher, delegates for each block are selected based on stake and blockchain history. The set of delegates for each block is typically small; a notable exception is Tendermint, for which each block can be signed by any of the users of the system. An alternative of DPoS versions is deposit-based proof of stake, in which a delegate need to show commitment by depositing his funds into a time-locked security account which is confiscated in case of malicious behavior.

In Proof of stake, there is no mathematical problem to solve, therefore the energy used for this type of protocol is very low. A combination of proof-of-work and proof-of-stake has been proposed, in which a fraction of the proof-of-work block reward is raffled among all active nodes, while their stake determines the amount of raffle tickets, for instance it is used for Decred.

Other protocols are also proposed : (i) NooShare proposes the scheduling of arbitrary Monte-Carlo simulations as a proof-of-work, (ii) Primecoin proposes the computation of long chains of prime numbers (Cunningham chains), (iii) Permacoin proposes proofs of retrievability, (iv) Another alternative is proof-of-space, where the miner must employ a specified amount of memory to compute the proof, (v) In proof-of-space-time the miner must prove that he stored data over a period of time.

Blockchain of 3rd generation : A third generation of blockchain arises aiming to solve the major problems of previous generations: governance, security, but especially scalability, interoperability and sustainability. These developments are in progress.

Although these alternatives largely reduce the energy consumption as with Proof-of-Work, there still are security issues when applying them to public blockchains.

Another differentiation observed with these successive generation of blockchains is the possibility to develop smart contracts. Smart contracts are sofware programs embedded in a blockchain that can

receive as well as send assets and information. Generally the distribution of information and assets by smart contracts is entirely predefined in code and tiggered by the fulfillment of certain conditions. Ethereum is the most popular platform supporting smart contracts, and it is one of the main difference with the Blockchain Bitcoin. As users of cryptocurrencies need to pay small transaction fees for monetary transactions, users of smart contracts pay small fees for computations executed by the decentralized virtual machine of the blockchain for the smart contract. In the case of Ethereum, this computation fee is called gas. Recently the Ethereum core developing team is currently considering also Proof of Stake as a way to replace its current Proof-of-Work based security system. For instance, the Ethereum Core development team suggested the idea of a self-regulating network where a user caught cheating with his validating right would see his committed stake transferred to the user that caught his fraud attempts.

IV - What are the different features of a blockchain ?

We analyse in this Section some characteristics that users and developers need to take into account when developping blockchain protocols making them attractive for a lot of applications.

Security. A blockchain is a series of blocks that records data in hash functions with timestamps so that the data cannot be changed or tampered with. As data cannot be overwritten, data manipulation is extremely impractical, thus securing data and eliminating centralized points that cybercriminals often target. The key to blockchain's security is that any changes made to the database are immediately sent to all users to create a secure, established record. With copies of the data in all users' hands, the overall database remains safe even if some users are hacked. This tamper-proof decentralized feature has made blockchain increasingly popular beyond its original function supporting Bitcoin digital transactions. It exists several blockchain' protocols which can be used to attain this objective. Because of the energy-consuming side often denounced with regards of the Bitcoin blockchain, solution to cryptocurrencies' energy consumption problems have been developed, and we now have several conceptually different types of security protocols. Those that rely on Proof of Work (the historic solution, i.e. Bitcoin), and those that rely on Proof of Stake (more recent i.e. BlackCoin) or Delegated Proof of Stake (i.e. BitShares) (both kept the time stamping solution). Some have a hybrid solution relying on both concepts (i.e. PeerCoin, Ethereum's Casper and then Slasher). Others are in development.

Concerning the security of a private blockchain, even if it is said that the security level is less than with the public blockchain, it seems not necessarily essential that the level of security be the same as that of an open and anonymous network. As part of a private blockchain all participants are known and normally there is some degree of confidence.

Scalability. With scalability the question is to keep a strong security on the system while having a sufficient speed of transactions. Several approaches have been proposed : (1) The well known lightning network for example is a solution to offchain operation to solve some problems of Bitcoin network and it is still in progress: the intermediate transactions occurring in the payment channel are not included in the blockchain ; (2) The Ethereum also has its share of offchain solutions but will also adjust setting parameters of the blockchain over its lifetime; (3) Ripple or Stellar operate in small closed groups; (4) Cardano uses the Recursive Internet work Architecture focusing on the scalability of the bandwidth; (5) Mini-blockchain is a scheme proposed by Cryptonite ; (6) Namecoin uses merged mining with the Bitcoin blockchain. Other options are proof-of-burn, sidechains…. In that last case, the use of side-chains may become complex for the clients, because they typically need to be

able to process transactions from the main chain and the side-chain. Thus the scalability property is still in development and then competitive solutions are in process.

I**nteroperability**. Blockchains cannot talk to each other at least not without a third party. We call that the interoperability between blockchains. It seems essential to allow cross-chain transactions. To implement interoperability companies need to develop interfaces to which each party need to adopt, or to obtain consensus in the interoperability standard for the whole market, based on principles of openness, transparency, in line with the General Data Protection Regulation (GDPR, https://www.eugdpr.org/). After the public European consultation on blockchain some ideas raise: (i) blockchain based applications which rely on distributed ledger may raise juridictional issues regarding the law applicable and liability issues for events taking place on the ledger; (ii) the legal validity and enforceability of smart contracts protocols stored on the ledger may need clarification; (iii) some uncertainties surrounding the legal status and applicable rules with respect to ICO need to be specified.

Anonymity: Although the Bitcoin blockchain is perceived to be anonymous, research has shown that Bitcoin transactions can be linked to compromise the anonymity of Bitcoin users. Different techniques have been proposed to preserve anonymity on blockchain. Zcash, also called Zerocash or Zerocoin, encrypts the payment information in the transactions and uses a cryptographic method to verify the validity of the encrypted transactions. Other systems use payment containing multiple input addresses and multiple output addresses e.g., CoinJoin, Blindcoin, CoinSwap, Enigma among others. In another side the question of anonymity will become crucial in the future as soon as the regulation will develop specific rules concerning the cryptocurrencies, and also if the question of interoperability is developed in the future.

Immutability. Every chain employs some sort of strategy to ensure that blocks are generated by a plurality of its participants. This ensures that no individual or small group of nodes can seize control of the blockchain's contents. Most public blockchains like Bitcoin use Proof-of-Work which allows blocks to be created by anyone on the Internet who can solve a difficult mathematical puzzle. By contrast, in private blockchains, blocks tend to be signed by one or more permitted validators, using an appropriate scheme to prevent minority control. Immutability denotes something which can never be modified or changed. In a blockchain, it refers to the global log of transactions, which is created by consensus between the chain's participants. The basic notion is this: once a blockchain transaction has received a sufficient level of validation, some cryptography ensures that it can never be replaced or reversed. This marks blockchains as different from regular files or databases, in which information can be edited and deleted at will. In reality for blockchains, there is no such thing as perfect immutability. The real question is: What are the conditions under which a particular blockchain can or cannot be changed? All depends on the protocols used.

For instance, in case of Bitcoin blockchain the immutable property costs a lot, due to the Proof-of-Work whose difficulty has increased by a factor of 350 000 since the beginning, requiring more and more energy to insure that no Sybil attack is possible and then maintening the immutability of the network. But the Bitcoin blockchain is not immutable in any perfect or absolute sense. It is immutable so long as nobody big enough and rich enough decides to destroy it. Private blockchains are far less costly to run, since blocks only need a simple digital signature from the nodes that approve them. So long as a majority of validator nodes are following the rules, the end result is stronger and cheaper immutability than any public cryptocurrency can offer. On the other hand, for enterprises and other institutions that want to safely share a database across organizational boundaries, Proof-of-Work immutability makes no sense at all. Not only it is extremely expensive, but it allows any sufficiently motivated participant to anonymously seize control of the chain and censor or reverse transactions. As

the actors of these blockchains are known, they will be quickly sanctioned. Thus immutable blockchain does not exist totally.

If immutability is assumed for blockchain, this blockchain is probably not GDPR compliant. Thus how to apply the GDPR directive to this technology which by nature is immutable ? Indeed, The GDPR was written on the assumption that we have centralized services controlling access rights to the user's data, which is the opposite of what a permissionless blockchain does. Looking at the GDPR directive we have to be able to remove some data. It is technically possible to rewrite the data held on a blockchain, but only if most nodes on the network agree to create a new "fork" of the blockchain that includes the changes and then to continue using that version rather than the original one. Another possibility is to use the blockchain as a proof of existence and not as a way to contain the data.

Sustainability in time. How to make the blockchain persistant in time? The answer to this question is totally opened. Some projects think to create sutainable blockchains in time, as Cardano or Ethereum. For the moment it seems a little presumptuous to decide that a blockchain has this property due to the dynamic evolution of protocols to create blockchains.

V - What is the regulation for blockchain ?

The positions of the governments are totally dynamic concerning the question of regulation : some wait and see, some propose guidance, some propose sandbox. We specify here the position of the European Commission and of the French government.

In 2017, the European Commission has launched many Blockchain-related research projects, in particular the creation of a European expertise hub on Blockchain technology called the “EU Blockchain Observatory and Forum” which begins in January 2018 and a study to assess the opportunity and feasibility of a EU Blockchain infrastructure. Meanwhile, the European Parliament has developed various initiatives, including an in-depth analysis on its impact and funding proposals in the 2018 EU budget. We observe also that the European Central Bank acknowledges some benefits of the Blockchain technology, as did the ESMA in February 2017.

In France we observe advanced far-reaching legislative projects with the legal bills recognizing the Blockchain technology since 2015. First there is the adoption of the Law of 6 August 2015 (also named “Macron 2 Law”) which empowered the French government to authorize by ordinance the use of distributed ledger technology for the issuance and recordings of the “mini-bonds” which can be transfered in the shared electronic registration technology. The order n ° 2016-520 of April 28, 2016 on the vouchers makes it possible to register minibons (financing of "type bond") on the blockchain. On December 9th, 2017, the blockchain order (officially the ordinance n ° 2017-1674 of December 8th, 2017 relative to the use of a device of shared electronic recording for the representation and the transmission of financial securities) is adopted. The decrees of implementation are expected for June 2018. With this new ordinance, the government wanted to open the blockchain experiment: by moving from the niche sector of minibons to a much larger sector, that of financial securities. From now on, with equal legal value, they can be registered directly on a blockchain, then be exchanged without going through intermediaries such as account keepers, custodians or central depositories

The recent French position is interesting because it is concommittent with the decision taken by the AMF to organize in December 2017 a public consultation on the ICO whose « regulation » could be given during the first semester 2018. Initial Coin Offerings can be described as ways of raising funds through Distributed Ledger Technology (DLT), which results in token issuance. These digital tokens are digital assets issued against a pre-existing cryptocurrency at a price set by a company to finance,

then potentially tradable on a secondary market (on platforms such as Kraken and Poloniex). Unlike traditional financial securities, tokens are very varied and do not all grant the same rights (voting rights, share of capital or any particular advantage ...).

VI – **Conclusion**

The application around the blockchain technology will be developed more and more in the future. We have described some challenging issues concerning this technology. We cannot avoid to discuss the costs associated to the technology itself, and also some recent developments in quantum theory which can question the futur of the blockchain technology.

An important issue relative to the blockchain technology is the costs it arises. Indeed, even if blockchains could reduce transactions costs as it is often mentioned in the literature, they could also generate new kinds of costs. First, while smart contracts reduce part of transactions costs, negotiation costs become more complex in counterparty they are also time-consuming because smart contracts need time and expertise to ensure that all possibilities are taken into consideration by the contract. Another indirect cost is the fact that smart contracts attempt to control exchanges and predict almost every possible future situations, implying less uncertainty. However, sometimes uncertainty can have positive effect on projects. With locked-in contracts, serendipity has a smaller chance to appear and give new opportunities/targets for potential customers. Second, full transparency promoted by blockchains is not ideal because secrecy and privacy are required for business making. Hence, private blockchains may control access to information. Moreover, sometimes transparency or decentralization is not really suitable. Decentralization, even more in a public blockchain, is a huge issue to manage because the number of participants is high and the information must be reliable.

Now looking at the accelaration of computing based on quantum computers, as soon as it will exit a quantum computer capable of breaking elliptic curves, security link to the blockchain can desappear. All the research around this subject called post-quantum cryptography is in full development.

Thus the futur of blockchain protocols, cryptocurrencies and smart contracts based on cryptography is function of a lot of new research which includes sustainable protocols, improvement of all properties listed previously, the futur of quantum cryptography and RSA codes.

Some benchmarks from academic references

A taxonomy of blockchains can be viewed in Xu et al. (2016). In Guégan (2017a) a discussion on private and public blockchain is available and an introduction on ICO in Guégan (2018a). Comparaison between Proof-of-Work and Proof-of-Stake in Bitfury Group (2015). Presentation of some altcoins with their protocols are developed in Bitfury Group (2015), see also ECB (2015) and Guégan (2017b). For information on the rules considered in US and Europe concerning Blockchain until december 2017 we refer to Blemus (2017). Some properties of blockchain are investigated in Cronan (2015), Wright and de Filippi (2015), Chartier and Zweifel (2017), Shermin (2017) among others.

Bitfury group (2015) Proof of Stake versus Proof-of-Work, mimeo, USA.

Blemus S. (2017) Law and Blockchain : a legal perspective on current regulatory trends worldwide, WP Paris 1, France.

Chartier R. T., T.D. Zweifel (2017) Blockchain, leadership and management : business as usual or radical disruption, WP. Eureka, France.

Cronan K., C. Decker, I. Eyal, A. Efe Gencer, A. Juels, A. Kosha, A. Miller, P. Saxena, E. Shi, E.G. Sirer, D. Song, R. Wattenhofer (2015) On scaling Decentralized Blockchains, Cornell Tech, USA.

European Central Bank (2015) Virtual Currency Schemes : A further analysis, 9. Franckfort, Germany.

Gattesci V., Lamberti F. Demartini C (2017) Blockchain or not blockchain, that is the question of the insurance and other sectors, IEEE, DOI 10.1109/MITP.2017.265110355

Guégan D . (2017a)) Blochchain publique versus blockchain privée: limites et enjeux, Revue Banque, N° 810., Sept 2017, France

Guégan D . (2017b) Blockchain publique et contrats intelligents (Smart Contrats) :) Les possibilités ouvertes par Ethéreum… et ses limites, Revue Banque, N° 814, Dec. 2017, France.

Guégan D . (2018 a) Les ICO une nouvelle façon de lever des fonds sans contrainte ?, Revue banque, N° 817, Feb 2018, France.

Guégan D. (2018 b) The Digital World : I The non mediatic side of Bitcoin, Bankers Markets Investor, April 2018.

Shermin V. (2017) Disrupting governance with blockchains and smart contracts, https://doi.org/10.0002.jsc.2150

Wright A., P. de Filippi (2015) Decentralized Blockchain Technology and the rise of lex cryptographia, WP, SSRN

Xu X., I. Weber, M. Stapke, L. Zhu, J. Bosch, L. Bass, C. Pantasso, P. Rimba (2016) A taxonomy of blockchain-based systems for architecture design, WP, CSIRO, Sydney.