A Probative Value for Authentication Use Case Blockchain

Dominique GUEGAN[1,2] – Christophe HENOT[1]

[1] University Paris 1 Panthéon–Sorbonne and LabEx ReFi

[2] Ca'Foscari University of Venezia

September 8, 2018

Abstract

The Fintech industry has facilitated the development of companies using blockchain technology. The use of this technology inside banking system and industry opens the route to several questions regarding the business activity, legal environment and insurance devices. In this paper, considering the creation of small companies interested to develop their business with a public blockchain, we analyse from different aspects why a company (in banking or insurance system, and industry) decides that a blockchain protocol is more legitimate than another one for the business it wants to develop looking at the legal (in case of dispute) points of view. We associate to each blockchain a probative value which permits to assure in case of dispute that a transaction has been really done. We illustrate our proposal using thirteen blockchains providing in that case a ranking between these blockchains for their use in business environment. We associate to this probative value some main characteristics of any blockchain as market capitalization and log returns volatilities that the investors need to take also into account with the new probative value for their managerial strategy.

JEL: C9 – E42 – G18 – G32 – K23

Keywords: Attack, Blockchain, Crypto-currency, probative-value, evidential- value, Hash rate, Immutability, Mining, Proof of work, Regulation, volatility,

I - Introduction

The evolution towards the blockchain is due to: (i) The evolution of computing and computing powers; (ii) The internet tool; (iii) The globalization of social relations.

The blockchain is a distributed network or a distributed ledger or a platform for a distributed organization. Over the technological evolution, we moved from a centralized organization to decentralized organizations, then to distributed organizations in which all participants (nodes) interact without any central, neither centralized control and where each node has a copy of the shared database (blockchain).

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 a 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. 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 (Nakamoto, 2008), 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.

The blockchain allows for value (including cryptocurrencies) to be traded between two parties without the involvement or approval of any other party. Such disintermediation enables everyone with access to a smart device and an Internet connection to transact in a peer-to-peer fashion, reducing the need for (and cost of) trusted central parties. 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.

This new technology represents a huge potential for banks and industry (Pilkinton, 2016). More generally, blockchain can be used in many domains where a third party is required, e.g. votes, administration, management and contracts (Sherman, 2017). This variety of applications requires blockchain adaptation, regarding their degree of opening. The question is to understand and explain why public blockchains can represent important innovation for specific enterprises. Another question is to understand why a firm focuses on a particular blockchain. One of the main characteristics of blockchains is immutability, and this characteristic is used in many cases as proof of authenticity, traceability, etc. Therefore, the choice of the blockchain is crucial for the company, which must be sure that the immutability is indisputable. In order to answer to this question, we introduce the notion of probative or evidential value associated to a blockchain in order to provide to the entrepreneurs an intrinsic value characterizing the blockchain he/she wants to use to develop his/her business. Because the immutability of several blockchains may appear sufficiently guaranteed, it may also be useful to arbitrate between these blockchains according to needs and to choose the one that will provide the required security at the lowest cost.

In order to provide this probative value, we quantify the cost of a 51% attack. We know that such attack determined the security of a blockchain. It exists some studies on this question, all from computing point of view or with theoretical models with ad hoc assumptions (Bradbury, 2013, Kroll et al. 2015). Here we quantify this attack looking at the revenues it can create for the miners, and we provide for each blockchain a corresponding cost. We call this value the probative value associated to the blockchain and it will provide some ranking between the blockchains distinguishing those which are easy to attack (low cost) comparing to those which are difficult to attack (high cost).[1]

Thus, we consider several other features inherent to any blockchain. It concerns characteristics associated to its financial value: (I) the market capitalization, (ii) the volatility, and (iii) a form of governance (Gattesci et al., 2017, Blemus and Guégan 2018). These properties provide interesting information for the investor with respect to his risk adverse behavior looking at new crypto-assets whose volatility is generally important. We give the information at a certain date and for the volatility to different periods. Concerning the governance of the blockchain, we verify if the code can be changed in an easy way or not, driving the potential creation of forks which is also important for the investors.

The methodology proposed in this paper is new and important for firms but also for banks and insurance companies which want to implement some blockchain inside their business because the main point is the choice of the protocol which underlines the process. The probative value proposed in this paper is a new way to understand the use of blockchain process and to compare the blockchains between them. The estimation of the probative value also makes it possible to obtain an economic value because it is calculated on the basis of a specific market: that of the cost of mining, whose actors are constantly seeking balance and optimal arbitration. We also analyse how the probative value can be used from a managerial point of view depending on the goods or transactions will be transferred throught this blockchain protocole.

The paper is organized as follows: After introducing briefly the concept of blockchain in Section 2, we examine in Section 3 the characteristics of blockchains that are important for measuring the probative value as well as the legal values given to this protocol in different jurisdictions. In Section 4, we propose a way to evaluate their degree of resistance to attacks that could call into question their principle of immutability and present the results obtained with different cryptocurrencies. We then propose the choices that could be made by a company seeking the best blockchain as an authentication tool or the conclusions that could be drawn by a court to arbitrate a dispute from which evidence would come from a blockchain. Section 5 concludes

II – Blockchain concept

Blockchain is based on different kinds of software 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 make exchange on the blockchain), scalability. There are scalability limits on (i) the size of the data inside blockchain (for Bitcoin the current blocksize is 1MB), (ii) the transaction processing rate, and (iii) the latency of data transmission (Guégan, 2018 a, b).

[1] We do not discuss if it can arrive or not (it can always arrive, as a failure of a bank can arrive), we provide, at time t, an information that any investor can verify on the website).

We can distinguish different classes of blockchains: it concerns the storage of data, the mining (different kinds of Proofs). This kind of differentiation has conducted to permissionless blockchain (or public blockchain), and permissioned blockchains (or private blockchain).

A permissionless or 'unpermissioned' ledger such as the Bitcoin blockchain or the Ethereum blockchain has no single owner and allows anyone to contribute to create data. Everyone in possession of the ledger holds identical copies thereof. Permissioned ledgers on the other hand have one or multiple (but known) owners, for instance a group of financial institutions. When new records are added, the ledger's integrity is checked through a limited consensus process carried out by trusted actors. The distinction between public and private blockchains underlines that these tools are frequently presented as distributed ledged with no central controlling authority for the former, and designed as closed systems for the latter (Xu et al., 2016a, Bacon et al., 2017).

The protocol used to create the blockchain is also a way of differentiation, depending on the fact they use (a) Poof-of-Work (PoW), (b) Proof-of-Stake (PoS) or (c) Delegated proof-of-Stake (DPoS) for instance (Xu *et al.,* 2016b, Duong *et al.,* 2017). This paper discusses only the PoW protocols, and other proofs will be discussed in a companion paper.

Proof-of-Work (PoW) is a protocol whose objective is to solve a mathematical puzzle providing a value which is unpredictable. To get this random number the protocole uses a hash function as an input containing a certain number of information as the list of transactions, the hash of the previous block, a time stamp, and a random number called nonce that will be incremented until a valid answer is obtained: this answer is a number smaller than a certain target provided by the protocole. Once the answer is obtained (after a lot of repetitions), all the inputs are provided to the rest of the network which can be verified by all the participants of the networks, nodes and so-called miners. Indeed, the miners and the nodes can put the inputs into the hash function which will produce the same result. Thus, the winner creates a new block and is rewarded with coins, currently 12.5 BTC for the Bitcoin protocole, and 3 ETH for the Ethereum protocole plus the fees provided by each transaction.

Proof of stake is a different way to validate transactions based on distributed consensus. It is still an algorithm, and the purpose is the same of the Proof of Work, but the process to reach the goal is quite different. In the Proof of Stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake. In PoS, forgers are always those who own the coins minted. Thanks to a PoS system, validators do not have to use their computing power because the only factors that influence their chances are the total number of their own coins and current complexity of the network.

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.

In the following we analyse blockchains, and then cryptoassets created only by PoW protocol, the cryptocurrencies which are created by other types of protocols like PoS or DPos will be considered in another paper. Indeed, the way we use to attain the objective of this paper which is to define a probative value for a blockchain is totally different if we work with PoW or PoS protocols. This will be explained in more detail at the end of the paper.

When a blockchain is created, the first question that the authors try to solve is the security of the protocol. Proof-of-Work appears as a protocol whose main goal is deterring cyber-attacks such as a distributed denial-of-service attack which has the purpose of exhausting the resources of a computer system by sending multiple fake requests.

The Proof of work concept existed before Bitcoin, but Nakamoto (2008) applied this technique to create digital currency revolutionizing the way traditional transactions are set. In fact, PoW idea was originally published by Dwork and Naor in 1993, but the term Proof of Work was coined by Jakobsson and Juels in a document published in 1999. Proof of work makes it extremely difficult to alter any aspect of the blockchain, since such an alteration would require re-mining all subsequent blocks. It also makes it difficult for a user or pool of users to monopolize the network's computing power, since the machinery and power required to complete the hash functions are expensive. Proof of work is a requirement to define an expensive computer calculation, also called mining, that needs to be performed in order to create a new group of trustless transactions (the so-called block) on a distributed ledger called blockchain as we explain above. Mining serves to verify the legitimacy of a transaction or avoiding the so-called double-spending ; and to create new digital currencies by rewarding miners for performing the previous task.

In a PoW protocol the difficulty consists to raise a target or threshold. This is the key point for the competition between the miners and determine the competitive nature of mining: more computing power is added to the network, the higher this parameter increases, increasing also the average number of calculations needed to create a new block. This method also increases the cost of the block creation, pushing miners to improve the efficiency of their mining systems to maintain a positive economic balance. In Bitcoin, the difficulty updated occurs all the 2016 blocks with a new block generated every 10 minutes, that is approximately every 14 days. Proof of Work is not only used by the Bitcoin blockchain but also by Ethereum blockchain (Buterin, 2015) and many other blockchains. Some functions of the Proof of Work system are different because created specifically for each blockchain.

Blockchains also serve as a support on which new applications are constructed. This is for instance the case of the smart contracts (Buterin, 2015, Clark *et al* 2016, Guégan, 2017, Blemus and Guégan, 2018) that can be built on top of a distributed ledger like with the Ethereum platform.

III – How to choose a blockchain for a specific corporate project? The probative value.

3.1. The features to characterize a probative value of a blockchain

In case of a banking or an industrial project based on blockchain, we need to create a specific environment which can be more complex than to do only transactions. Naturally the concept of smart contracts emerges. Thus, if we use public blockchains it exists several possible choices: Bitcoin, Classical Ethereum, Ethereum, Litecoin, Monero, among others. We propose a way to choose between these different protocols.

To attain our objective, we introduce the concept of probative value for a blockchain whose importance is crucial as soon as a conflict can emerge, providing information on the blockchain concerning its safety and security. It can be used from a legal point of view ensuring that a transaction has taken place. This probative value is based on several properties of the blockchain. One of the most important being the security we propose to compute, in a certain way, if a 51% attack can take place.

Why the choice of the blockchain is important? Consider for instance the traceability in supplychain using a specific blockchain, depending on the values of the goods which are transferred, the choice of the blockchain cannot be the same. In some cases we can use a blockchain whose probative value is less that another one. If a blockchain is used to carry containers (whose economic value is large) we will use a blockchain which is more attractive that if we need to track coal (whose value is smaller). It is this notion we propose to illustrate using a quantitative approach in Section 4.

First we decide to work with an open-source software, in order to use the technology which already exists and is available to everyone. This means that we consider blockchain based on consensus without third party, thus working with permissionless blockchain. This choice is due to the idea that the protocols developed inside this kind of environment reduce costs (fees, developing codes etc.), permitting decentralized business, capability of storage, security (fault resistance, attack tolerance, collusion resistance, avoiding cartel or selfish attacks).

Thus, this environment provides good security: indeed, for instance until now the Bitcoin blockchain has not been hacked, and it is the case for other crypto-assets, even if some hackings have been observed but concerning mainly platforms and not coding. The only uncertainties arise when a fork[2] is done. If modifications in the blockchain are necessary after a certain time, thus a fork arises but the underlying project does not fall down. Indeed all the previous information remains in the past blocks. In the past we have observed several forks for the two most famous cryptocurrencies: Bitcoin and Ethereum. What do these forks say? A blockchain which has suffered a fork can lose a certain « value » but not always.

For instance, for Ethereum, in 2016, following the DAO failure (SEC, 2017), there is a fork: the developers decide to change the code to avoid that the same problem arises latter, and create Ethereum. At the same time some actors decide not to change the code and then Ethereum Classic emerges. Economically speaking Ethereum has a higher price than Ethereum classic (coinmarketcap.com). The former has been created with the consensus of the community which seems to consider it more interesting.

If we consider now the case of Bitcoin, there have had a lot of forks since 2009. The last one in August 2017 sees the creation of Bitcoin Cash (for which the volume of transactions of a block has increased). This fork has generated market value for Bitcoin: indeed, the market value of Bitcoin Cash was important since the beginning, and contrary to the fear of some market players, the value of the original BTC has not decreased and still remains much higher than that of Bitcoin Cash. Thus, the situation, in that case from a financial point of view, is the inverse of Ethereum.

[2] The notion of fork is illustrated in the Section 4.2.1

Finally our *a priori* is to work with public blockchain and to compare their security looking at the 51% attack. We illustrate in the next Section how we can quantify this attack using an empirical approach providing a ranking of the blockchains.

Besides this technology problem, any investor could be interested by the financial value of a blockchain link to some features like its market capitalization and its volatility. Indeed, a high market cap attracts the investors and it is important from a business point of view. We assume that If the market capitalization is sufficiently high, (i) it permits to make the network more secure because it is an important incentive for miners, (ii) as soon as the value of the cryptocurrency is high with respect to the dollar, the miner knows that it can win a lot of money (in case of PoW and public blockchain), (iii) it can increase the computing power because the number of miners increases in that latter case. The volatility could be important for the banker or the entrepreneur: it could be an incentive not to use the crypto-asset. Thus, the more important is to verify what is the behavior of this crypto-asset on a long period to be able to anticipate some events. If the volatility is strong, the market capitalization is instable, and then the blockchain can be less attractive. From an economic and business point of view, the uncertainty associated with cryptocurrency's volatility can be problematic. We will discussed all these points in the fllowing for different cryptocurrencies.

3.2. Legal framework for a blockchain

Concerning the probative value the purely legal aspect of the blockchain could be interesting to look at. But this kind of information does not depend on the actors (developers, miners, investors) but of the legal framework of the countries where the activity in question takes place. Nevertheless we provide some information concerning the blockchain technology, knowing that the framework we describe will be changing very quick, and thus cannot be considered from a quantitative point of view.

The European Central Bank has created a Task Force on Distributed Ledger Technology (DLT) in August 2016 and has launched a joint research initiative with the Bank of Japan. In the member states, countries such as Great Britain and France have followed the same trend in order to follow closely the evolutions of the Blockchain practical uses. In 2016, the Bank of England has become a member of the Linux Foundation-led Hyperledger Blockchain initiative, and the UK prudential regulator FCA has drafted a broad paper in April 2017 on DLT and crypto-tokens. France has adopted two legal bills recognizing the Blockchain technology in 2016 and 2017. These laws are related to the use of Blockchain as a way to record efficiently financial and other instruments and to improve their ownership authentication. The first step was the adoption of the Law of August 6, 2015 (also named "Macron 2 Law") which empowered the French government to authorize by ordinance the use of DLT for the issuance and recordings of a new type of debt-based instrument: the "mini-bonds". This rule provided that the issuance and transfer of "minibonds" could be registered in a shared electronic registration technology and that a registration of a "mini-bond" transfer in the shared electronic registration technology constitutes a written legal contract under French law. French legal recognition of Blockchain technology came a step further after the adoption of the "Sapin 2" law in December 2016. While this new ordinance has not yet been published at the date we write this paper, the main terms of the text concern the registration of some financial instruments on a shared electronic registration technology, as decided by the issuer, which would be assimilated to a registration in bookentry form. The financial instruments that could be registered on a Blockchain would be notably shares and some debt instruments of non-listed companies and units of OPCs would have to be pledged.

In the Pacte law (French law), which is expected to be voted in December 2018, new clarifications concerning the use of blockchain as evidence proof are expected. It is to have a right opposable to what is written in the blockchain as well as to specify the questions relating to the property. Nevertheless it seems that no discussion includes the kind of blockchains that people can use, which is the objective of this paper.

In the US, in December 2016 the FED publishes a report stating that Blockchain technology represents "potential opportunities" in payments, clearing and settlement, notably by providing "a new asset-agnostic way of storing, recording, and transferring of any type of digital assets". Thus, we observe in US, a trend towards legal recognition of the Blockchain technology which is set to continue in several states (Arizona, Nevada, Delaware). In June 2018, the Hangzhou Internet Court in China decided that the use of blockchain technology in evidence deposition can be legally viable on a case-by-case basis. Bitcoin blockchain and Factom were used in this case. In September 2018, the country's Supreme People's Court in China extend this directive to all country considering that blockchain can now be legally used to authenticate evidence in legal disputes, clarifying various issues relating to how internet courts in China should review legal disputes. Part of the new regulation specifies that internet courts in the country shall recognize the legality of blockchain as a method for storing and authenticating digital evidence, provided the parties can prove the legitimacy of the technology being used in the process. For more detailed information and developments on other countries, we refer to Blemus (2018).

Concerning the smart contracts (contracts which can be automatically executed by a computing system, (such as a suitable distributed-ledger system) associated to specific crypto-assets in order to develop business in industry we observe that the discussion is always in turn between the law professionals that define a contract as a formal legally binding agreement between parties, while computer engineers perceive it as computer code, i.e. an arrangement of data and computer instructions executing pre-selected actions in computer programs. Three categories can be distinguished: (i) The "smart legal contract" focuses on the legality and enforceability of the smart contract, by the interaction/conjunction between computer code and legal wording, or by the partial or complete substitution of the former by the latter; (ii) The "smart contract code" refers to the technical execution of the smart contract, i.e. the pre-determined automated execution of a program or script once pre-defined conditions are completed. This term is frequently used when "smart contracts" mean a computer code without any mention to elements which constitute a legal contract; (iii) The "smart alternative contract" which would consist in new types of commerce agreement and newly rules which have nothing to do with the existing legal framework, Reidenberg (1997), de Filippi and Wright (2017), Guégan and Soritopoulou (2018) and Blemus (2018).

IV – How to compute the probative value of a blockchain?

Before developing the concept of probative value, we introduce the crypto-asserts we use in our exercise.

4.1. Presentation of some cryptocurrencies

We retain thirteen cryptocurrencies based on PoW for which we provide some information. The choice of these thirteen cryptocurrencies is based on their interest at the date of this work (market cap) and also on the fact that they have been created almost since one year. In any case the exercise can be conducted for other cryptocurrencies. The exercise done at date June 30, 2018, can be replicated at any date.

1- The Bitcoin (BTC) ptotocole was invented in 2008, the first bitcoins were created on January 3, 2009. Their number is limited to 21 million units and divisible up to the eighth decimal place. Nakamoto (2008) claimed to have worked on bitcoin from 2007 to 2009. In 2008, he published a document on a mailing list describing bitcoin digital currency. In February 2009, he posted an announcement about his work on the P2P Foundation site. On January 3, 2009, the first block is created. In February 2009, the first version of the Bitcoin software was released on the P2P Foundation website and, to make the network working, Nakamoto put his computer to work and thus created the first bitcoins. The protocol behind the Bitcoin blockchain is a Proof-of-Work. A block is generated every 10 minutes in mean.

2- BitcoinCASH (BCH) is a cryptographic currency derived from Bitcoin. In 2017, given the bitcoin scalability issues, some developers in the Bitcoin community proposed to increase the size of the mined blocks or to remove the signature from the transaction blocks and to create a separate register of signatures with the help of an update of the transaction register called Segwit. The divergence of the opinions of the miners gave rise to a hard fork of Bitcoin creating Bitcoin Cash whose blocks are 8 Mo instead of 1 Mo for Bitcoin. The methods of confirmation and monetary creation of Bitcoin Cash are identical to those of Bitcoin. The first Bitcoin Cash was issued on August 1, 2017.

3- Ether (ETH) was created in 2015. The algorithm is Ethash/DaggerHashimoto. It is a currency that looks more like an alternative currency than a cryptocurrency. It is an encrypted system more complex than Bitcoin with richer functionalities. Its essential functionality is smart contracts. The number of Ethers is not limited. The protocol for Ether blockchain is PoW but core developers would like to shift for PoS. Each new block is created every 15 seconds.

4- Ethereum Classic (ETC) was born from an update of the original blockchain of the Ethereum platform in July 2016 following the piracy of the platform related to The DAO. During this hacking, the developers decided to modify the blockchain to invalidate the sending of ethers to the hacker address. It was after this change that the new blockchain Ethereum was born, the former was then renamed Ethereum Classic. The continued operation of Ethereum Classic is motivated by strict adherence to the principle of blockchain immutability. The characteristics of the Ethereum Classic are identical to those of the Ethereum platform with their own updates.

5- Litecoin (LTC) was created in 2011. The algorithm is Script with Proof of Work and is totally different from that of Bitcoin based on SHA-256. The idea of using Script allows miners to convert their outdated GPUs (to undermine Bitcoin) and earn income by undermining the Litecoin. It reduces to 2,5 minutes the time of mining, compared to the 10 minutes of Bitcoin. Exchange platforms list the exchange peers of the Litecoin, thus creating a secondary market.

The network is expected to mine 84 million Litecoin instead 21 million for Bitcoin. The fact of putting a lot less time in term of mining than Bitcoin gives this altcoin a certain advantage implying lower transaction costs.

6- Dogecoin (DOGE) uses the Litecoin script and was created in 2013. Originally considered as a "joke". This altcoin prides itself on being a community cryptocurrency forcing funds for good causes (JO participation of Bobsleigh team from Jamaica). It is based on mining and would involve 100 billion units, incremented by 5 billion Dogecoins beyond each year. Blocks are mined in less than a minute.

7- Dash (DASH) was created in 2014 under the name of Darkcoin. The algorithm is X11. It is a pioneer in the development of features on anonymity. It is probably the most popular anonymous altcoin. It is a mined altcoin with a maximum of 22 million coins (in 2050). The confirmation time of a transaction is 2.5 minutes. This cryptocurrency uses a client-server architecture that works in Proof-of-Work, but thinks in Proof-of-Stake by creating a subnet composed of special servers (masternodes) that provide additional features such as instant transactions and especially private transactions (darksend).

8- Monero (XMR) was created in 2014 from a fork of Bitcoin cryptocurrency and uses the CryptoNote algorithm. The mining is based on a Proof-of-Work. There is no limit for the creation of XMR. A new block is added every 2 minutes. This currency has 2 properties: (i) allows sending and receiving funds without the transactions being publicly visible; (ii) creates an ambiguity that makes it virtually impossible to trace the funds spent. The protocol uses a so-called one-time ring signature process, a very powerful anonymization technique to hide transactions. Monero uses a one-time public key that prevents recipient’s funds from being linked with the wallet. That address can be audited by a 3rd party to prove the transaction occurred. (With the sender sharing their public view key).

9- Z-Cash (ZEC) is a cryptocurrency founded in October 2016, with a decentralized blockchain that provides anonymity for its users and their transactions. Their number is limited to 21 million units with a block validated every 2.5 minutes. As a digital currency, Z-Cash is similar to Bitcoin in a lot of ways including the opensource feature, but their major difference lies in the level of privacy. This project was created to compensate the weaknesses of some existing virtual currencies that do not guarantee anonymity in transactions. Z-Cash provides a great level of fungibility by allowing its users to remain completely anonymous. Z-Cash employs a cryptographic tool called Zero-Knowledge Proof which allows two users to engage in transactions without either party revealing their addresses to the other. Zero-knowledge proof makes Z-Cash transactions untraceable on its blockchain by obfuscating the addresses of both parties, as well as the amount involved in each transaction.

10- ZenCash[3] (ZEN) is a decentralized platform created in May 2017 allows secure transactions and communication forked from Z-classic. It is a fork of Z-Cash. As Z-Cash, there are no more than 21 million of ZEN and each block is generated 2.5 minutes. It is based on the Zero knowledge Proof. As the demand for privacy increased as big data became easily accessible,

[3] On August 22, 2018, “ZenCash” changed its name to “Horizen”. We have kept the name used on June 30, 2018, the date of our data.

cryptocurrency users began seeking other digital currencies that could fill the privacy hole that Bitcoin could not.

11- Vertcoin (VTC) created in January 2014 is a software fork of Litecoin. It is a Bitcoin-like blockchain currency with additional features such as Open-Source lightning Network implementation and ASIC resistant Proof-of-Work function. Vertcoin has already forked two times to a new PoW function because of an important threat of centralized mining. The network will mine a maximum of 84 million coins. Blocks arise every 2.5 minutes. The average transaction fee is very low.

12- Monacoin (MONA) is a Japanese cryptocurrency launched in December 2013 as a fork of Litecoin, with the genesis block occurring in April 2014. The Monacoin blockchain has a block time of 1.5 minutes. This platform has total of 105,120,000 MONA. The block time generation of MonaCoin is also much faster than Litecoin and is appreciated by Japanese investors.

13- The Electroneum (ETN) blockchain officially launched on November 2017 and the mobile miner launches on March 2018. ETN is based on the Monero codebase to allow for transactions on a decentralized blockchain with the same privacy features. The main characteristic of Electroneum is its mining by mobile phone. Transactions are relatively fast with dynamic fees based on the level of traffic on the network. The vast majority of the blocks have less than 0.2 ETN in total fees and new blocks are less than 2 minutes.

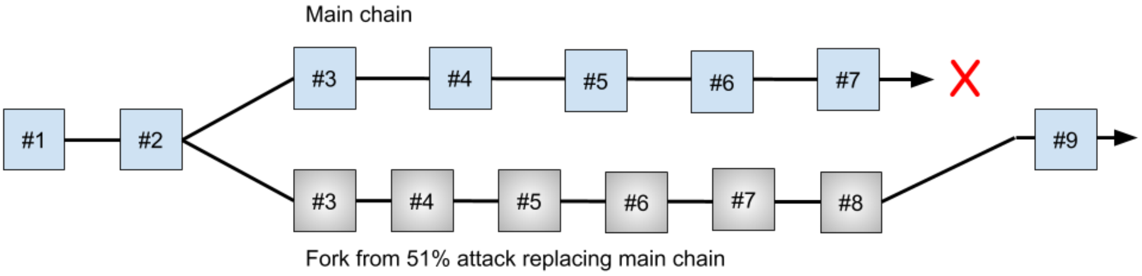
4.2. Comparison of the protocols‘ properties of these crypto currencies

In this Section, we explain how we can quantify the 51% attack in order to provide the probative value associated to each blockchain permitting a first ranking of these 13 crypto-assets. We briefly recall what is the 51% attack, then what is the cost of such attack for the miner.

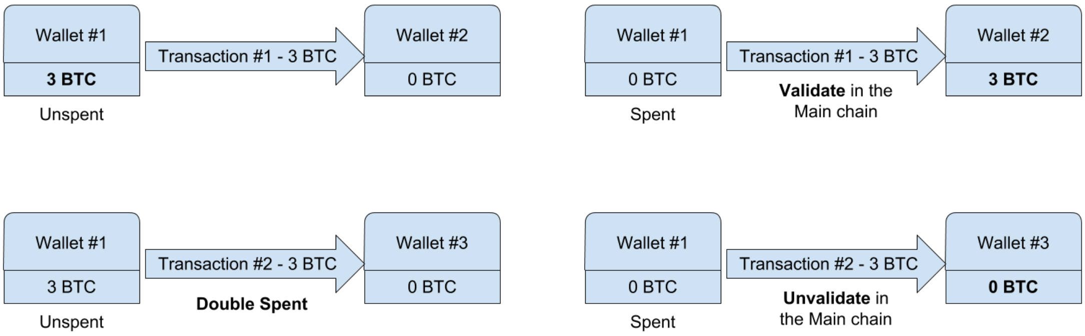
4.2.1. What is a 51% attack?

First we introduce the notion of fork and then the definition of a 51%attack.

The fork is the simultaneous existence of blocks with the same order number, which corresponds to a doubling of the main chain. The network will ultimately retain the longest chain. It is then possible, for a miner, to renounce to broadcast on the network a block that he would have validated and to continue the building of his own branch of blocks. Then, if he manages to obtain a longer channel than that produced by all the other miners, he has only to broadcast his channel on the network. The network will then adopt it to replace the original network which is shorter.



Statistically to succeed in validating more blocks than other miners at the same time, it is necessary to have more computing power than all the others, i.e. the majority, more than 50% of the total power. By simplification, we are talking about 51%. Successful 51% attack does not allow to modify the transactions, because the attacker does not have the private keys of the wallets. However, it allows to choose the transactions he/she will include in the "new" blocks. Then, it is possible for an attacker to carry out a double transaction, to cumulate his own blocks in which his double transaction will be validated, to let believe that the original transaction has been validated by enough blocks, then to substitute the original blockchain by his own.



The victim who notices that the transaction initiated by the fraudster has been validated by enough blocks, however, will no longer be able to use the crypto-asset he thought he had received when the "new blockchain" has done away with this transaction.

4.2.2. The cost of mining limits the 51% attack possibilities.

To attempt an attack, it is necessary to devote computing power to validate blocks that will not be broadcasted on the network and therefore take the risk of forgoing the gains from these blocks while bearing the cost of mining. The cost of mining is therefore the first limit to a 51% attack attempt. In a Proof-of-Work (PoW) protocol, this cost consists of the purchase or rental of equipment and energy consumption.

Thus, the higher the value of crypto-currency, the higher its capitalization, the higher the cost of mining will be. For economic reasoning, if a crypto-currency had a higher value than the others, but a low mining cost, it would create an arbitrage opportunity for the miners who would allocate all computing capacity to this crypto-currency. Therefore, competition would increase the cost of mining until a value/cost balance is achieved. this is the point we analyze through the cost of an attack.

To analyse the cost of an attack, we need to consider the availability of equipment. For bitcoin mining, for example, ASICs offer such performance that mining with other equipment is not cost-effective. All ASICs produced are immediately purchased and integrated into mining farms. The demand for equipment becomes greater than the supply. The available hardware capacity is thus not sufficient for a single player to be able to bring together more than all the total power available today on the Bitcoin network. However, this reasoning is not valid for other crypto currencies and it is possible that production capacities become more important one day, and lead to a decrease in marginal cost. This factor may or may not be used on a case-by-case basis and depends on the situation.

The longer the chain is to be substituted in a 51% attack, the more expensive it is. A chain of 6 blocks on Bitcoin (corresponding to what is considered sufficient to secure a transaction) represents an attack of one hour (at the rate of one block every 10 minutes on average). This cost can be estimated in two different ways:

(a) using the services of a mining market place.
(b) purchasing the necessary equipment.

We estimate the cost for each of these two cases at date June 30, 2018.

(a) The best-known market place for the rental of computing capacity for mining, nicehash.com, allows you to rent computing power to mine certain crypto-currencies. By taking the average of the equilibrium prices between supply and demand, we obtain the cost for a mining day for a given power.
For example, if the mining price of Bitcoin is :

0.04712 BTC/PH[4]/Day (SHA-256 algorithm)

and we want to create an attack at 51% knowing that the network difficulty is estimated at 38,326 PH/s[5], it will cost at least:

38,326 PH/s * 0.04712 BTC / 24 h = 75.247 BTC

for a one-hour channel (about 6 blocks), or $481,882 (with a $6,404 BTC).
Assuming that the attacker manages to validate 6 blocks in this time and before the rest of the network, the gain of such an attack would be:

6 * 12.5 BTC = 75 BTC, or $ 450,000.

The issues of an attack of this type must therefore be higher than 4 BTC. If the beneficiary of a transaction fears a double transaction with a 51% attack, it is sufficient to require a longer validation period. For example, if the amount involved in the transaction is $50,000, a validation time greater than 2 hours would be enough to make the cost of an attack unprofitable in our example:

(481,882 – 450,000) * 2 h = $ 63,764.

Another guarantee, valid in our example, would be to evaluate the material capacity to carry out this attack. Thus, for Bitcoin, the servers available for rent in Europe and the USA represent a total of 471.89 PH/s, which is insufficient compared to the 38,326 minimums necessary (and without counting the fact that renting all the servers would increase the cost of renting) to be able to create an attack. This guarantee is therefore the one that ensures that a 51% attack is not possible on Bitcoin and that the beneficiary of a $1 million transaction does not have to wait 40 hours!

But not all crypto currencies have the same guarantee as Bitcoin. Let's study for example the Vertcoin with the same conditions. With a network difficulty of 816.56 GH/s and an average price of :

[4] PH : PetaHash = 10^{15} Hash

[5] See blockchain.com

2.713 BTC/TH[6]/Day (Lyra2REv2 algorithm), i.e. 0.002713 BTC/GH/Day,

the cost of one hour of attack would cost:

816.56 * 0.002713 / 24 = 0.0923 BTC, or $591.

The material capacity available for rent is over 3,610 GH/s. Vertcoin is equal to:

0.00013585 BTC ($0.87),

one hour of mining would yield 25 Vertcoin per block at the rate of one block every 2.5 minutes:

25 * (60/2.5) = 600 VTC, or 0.0815 BTC.

It would cost

(0.0923 – 0.0815) BTC * $ 6,404 = $ 69.

In this example, as long as the stakes are well over $ 69, there would be no major difficulty in carrying out this type of attack.

With these two examples, we show that a 51% attack on Bitcoin will cost $ 31,882, and on Vertcoin $ 69. This information is important for an investor who does not know all the refinement associated to these different technologies. Higher the cost is, more secure the blockchain could be. This corresponds to the case that the miners rent their material.

However, it must be taken into account that the mining power rental market (market place and rental companies) has no interest in their services being used to carry out attacks at 51%. Indeed, when an attack of this type is carried out on a blockchain, confidence in that blockchain collapses, as does its value. Rental companies that have invested in equipment that only allows the mining of this type of blockchain will therefore have great difficulty in making their investments profitable. It is therefore in their interest to limit the options for using their equipment, especially the possibility of choosing their own blocks in the mining software used. In Table 1, columns 11, we provide the cost of a 51% attack when renting hashrate on Nicehash.com for thirteen cryptocurrencies.

Table 1 (to include here)

It may therefore be more practical to have your own equipment; the cost is then assessed in (b).

(b) To estimate the cost of acquiring the necessary hardware for an attack at 51%, we selected the most efficient hardware. ASICs when needed, otherwise the most powerful graphics cards. For example, for Bitcoin, a 51% attack would require acquiring nearly 3 million of the latest ASIC

[6] TH : TeraHash = 10^{12} Hash

model SHA-256 which is Antminer S9i for a cost of about 2 billion dollars. Table 1 summarizes the costs required for thirteen crypto currencies using PoW protocol.

Looking at Table 1 column 9, we note that it would cost $1,987,274,074, i.e. nearly 2 billion dollars of investment, to hold enough hashrate to lead a 51% attack on Bitcoin. Above all, it should be possible to acquire 2,838,963 (column 8) million Asics, i.e. much more than the annual production capacity. The limitation of hashrate available is also found in the column 12 ("MH/s Available") available for rent on NiceHash.com. The column 13 ("% Network available") gives an indication of the difference between the hashrate available and the one need to conduct a 51% attack.

If we take the example of Vertcoin, the acquisition of 12,759 graphic cards (column 8) would be necessary. The cost would be significant ($11,482,875) (column 9), but the purchase feasible. On the other hand, the expected gain from an attack should be greater than the investment. For instance, for Vertcoin, the whole mining network power is 816,560 MH/s (column 2) and we can rent a mining power of 3,610,000 MH/s on Nicehash.com website (column 12): this means that we have 442,10 % (column 13) of the hashrate necessary to generate our own block and impose it to the network. In contrary, if we look at Bitcoin network doing the same computation: comparing the whole mining power 38,326.10^9 (column 2) and an available rent hashrate 471,890.10^6 (column 12) this corresponds to 1,23% (column 13) of the whole mining power, and makes in that case the 51% attack impossible.

The argument that the equipment could be resold or rented on NiceHash.com after the attack is not entirely valid because it is necessary to take into account the increase in supply of equipment that would significantly lower prices. Moreover, the attack of a blockchain leads to a drop in confidence and consequently a drop in its value. It then no longer becomes profitable for the miners who leave it and the dedicated mining equipment no longer interests anyone and becomes unsaleable.

Therefore, some blockchains have a hashrate rate making any attack impossible due to lack of available hardware while other blockchain may be subject to a 51% attack, but provided the stake has a value greater than the cost of the necessary investment.

The result that we obtain and provide in the column 13 of the Table 1 provides us the information on the probative value we expected. Indeed, it tells us the level of the security for each blockchain a firm can use to make its business, and the tangible evidence that the transaction cannot be modified during the process. Thus, we call the value associated to the blockchain provided in this column the probative value. In any case, it is a relative value because it is computed at a given time[7]. What is interesting is the ranking that we can do between all these blockchains. For instance, Bitcoin appears the more secure, then Ethereum, Dogecoin, Litecoin, BitcoinCash, etc.

Thus, several informations must be taken into account to select the blockchains:

1) the availability of mining equipment
2) the cost of purchasing mining equipment
3) the availability of the computing power rental
4) the hourly cost of an attack in case of computing power rental

[7] These computations can be replicated for any date.

Criteria 1 and 3 are the most important because they establish the existence of a physical barrier to the possibility of being able to carry out an attack. The production capability of ASICs used to calculate hash with the SHA-256 function, used by Bitcoin for instance, is limited and decreases the demand. However, to hope to carry out an attack on Bitcoin, column 8 of Table 1 shows that it would be necessary to acquire nearly 3 million ASICs (2,838,963), which is impossible. The rental capacity of 1.23% of the required computing power (when more than 100% is required) also proves this impossibility.

Thus, the choice of a particular blockchain to obtain a sufficient evidentiary value depends on the importance of the value which can be guaranteed by its protocol. Indeed, Table 1 shows that, as at 30 June 2018, some blockchains cannot be physically attacked at 51%, others are on the other hand more fragile, but the cost of an attack may still have to be profitable in relation to the value at stake.

For instance, if a company wants to authenticate loyalty consumer points which value never exceeds $100 per hour and $5,000 annually, even if the blockchain is least resistant to a 51% attack, Vertcoin, could be appropriate because the financial stake in question is much lower than the cost of an attack.

If, on the other hand, these are financial securities worth several million dollars, it is preferable to be sure that all guarantees are taken so that no attack can be possible. Bitcoin or Ethereum blockchains would be perfect.

When this impossibility is not certain, the cost criterion comes into play. Looking at table 1, we observe that this could concern 4 crypto-currencies with an availability rate for rent close to or higher than 100%: Ethereum Classic, ZenCash, Monacoin and Vertcoin. The respective costs of a one-hour attack would be $15,158, $4,479, $3,155 and $591 respectively. If the value of good or transaction which must be guaranteed for one hour is less than these amounts, there is no point in conducting an attack. If this value is higher, then it would be sufficient to wait several hours until the total cumulative hourly cost becomes lower to ensure that no double transactions have been made.

In the event of a dispute, a court, based on our findings, may find that a blockchain has immutability sufficient to constitute evidence. On the other hand, if one of the parties wishes to challenge this evidence, it suffices for him to (i) show that an attack is possible and that immutability is not guaranteed, and / or (ii) demonstrate that an attack has occurred by showing the existence of a fork with the block containing the transaction serving as proof, at a given date.

4.2.3 Other features of a blockchain

We now analyse otherproperties on the different blockchains, quantifying some financial variables associated to crypto currencies as market capitalization, price, volatility and governance. These values are also provided at June 30th, 2018. Table 2 contains these informations for the same sample of crypto currencies used in the previous Section.

Table 2 (to include here)

In columns 7-8-9 we provide information on the Log return Volatility. The computations of historical volatilities show the high volatility of non-indexed crypto currencies. Considering the annualized standard deviation of the daily log returns at June 30, 2018, we observe that the S&P500 index has a quarterly, half-yearly and annual volatility of 11.7%, 16.4% and 12.5% respectively. Looking at the results provided in columns 7-9 we observe that the crypto-currencies are therefore, on average, 10 times more volatile. The minimum value is obtained for Bitcoin whose quarterly volatility is 6 times that of the SP500 and the maximum value is obtained for ZenCash whose annual volatility is 16 times that of the SP500. The volatility gives also information on the stability of the blockchain's value. Indeed, if the market value falls sharply due to speculative movements, the resulting loss of profitability for miners may encourage them to devote their computing power to another blockchain using the same algorithm or to rent their equipment. The level of difficulty of this blockchain would therefore decrease while, at the same time, the computing capacity available on the market would increase. Thus, the fall in the value of a blockchain linked to high volatility greatly reduces the cost of an attack.

In column 10 we provide information on a part of the governance of cryptocurrencies. In order to limit risks related to the volatility of random block validation and reward success, miners group together in a mining pool. They pool their computing power and share the earnings in proportion to their contribution to the network. This explains why mining pools often represent significant percentages in the hashrate distribution of a blockchain.

Their economic interest being directly linked to the confidence which can be allocated to this blockchain to which they contribute. These pools generally not take care to become majority in the distribution of the global hashrate because they would have the capacity to lead a 51% attack. However, it is not because a pool could that it would benefit, since this would require the will of all the miners gathered in this pool. However, in order to avoid sending a negative signal to players and the market, mining pools ensure that such a rate is not reached. It should be noted that, in the past, it has happened that on some blockchains, a pool temporarily reaches a hashrate rate higher than 50% without this having had any significant impact, except for more intense activity on the social networks dedicated to this blockchain.

Indeed, the other problem related to the concentration of the mining power is not only related to the risk of 51% attack, but to the governance of the blockchain. The evolution of the code of a blockchain is done by consensus. Proposals for the implementation of new functionalities, which stem from strategic development choices or visions, may be accepted or rejected by the stakeholder community. The latter are made up of miners, network nodes and, ultimately, users who can leave the use of one blockchain in favor of another one. For miners and network nodes, this choice is made by deciding whether or not to adopt the software update incorporating these proposals. One or few mining pools with a dominant position could therefore have a particularly important influence, even if this is not sufficient to take control of a blockchain. We note that on June 30, 2018, the main mining pool of each blockchain listed in Table 2 rarely exceeds 27% of the total hashrate. Of particular importance is the main pool of Ethereum Classic, which reached 45% at the date of June 30th, 2018.

The value of the market capitalization provided in column 6, Table 2 is important because the more a blockchain increases in value, the higher the gains from mining and therefore, the more miners there are. However, it is because there are more and more miners that the level of difficulty increases and it becomes more difficult to carry out a 51% attack. The monetary value of the blockchain therefore influences its resistance to attacks; however, this is not a sufficient factor to guarantee it. Looking at

Table 2, column 4, we show that the market cap factor is relatively well correlated with the low availability of computing power in the rental market.

As we have seen before, it appears that a mining pool theoretically has no interest in seeking to carry out a 51% attack on the blockchain that pays it. Indeed, its revenues are directly linked to the market value of this blockchain. However, the fact that this is possible or that certain issues are more important than the financial loss it causes, does not exclude the possibility of a takeover by a miner. Finally, the fact that the weight of the principal miner is far below the majority does not guarantee good governance. It is quite possible that several miners may agree and act in concert. But this information is not available on the market and requires a thorough investigation.

4.2.4 The probative value

Considering the previous analysis, we retained four parameters to analyse the reasons permitting to retain one blockchain vis-à-vis another one, in case of business based on the use of blockchain.

First the marketcap is certainly the first information a person will consider in using a blockchain for business. Indeed, it provides the information on the importance of the cryptocurrency from a financial point of view, but from our point of view, it is important because it informs on the high or less activity of a blockchain, at a given time, and then on the fact that its security is more or less important.

The second important information is the volatility. We observe that most of the crypto assets are extremely volatile comparing for instance to other financial assets. Thus, this information is important because, associated to the marketcap information, it permits to discriminate between the cryptocurrencies which have a high marketcap and a low volatility.

The governance information, as we have introduced it in this paper, permits to know if it exists an important concentration of the mining concerning a specific blockchain at a given time which can creates specific attacks on the blockchain and make it less immutable.

Finally the 51% attack that each protocol tries to avoid in order to ensure its security is analysed in detail because it characterizes the immutable property of a blockchain. This immutable property has been quantified throught the costs of an attack in the previous paragraph. We have provided a ranking between several blockchains thanks to these computations. This immutable property is the key point for the choice of a blockchain because it gives the proof that a transaction or a transfert exists and cannot be suppressed from the blockchain and then challenged in case of dispute by one of the parties. Stronger is this property, more interesting is the blockchain for business. This property assures the contractor that the transfers have taken place.

Thus, the four ingredients (marketcap, volatility, governance, immutability) need to be analysed and known by any person who are interested to use a public blockchain environment for its business. Any entrepreneur have to keep on eyes on them during several periods to observe if they stay stable or not. In case of an entrepreneur uses one blockchain and observes suddenly a high instability, probably it will be necessary to change blockchains. This means that the notion of interoperability has also to be analysed in that case to ensure the compatibility between two blockchains. This will be analysed in another paper.

Finally, the concept off probative value discussed in this paper is a preliminary research to define a legal and economic indicator for the blockchains in view to use them for a business objective. We consider that this indicator will be based almost on these four properties.

V – Conclusion

The blockchain protocol promises a major change in the way certain sectors are structured today. The digital and self-regulating third party trust that it constitutes is made possible thanks to the various properties that its technology ensures, and in particular that of immutability. However, we have noticed that this immutability is not guaranteed under the unique pretext of respecting the protocol of a blockchain. We explained that permissioned blockchains, controlled by a small group of actors and not benefiting from a robust Proof-of-Work process, could easily be modified, recalling that this risk is limited to the mechanism of double spending and not to access to the wallet for which we do not hold the private key.

As soon as permissionless blockchains can be attacked and allow, under certain conditions, to modify the history of recorded transactions, we quantify this risk, making it possible to ensure that certain blockchains constitute reliable tools of confidence, up to a certain value because the importance of the cost of an attack would be sufficiently dissuasive. Thus we illustrate the fact that some blockchains, such as Bitcoin, are not physically attackable at present, whatever the funds that could be spent on them.

We do not provide a table classifying the blockchains according to their probative value which requires defining weights for the different criteria we have chosen because in the absence of sufficient data to carry out an econometric study, we cannot determine the value of these weightings whose values can only be provided arbitrarily. For another side it is obvious that the availability of hashrate for rental is the most important criterion, and thus the lack of availability makes it impossible to carry out an attack whatever the cost. Thus, following the results provided in Table 1, we can classify the blockchains in three groups: (i) a first group of blockchains which have an available hashrate rate less than 25%, they are eight (these blockchains have some security as soon as their rate does not increase); (ii) a second group of blockchains whose available hashrate is above 100%, it corresponds to 3 blockchains (for these blockchains an attack is possible at any time); and (iii) a group of 2 blockchains with rates below 100%, but high enough to make an attack possible if these rates increase or by combining the rental and purchase of equipment. These results provide an possible classification of the 13 blockchains studied in this paper concerning their security even if we consider that it is difficult to determine a classification of blockchains according to their ability to prevent a 51% attack.[8]

In summary, in this study, we propose a new way to use blockchain quantifying the difference between the blockchains for business purposes. We provide a probative or evidential value associated to the level of the security of the blockchain based on the way to be able to physically attack the blockchain and make the transactions no secured. Our approach provides a probative value permitting a ranking between the thirtheen blockchains considered in this study. We associate to this probative value a set of quantified data (volatility, market capitalization and number of miners on the network) that any

[8] The clarification provided in this paragraph has been done following a specific demand of one of the reviewers.

investor can always be used to decide its managerial strategy for his/her business. Finally, an entrepreneur who wishes to use a blockchain to authenticate a transaction or a transfer of goods, for example, has an interest in ensuring that a doubt cannot occur in the event of a dispute, this is the interest of the approach that we propose, because it provides a way to quantify this information.

The subject is not close and will necessitate a lot of other researches to improve our result including the innovation that will be developed in blockchain technology in the future.

References

Aster T. (2017) The fair cost of Bitcoin proof of work, WP, UCL, London UK

Bacon J., J.D. Michels, C. Millard,J. Singh (2017) Blockchain demystified, WP Queen Mary University of London, N° 268/2017, London, UK.

Baur, D.G., Lee A.D., Hong K. (2015) Bitcoin: Currency or Investment, OPUS, Sydney, Australia.

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, Revue trimestrielle de droit financier, n° 4-2017, Paris, France.

Blemus S., D. Guégan (2018) Initial Crypto-asset Offerings (ICOs): tokenization and corporate governance, WP Paris1, Paris, France.

Bradbury D. (2013) the problem with Bitcoin, Computer fraud and security, 2013(11), 5-8.

Buterin V. (2015) A next generation smart contract and decentralized application platform, Ethereum White Paper.

Duong T., L. Fan, H-S. Zho (2017) 2-hop blockchain: Combining Proof-of-Work and Proof-of-Stake Securely, WP, Virginia University, USA.

Dwork C., M. Naor (1992) Pricing via processing or combatting junk mail, Annual International Cryptology Conference, 139-147 in Lecture Notes in Computer Science, Book Series, vol 70, Springer

Eyal I., A. E. Gencer, E. G. Sirer, R. van Renesse (2016) Bitcoin-NG: a scalable blockchain protocol, in the Proceedings of the 13th USENIX Symposium on Networked Systems Design and implementation, Santa Clara, CA, USA.

de Filippi P. and Wright (2017) Blockchain and the law: the rule of the code, WP, Harvard University ed., USA.

Frunza M. (2015 Solving Modern Crime in Financial Markets: Analytics and case studies, Elsevier, USA.

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. (2017) Les ICOs: la nouvelle façon de lever des fonds sans contrainte, Revue Banque, 817.

Guégan D., A. Soritopoulou (2017) Bitcoin and the challenge for regulation, Capital Markets Law Journal, issue 4.

Guégan D. (2018 a) The Digital World: I The non mediatic side of Bitcoin, Bankers Markets Investor, 151.

Guégan D. (2018 b) The digital world: II - What are the alternatives to Bitcoin Blockchain? Bankers, markets, Investors, 152.

Jakobsson M., A. Juels (1999) Proofs of work and bread pudding protocols, Secure information Networks, 23, 258-272, Springer

Kroll J.A., Davey I.C, Felten E.W. (2015) The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries? Working Paper, Princeton University, USA.

Landau J.P., A. Genais (2018) Les crypto-monnaies, Rapport Ministère de l'Economie et des Finances, Paris, France.

Nakamoto S. (2008) A Peer-to-Peer electronic Cash System, https://bitcoin.org/bitcoin.pdf

Pilkington (2016), Blockchain technology, principles and applications, in Research Handbook on Digital transformation, eds. F. Xavier Olleros, Majlinda Zhegu, 225 – 251, Edward Edgar Publishing.

Reidenberg J.R. (1997) Lex Informatica : the formulation of information policy rules through technology, Texas Law Review, 17 (3), 553-593.

Xu X., C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, S. Chen (2016a) The blockchain as a software connector, WP NICTA and CSIRO Sydney, Australia.

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

Blockchain (Algorithm)	Network Hashrate MH/s	Miner				Cost Elec $	51% attack by buying equipment			51% attack by renting hashrate on Nicehash		
		Model	Price $	Power MH/s	Cons. Watt		Nb miner	Cost $	Cost KW/h (1h)	Cost (1h)	MH/s Available	% network available
Number of column: (1))	***(2)***	***(3)***	***(4)***	***(5)***	***(6)***	***(7)***	***(8)***	***(9)***	***(10)***	***(11)***	***(12)***	***(13)***
Bitcoin (Sha 256)	38 326 .10^9	Antminer S9i	700	13 500 000	1 300	0,066	2 838 963	1 987 274 074	243 583	481 882	471 890 000 000	1,23%
BitcoinCASH (Sha 256)	4 826 .10^9	Antminer S9i	700	13 500 000	1 300	0,066	357 481	250 237 037	30 672	60 676	471 890 000 000	9,78%
Ethereum (Ethash / DaggerHashimoto)	240 150 000	Antminer E3	1876	180	800	0,066	1 334 167	2 502 896 667	70 444	310 053	9 440 000	3,93%
Eth Classic (Ethash / DaggerHashimoto)	11 210 000	Antminer E3	1876	180	800	0,066	62 278	116 833 111	3 288	15 158	9 440 000	84,21%
Litecoin (scrypt)	261 680 000	Antminer L3+	426	504	800	0,066	519 206	221 181 905	27 414	46 436	17 710 000	6,77%
Dogecoin (Scrypt)	297 810 000	Antminer L3+	426	504	800	0,066	590 893	251 720 357	31 199	49 328	17 710 000	5,95%
Dash (X11)	2 420 000 000	Antminer D3 X11	280	17 000	970	0,066	142 353	39 858 824	9 113	9 131	522 030 000	21,57%
Z cash (equihash)	590	Antminer Z9 mini	850	0,01	266	0,066	59 000	50 150 000	1 036	45 034	68,80	11,66%
ZenCash (equihash)	65	Antminer Z9 mini	850	0,01	266	0,066	6 500	5 525 000	114	4 479	68,80	105,85%
Vertcoin (Lyra2REv2)	816 560	GTX 1080 Ti	900	64	190	0,066	12 759	11 482 875	160	591	3 610 000	442,10%
Monacoin (Lyra2REv2)	2 540 000	GTX 1080 Ti	900	64	190	0,066	39 688	35 718 750	498	3 155	3 610 000	142,13%
Monero (CryptoNightV7)	454	RX Vega 56	700	0,00185	190	0,066	245 405	171 783 784	3 077	16 318	69,52	15,31%
Electroneum (CryptoNightV7)	95	RX Vega 56	700	0,00185	190	0,066	51 351	35 945 946	644	2 543	69,52	73,18%

Table 1

Power requirements, equipment characteristics and costs (in $) of a 51% attack by buying the equipment and renting hashrate on Nicehash.com website on June 30th, 2018 for 13 crypto-currencies. (Blockchains grouped according their algorithm)

Data are downloaded from specific platforms and blockchain explorer associated to each crypto-currencies. The limitation of hashrate available is also found in the column 12 ("MH/s Available") available for rent on NiceHash.com website. The column 13 (“% Network available") gives an indication of the difference between the hashrate available (column 12) and the one need to conduct a 51% attack provided in column 2.

Blockchain	Code	51% attack		Market values (a)		Log Return Volatility (b)			Governance (c)
		Invest (M$)	Hashrate available	Price $	Market cap K$	90 days	180 d	365 d	
Col #: (1)	***(2)***	***(3)***	***(4)***	***(5)***	***(6)***	***(7)***	***(8)***	***(9)***	***(10)***
Bitcoin	**BTC**	1987	1,2%	6 404,00	106 405 000	71,1%	96,3%	103,6%	22%
Ethereum	**ETH**	2503	3,9%	455,18	43 789 500	100,3%	115,5%	120,2%	26%
BitcoinCash	**BCH**	250	9,8%	715,71	11 409 400	126,5%	146,5%	–	24%
Litecoin	**LTC**	221	6,8%	81,37	4 515 210	93,0%	122,0%	141,0%	23%
Monero	**MNR**	172	15,3%	131,01	2 050 040	107,0%	136,0%	148,2%	21%
Dash	**DSH**	40	21,6%	238,36	1 913 510	100,3%	121,1%	136,1%	23%
Ethereum Classic	**ETC**	117	84,2%	16,10	1 572 500	117,4%	150,7%	158,5%	45%
Zcash	**ZEC**	50	11,7%	163,99	695 259	121,0%	137,3%	142,1%	33%
Dogecoin	**DOGE**	252	5,9%	0,00	280 151	103,6%	149,3%	166,7%	20%
Monacoin	**MONA**	36	142,1%	2,11	123 957	94,24%	147,65%	208,28%	6%
Electroneum	**ETN**	36	73,2%	0,01	71 940	140,1%	188,5%	–	34%
ZenCash	**ZEN**	5,5	105,8%	17,68	67 949	130,7%	153,6%	202,4%	27%
Vertcoin	**VTC**	11,5	442,1%	0,87	38 075	119,2%	151,3%	200,4%	27%

Table 2
Features of the blockchain protocols for 13 crypto-currencies on June 30th, 2018.
(Blockchains sorted by market Capitalization)

(a) Data from coinmarketcap.com on June 30th, 2018.

(b) Volatilities are calculated from the log-return of the daily closing prices of the crypto currencies from coinmarketcap.com, over the 90, 180 and 365 days preceding the 1st of July 2018. The daily log-return is calculated by : *ln*(*price D* / *price D-1*). Volatilities are obtained by calculating the standard deviation of *n* log-return values *x*, i.e. : $[\ \mathit{Sum}\ (x\text{-}\mathrm{E}(x))^2\ /\ (n\text{-}1)\ ]^{0.5}$. Annual volatilities are calculated by multiplying daily volatilities by the square root of 365.

(c) Governance: hashrate percentage of the biggest miner.