Waelbroeck, Patrick

Working Paper

An Economic Analysis of Blockchains

CESifo Working Paper, No. 6893

Provided in Cooperation with:
Ifo Institute – Leibniz Institute for Economic Research at the University of Munich

Suggested Citation: Waelbroeck, Patrick (2018) : An Economic Analysis of Blockchains, CESifo Working Paper, No. 6893, Center for Economic Studies and ifo Institute (CESifo), Munich

This Version is available at:
https://hdl.handle.net/10419/176912

CESifo WORKING PAPERS

6893
2018

January 2018

An Economic Analysis of Blockchains

Patrick Waelbroeck

CESifo

Impressum:

CESifo Working Papers
ISSN 2364-1428 (electronic version)
Publisher and distributor: Munich Society for the Promotion of Economic Research - CESifo GmbH
The international platform of Ludwigs-Maximilians University's Center for Economic Studies and the ifo Institute
Poschingerstr. 5, 81679 Munich, Germany
Telephone +49 (0)89 2180-2740, Telefax +49 (0)89 2180-17845, email office@cesifo.de
Editors: Clemens Fuest, Oliver Falck, Jasmin Gröschl
www.cesifo-group.org/wp

An electronic version of the paper may be downloaded
· from the SSRN website: www.SSRN.com
· from the RePEc website: www.RePEc.org
· from the CESifo website: www.CESifo-group.org/wp

CESifo *Working Paper No. 6893*
Category 14: Economics of Digitization

An Economic Analysis of Blockchains

Abstract

The blockchain is a technology that goes beyond timestamping, bitcoin and secure financial transactions. The development of an ecosystem around smart connected objects will probably not happen without the blockchain (in one form or another). The blockchain opens the door to the liquification of the physical world, to the economy of real-time micro-transactions and to smart data sharing. However, it is necessary to distinguish between the different types of blockchains, especially between public and private blockchains, because their economic properties are contrasted. Moreover, governance issues in public blockchains seem to indicate that the technology alone cannot guarantee trust.

JEL-Codes: E510, G340, H410, L140, L520.

Keywords: blockchain, bitcoin, ether, security, payment, governance, trust, oracles, forks, hash, smart contracts, tokens, smart locks, technology diffusion, crypto-currency, financial privacy.

Patrick Waelbroeck
Telecom ParisTech
Department SES
46 rue Barrault
France - 75013 Paris
partick.waelbroeck@telecom-paristech.fr

January 2018

Foreword

The blockchain is a technology that can secure a digital registry in a decentralized way. Each block contains the fingerprint of the previous block, thus forming a chain of data blocks. A new block cannot be falsified or predated because the blockchain is copied on all nodes of the network. We will discuss in this article the many uses and applications of the blockchain and analyze whether this technology is disruptive or not. As a first application, a blockchain is a technology for generating trust by building an unfalsifiable register. The blockchain thus makes it possible to irrefutably mark when a transaction was carried out: it is a generalized timestamping technology. In addition to financial transactions, the blockchain can be used to register intellectual property claims and cadastral data. Some blockchains, such as the blockchain Ethereum, allow programmers to execute code on blockchain elements. These codes called smart contracts open new perspectives on smart connect objects. Perhaps, the largest number of applications will come from the combination of the blockchain technology with the Internet of Things.

There are mainly two types of blockchains: public blockchains and private blockchains. They differ from one another through the permissions granted to the nodes of the network. In a public blockchain, all nodes have permission to write to it and to read its data. In contrast, only a small number of nodes have permission to write to a private blockchain. The validation rules for adding a new block also differ. For example, in the case of the public bitcoin blockchain, the incentives to secure the elements of the blockchain take the form of a payment in crypto-currencies through two mechanisms: a fixed amount per blocks that are mined and a variable amount related to transaction costs. In a private blockchain, the incentives are rather linked to the governance of the blockchain (we propose in section 2 an economic analysis of the different types of blockchain).

Why should an economist be interested in blockchains? There are at least five reasons.

First, blockchains offer an interesting perspective for the economics of security by creating a decentralized system of incentives to secure a computer infrastructure. We analyze the impact of blockchains on the economics of computer security in section 3.

Secondly, blockchains and smart contracts make it possible to connect economic agents in a decentralized way, thus redefining the notion of the firm and the nature of work. They also have an impact on the organization of industries, as agents can share computing resources, thereby reducing fixed entry costs in sectors that require significant investment in servers and hardware. The blockchains also represent a counterweight to the centrifugal tendencies of multi-sided platforms concentrating the market power of some Internet players. This is discussed in Section 4.

Thirdly, the blockchain is also a technological innovation that can spread more or less rapidly in the economy. The question of whether this technology is sufficiently

disruptive for rapid diffusion, or whether it is a transformative innovation that may take several decades to spread throughout all industries is analyzed in section 5.

Fourthly, crypto-currencies such as the bitcoin offer new perspectives on payment instruments when consumers have financial privacy concerns. We start by analyzing the supply of and the demand for crypto-currencies in section 6. We then focus on the governance of the bitcoin in section 7.

Finally, smart contracts need external data to run self-executing programs. Oracles are software, hardware or human intermediaries who verify that data from the physical world can be trusted. New solutions based on decentralized networks of oracles create markets for trust and are analyzed in Section 8.

Part 1 – Introduction

1 What are the innovations behind the blockchain?

The blockchain goes well beyond its use as a simple digital register producing timestamps. Three aspects deserve to be emphasized: tokens, smart contracts and the liquification of the physical world.

1.1 Token economics

The blockchain gives incentive to secure the network infrastructure by issuing tokens. These may correspond to a crypto-currency, but tokens can also be used:

- to guarantee voting rights at a general assembly, during political elections or during an automated consensus decision (see for instance Swan, 2015).
- to assess the validity of a travel pass and to allow a passenger to access restricted areas, get vouchers for dinner, etc.
- to access shared medical, legal, technical files
- to trace persons and objects in the physical world and data in the online world (for instance ads)
- to automatically rent computer power, data storage, apartment, cars, parking space, storage space (etc.) by machine to machine communication
- to finance a project using crowdsale (Initial Coin Offering).
- most importantly, to materialize externalities and create monetary incentives in situation where markets do not exist, through micro-payments.

1.2 Smart contracts

Smart contracts are bits of code, which, executed on the blockchain, allow a user to validate tasks and get a related payment.

Example 1: Ubik.

In the book by Philip K. Dick (1969), Joe Chip, a telepath hunting specialist, lives in a rented apartment. He is expecting a visit and wants to clean his apartment. He calls the maintenance department of the building to send him robot cleaners. The concierge service is automated: the robot (or the chatbot using today's terminology) informs him that he has a debt to pay before he can recruit the robot cleaners. Since he is penniless, he wants to contract a microcredit in real time. However, the robot also informs him that the credit company has lowered his personal credit rating from triple G to quadruple G and is blocking any new credit application. He pays 10 cents to start the coffee machine, but he misses 5 cents to open the door of his apartment for his guests (who ultimately pay to open the door). He offers them a coffee, but the refrigerator is also automated and 10 cents are needed for opening the door and 5 cents to get the cream. Philip K. Dick describes a micropayment, micro-transaction economy in real time. The micro-payment eco-system was proposed as an

alternative to copyright to pay content creators by Lanier (2014). The idea of the connected door of Ubik is under development at Slock.it (See Figure 1).

Figure 1. Smart lock from slock.it.

1.3 The liquification of the physical world

The blockchain can also trace and authenticate people and physical products using fingerprinting technologies, digital passports and physical sensors. For example, a serial number, or the "passport", of a physical object can be inserted in the production chain. These technologies are merging the physical world and the digital world by improving the traceability of products and services in order to make the economy more "liquid".

Example 2: *Daemon*.

A daemon is a computer program that resides in memory and that automatically executes tasks when certain events occur. It is a prototype of a smart contract, but without the micropayment dimension. Daniel Suarez (2006) tells the story of a genius video game programmer Matthew Sobol who, after his death, orchestrates automatic executions of connected objects: a house with traps, an electrified door, a self-guided killer vehicle (not really artificial intelligence, but rather a distributed conditional automated execution). The daemon self-executes tasks through physical sensors that enable it to detect actual events. It also "follows" the news on the Internet to check how events unfold. Using terminology of section 8, the daemon uses a software-based oracle, i.e. a third party trust solution, to push external data into its smart contracts.

Example 3: Everledger.

Everledger is a diamond blockchain that track transactions through a digital passport assigned to each diamond. The metadata of each diamond (its size, diameter, weight, etc.) are also recorded in the blockchain (see Figure 2).

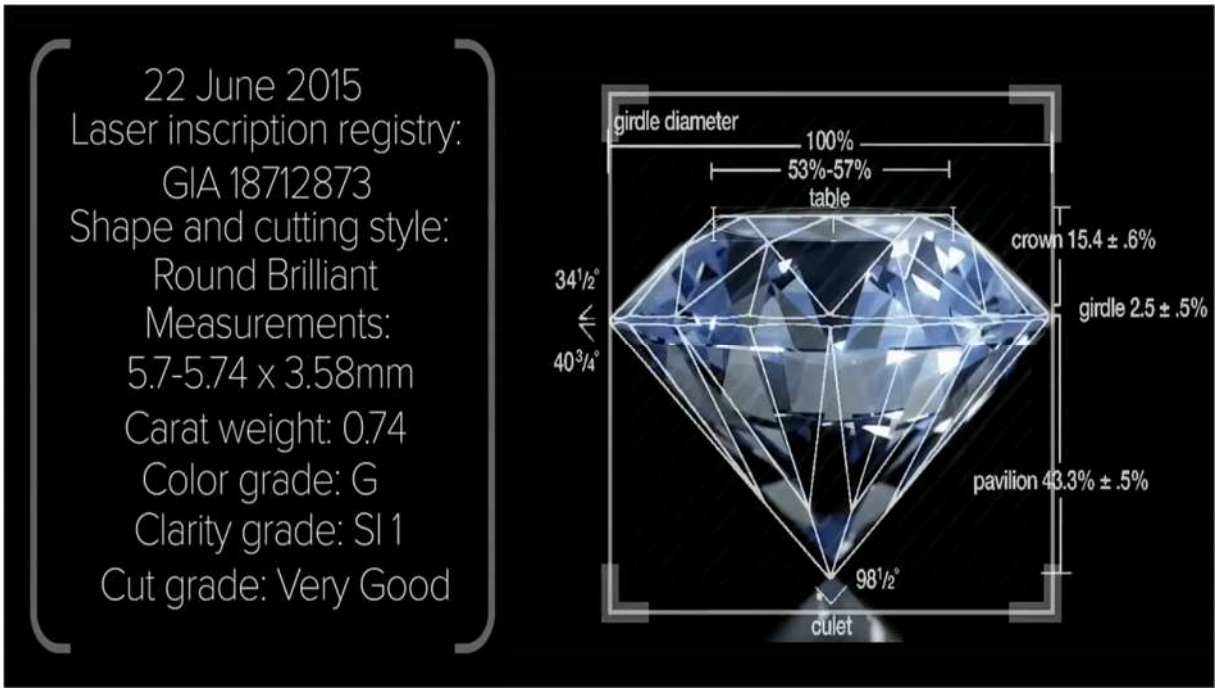


Figure 2. Characteristics of a diamond recorded in the *blockchain* Everledger. Source: https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/ (checked on May 17, 2017).

Part 2 - Economic analysis

2 An economic analysis of blockchains

Blockchains differ according to whether permissions are needed to write data to it and to read data from it. Depending on the configuration of permissions, the economic properties of rivalry and excludability differ. Finally, blockchain generate network externalities that can be both positive and negative.

2.1 Read and write permissions

It is important to distinguish blockchains according to whether or not permission is needed to write to it and to read data from it. The four configurations of possible permissions are shown in Table 1.

	Permission to read required	Without permission to read
Permission to write required	*Private/consortium blockchain*	*e.g. Government blockchain*
Without permission to write	*e.g. Surveillance or insurance blockchains*	*Public blockchain*

Table 1. *Blockchain* permissions

Two configurations are generally discussed by experts in the field. On the one hand, private or consortium blockchains require both permission to read the stored data and permission to write to it. They develop very quickly, because their governance is manageable and the confidentiality of data is relatively guaranteed, since only a limited number of actors can access them. This limited number of actors also makes it easy to determine responsibilities if a problem occurs. These are typically blockchains corresponding to a specific use, such as the blockchain Everledger (that we have presented above). On the other hand, public blockchains are open to all, creating issues of governance and responsibility. These are the first blockchains to have been developed with the creation of crypto-currencies, such as the bitcoin or the ether. The confidentiality of their data is guaranteed by the use of pseudonyms. Nevertheless, all transactions corresponding to a pseudonym are visible to all and can be explored using search tools such as blockchain.info.

The other two configurations of permissions are less common, but they are also being rapidly developed. As an example of blockchains without permission to write to, but with permission to read from it, one can think of certain governmental blockchains, such as cadastral registers. The US state of Delaware is currently developing an initiative with the start-up company Symbiont.io to automate its Initial Public Offering (IPO) process through smart contracts. As for blockchains without permission to write, but with permission to read, we can also think of the blockchains of insurance companies that monitor events with connected objects and that trigger

automatic reimbursements through smart contracts, if the required conditions are met.

2.2 Rivalry and exludability

Economic goods are generally considered to have two characteristics: rivalry and excludability. On the one hand, data stored in a blockchain remains non-rival. On the other hand, the mode of governance of the blockchain allows, in some cases, to exclude certain users from reading or writing data. Thus, one is either in the case of non-rival and excludable goods, i.e. clubs, or in the case of non-rival and non-excludable goods, i.e. public goods.

Now consider the tokens generated by the blockchain. These tokens are rival, and only one person can use a given token at a given time. On the other hand, we can exclude some people from accessing it (private blockchain), in which case we are dealing with a private good. If everyone can access the resource, as in the case of public blockchains, we are in the presence of commons.

2.3 Negative and positive externalities related to mining investments

When a blockchain requires mining to validate new blocks, there are two types of direct network externalities.

First, there are positive network externalities related to the global level of security of the blockchain. Positive network externalities occur when the value of the product or service increases with the number of users. For example, the value of some software increases with the number of its users because it is easier to exchange files with friends, colleagues and other contacts. In the case of the blockchain, each additional node reinforces its security, because it is more difficult to carry out attacks such as the 51% attack or to guess the winner of the mining process and to carry out an attack on his computer infrastructure using DOS attacks (Denial Of Service).

However, there is also a negative externality: when a mining pool invests in a new equipment, it increases its marginal income, but it also increases the overall cost of mining because the global difficulty of the cryptographic problem to be solved increases with the number of miners and their hash-power. For example, for the bitcoin or the ether network, the difficulty of the cryptographic problem to be solved using a proof-of-work consensus increases with the global hash-power of the network (see Figure 3). There is therefore a risk of overinvestment in mining capacity, as individual miners do not take into account the negative effect on the entire network. It is important to emphasize that increasing the difficulty of mining reduces the incentives to mine and increases the validation time, and therefore the very effectiveness of the blockchain. This mechanism can be paralleled to the tragedy of the commons (the hash-power). There is therefore a risk that the mining capacities could be strongly concentrated in the hands of a small number of actors, nullifying the principle of the public blockchain and creating governance issues (see section 7).

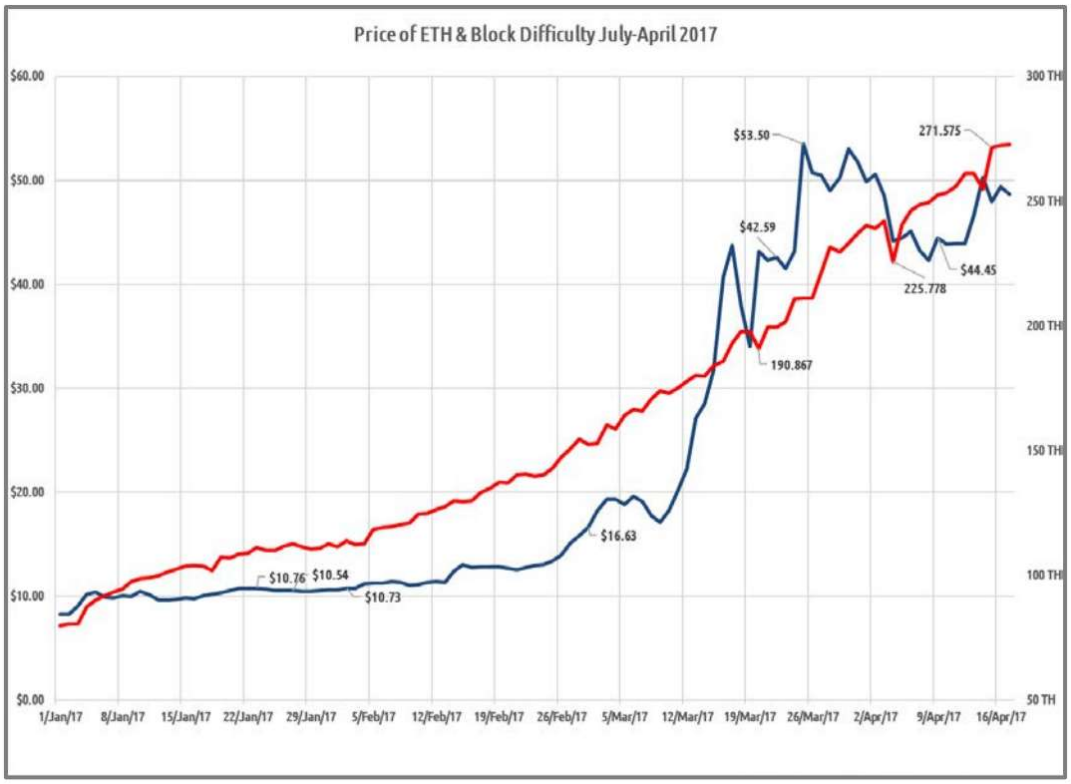


Figure 3. Price of ether (blue line) and block difficult (red line), January 2017 – April 2017. Source: Karan (2017).

Private blockchains avoid negative mining externalities, at the risk of creating a tragedy of the anti-commons, which reflects the idea that there would be no common resources, but only private resources protected by private property law.

2.4 Cost of mining

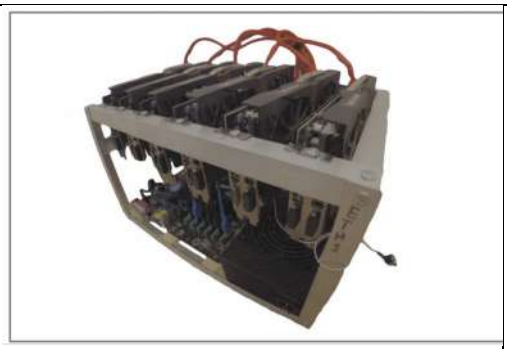
A standard ASIC (Application Specific Integrated Circuit) unit costs about EUR 250 for bitcoin mining. A typical mining pool use hundreds of ASIC units (see Figure 4). In November 2015, the haoBTC mining pool had a fixed setup cost of USD 600000-700000. The annual operational cost was USD 242000. Electricity represented USD 219000.

(a)

(b)

Figure 4. (a) ASIC Butterfly Monarch 700 (SHA-256); (b) haoBTC mining farm, Kangding, Sichuan, 2015 (source: https://news.bitcoin.com/china-bitcoin-myths-realities/ last checked on May 17, 2017);

For ether mining, a GPU rig requires graphics cards that cost about USD 250 per unit. A standard rig has usually 4 to 6 graphics cards. A typical 5 GPU system costs about USD 1500 and consumes about 750W for a hash power of 100 MH/s. Computing the expected profit of any mining installation requires a scenario on the evolution of the hash difficulty and the price of the ether (see Figure 3) in addition to a forecast of the evolution of the price of electricity and of the depreciation of the hardware.



(a)

(b)

Figure 5. (a) A 5 GPU ethereum mining rig; (b) Genesis mining farm, 2016 (source: http://uk.businessinsider.com/photos-iceland-bitcoin-ethereum-mine-genesis-mining-cloud-2016-6/#the-price-of-ethereum-is-now-1670-while-streng-says-electricity-costs-to-mine-it-are-385-12 last checked on January 2, 2018)

2.5 Indirect network externalities

Blockchains can be analyzed as a platform matching different groups of agents. For instance, crypto-currencies can be used by consumers and by merchants as a payment instrument. They can also be exchanged in platforms linking borrowers and lenders. These platforms can be considered as multi-sided in the sense that two or more groups of agents interact on them and that there are indirect, often positive externalities: the value of the service offered by the platform for one group of agents increases with the number of agents of the other group. These markets are typically heavily concentrated in the digital economy. We can think of platforms such as YouTube, Google, Facebook, eBay, etc. It is interesting to note that contrary to these examples, public blockchains are not centralized, they are on the contrary highly decentralized and distributed (we will return to this point in Section 4).

2.6 Differences between private and public blockchains

We now compare the advantages and disadvantages of private blockchains to those of public blockchains. If the public blockchain represents a solution of decentralized trust for many, the private blockchain can be completely centralized or controlled by a small number of actors, challenging the libertarian dream of the public blockchain.

One of the major differences between private blockchain and public blockchain is the confidentiality of smart contracts, of transactions and of personal data.

As noted earlier, it is relatively easy to guarantee the confidentiality of data stored in private blockchains, since only a limited number of nodes can access it, which explains their rapid development.

The data stored in the public blockchains are, on the contrary, accessible to all, since data are used to build a decentralized public register. That said, it is possible to guarantee certain forms of confidentiality in public blockchains using pseudonyms (this is the case for the bitcoin network). In addition, certain technical solutions are developed on public blockchains to protect sensitive data. For example, the Massachusetts Institute of Technology (MIT) Enigma project provides a health data blockchain in which a node of the network cannot access the integrality of the data requested by a user by implementing a Secure Multiplatform Computation infrastructure: sensitive data can only be partially disclosed. Other initiatives are based on a zero knowledge proof algorithm that checks the validity of transactions, while keeping the metadata encrypted.

Private blockchains and public blockchains also differ on three other dimensions: the effectiveness of the validation process, the governance of the blockchain and the issue of legal responsibility.

First, there are scaling issues in a public blockchain using a consensus based on proof-of-work (like the one used by the bitcoin network), since it requires a hash-power that grows with the size of the network and requires several validations before adding a new block (typically 10 minutes on the bitcoin network). Other types of consensus are studied, such as proof-of-stake, on the Ethereum network. Private blockchains use other types of consensus to write thousands of transactions per

minute, for instance based on delegated proof-of-stake. However, increase in the speed of block validation comes at the cost of security, since there are fewer nodes of the blockchain that validate new blocks in private blockchains.

Secondly, the governance of a public blockchain requires the agreement of all the nodes of the network to implement a major change in the communication protocol (we will develop this important point in section 7). A decision can be made by a much small number of nodes in the case of a private blockchain.

Finally, the question of legal responsibility arises and remains open. Blockchain specialists consider that it is much easier to establish responsibilities in the case of a private blockchain (especially if the legal contract underlying self-executing smart contracts is subject to the same national law). In the case of an international public blockchain, this question is the subject to legal analyzes. The discussion is summarized in Table 2.

	Private Blockchains	***Public Blockchains***
Governance	**+**	**-**
Indirect externalities (multi-sided platforms)	**0/+**	**+**
Security externality	**0**	**+**
Effectiveness of the validation process	**+**	**-**
Negative mining externalities	**0**	**-**
Transparency	**-**	**+**
Confidentiality, privacy	**+**	**0**
Accountability, legal responsibilities	**+**	**-**
Openness and interoperability	**-**	**+**

Table 2. Comparison of private and public blockchains; ‘0’ indicates a neutral effect, ‘-’ indicates a negative effect, ‘+’ indicates a positive effect.

3 Blockchains and the economics of security

We now study the factors that can influence the decisions of companies to secure their IT infrastructure. We will first argue that economic forces push companies to underinvest in computer security. We will then analyze how the blockchain can provide solutions to this underinvestment problem.

Consider customer data. First, there are negative externalities associated with the lack of data protection that are not offset by market mechanisms (spam, black market for digital identities, etc.). This can lead to situations where customer data is exposed to leaks, fraud or theft. Moreover, companies develop strategies enabling them to rapidly reach critical mass, at the detriment of their data infrastructure. Finally, information asymmetry between customers and companies with respect to the security level of the data infrastructure allows companies to share their customers' personal data with third parties who do not necessarily have incentives to protect them.

3.1 Public goods

Security is non-rival and non-excludable. These two characteristics imply that a single agent cannot capture the total surplus that he or she creates for the whole society when he or she invests in security. There will therefore be underinvestment in computer security by the private sector. In addition, in an ecosystem of data-sharing companies, individual members benefit from the efforts of other members who secure the system. Data in the ecosystem will therefore be poorly protected.

3.2 Network externalities

Moore and Anderson (2012) study the effect of network externalities on the level of security implemented by software manufacturers. It is important for a company that wants to dominate a market characterized by strong positive network externalities to quickly reach a critical mass. In this context, there are little incentives to devote much time and effort to the security of personal data. On the contrary, it is often more profitable to let others find bugs and security holes, then to solve these problems by means of updates and software patches. The problem is exacerbated when the company has a dominant position and customers cannot switch to the competition (data lock-in).

3.3 Business models based on data exchanges

When companies develop marketing strategies based on advertising, they generate revenue by selling their customer data to third parties. Such companies are encouraged to write general terms of service in order to be able to use (and re-use) their customer data extensively. When personal data is transferred to third parties, it is really difficult for the customer to determine how his data is used, stored and secured (information asymmetry). Real-time auctions on ad exchanges exacerbate these problems because personal data available in cookies is transmitted and matched by other platforms and/or third-party companies and it is therefore difficult to track data usage.

3.4 The *blockchain* approach

The blockchain brings solutions to underinvestment in security by giving explicit incentives to secure data to private actors. In the case of the proof-of-work consensus used in the bitcoin network, the incentives are directly monetary in the form of gains in a crypto-currency. In the case of the proof-of-stake consensus, securitization makes it possible to engage more in the governance of the blockchain and to obtain shares of voting rights. The governance of the blockchains also allows the nodes of the network to coordinate in order to counter attacks (see Böhme et al., 2015).

Nevertheless, there are still security concerns with blockchain networks. First, the bitcoin hash algorithm is based on a SHA-256 (Secure Hash Algorithm) technology, which could become obsolete. Moreover, unlike the terminology used, smart contracts are only bits of code, which can contain bugs, like any computer program. One could mention with this respect the smart contract DAO, on the ethereum

network, which contained a bug that allowed a group of hackers to steal about 50 million dollars (this led to a hard fork to undo the damage done by the smart contract; see Section 7). Finally, the data is protected by a private key which, if lost, prevents access to the stored data but, if it is extorted, compromises the security of the data network.

4 Blockchains, the nature of the firm, business models, and industrial organization

The blockchain may also question the definitions of the firm and of wage labor, as well as the organization of industries. Each digital industry is today dominated by a company in a quasi-monopoly position. This is mainly due to two economic forces. First, investments made by the incumbent firms in equipment and infrastructure generate fixed costs of production and entry into the market, which create increasing returns to scale that favor the incumbent firm producing on a large scale. Secondly, the direct and indirect positive network externalities in multi-sided platforms create a centrifugal force generating a "snowballing effect" and leading to winners-take-all situations. These two forces are challenged by decentralized blockchains.

4.1 Smart contracts and Decentralized Autonomous Organizations

A blockchain can implement a decentralized voting system. This may call into question the very role of hierarchical structures in which the decisions of workers at the bottom of the hierarchy are delegated to a superior, going up successively to the CEO. Using the blockchain voting system, all these workers could in principle choose the strategic decisions themselves. By pushing the reasoning to the extreme, one could run a company without a CEO (for a discussion, see Swan, 2017).

It is often accepted, after the work of Coase (1937), that the size of the firm is determined by transaction costs required to perform a task internally or externally. Blockchain extends contractual relationships to lower-cost suppliers and workers. By pushing the reasoning further, the blockchain has two consequences on business processes and wage labor. First, the concept of a firm is itself questioned: an industry could be organized around a blockchain and smart contracts concluded between different units of relatively small size in a Decentralized Autonomous Organization. Tapscott and Tapscott (2016) argue that the blockchain change search costs, contracting costs, coordination costs and the costs of (re-)building trust. The blockchain challenges existing business models and innovation models. Secondly, wage labor could also be replaced by self-employment. This trend is already visible on centralized platforms like Uber, but it is not contradicted by the advent of decentralized blockchains.

4.2 Market entry and contestability

If fixed IT and hardware infrastructure costs coupled with strong direct and indirect positive network externalities discourage entry in online markets, the blockchain technology allows independent agents to pool resources to perform automated tasks. Some specialists argue that Google computer power only represents 1% of the

computing power of the bitcoin network (see https://www.ccn.com/bitcoin-100-times-powerful-google/ last checked January 2, 2018). Markets become again contestable and the entry of a new eco-system could pose a challenge to existing companies (even those with a near monopoly position).

4.3 Delegation of tasks

Finally, the blockchain, through the decentralization of tasks and work, represent a counter-trend to the development of centralized platforms such as Uber or Airbnb. Indeed, if we go back to the example of Ubik and the smart door, any object with an smart lock allows a person to automatically rent an apartment or to open safes. However, even if some observers put forward the idea that the blockchain could end up "uberizing Uber", nothing is less certain. Indeed, Uber could also develop its own blockchain to automate its contracts with drivers. In the same way, Airbnb could develop its blockchain to automate the payment of rentals and the concierge services. More generally, governments and large corporations could use private blockchain to reinforce their established power by preventing some users to access the resources available on their blockchains.

5 Economic perspectives

The blockchain is key to the development of the Internet of Things. However, the speed at which this transformation will take place is the subject to a debate among specialists. There are two opposing views: the vision of those who think that the technology will take decades to spread and transform into the industry, and the vision of those who think that the blockchain is a disruptive technology.

5.1 Is the blockchain transformative…

Iansiti and Lakhnani (2017) recently suggested a parallel between the diffusion of transformative technology such as TCP/IP and the blockchain technology. In both cases, this diffusion takes place in four phases, which may take decades to reach the last phase, that is the transformative phase (See Figure 6).

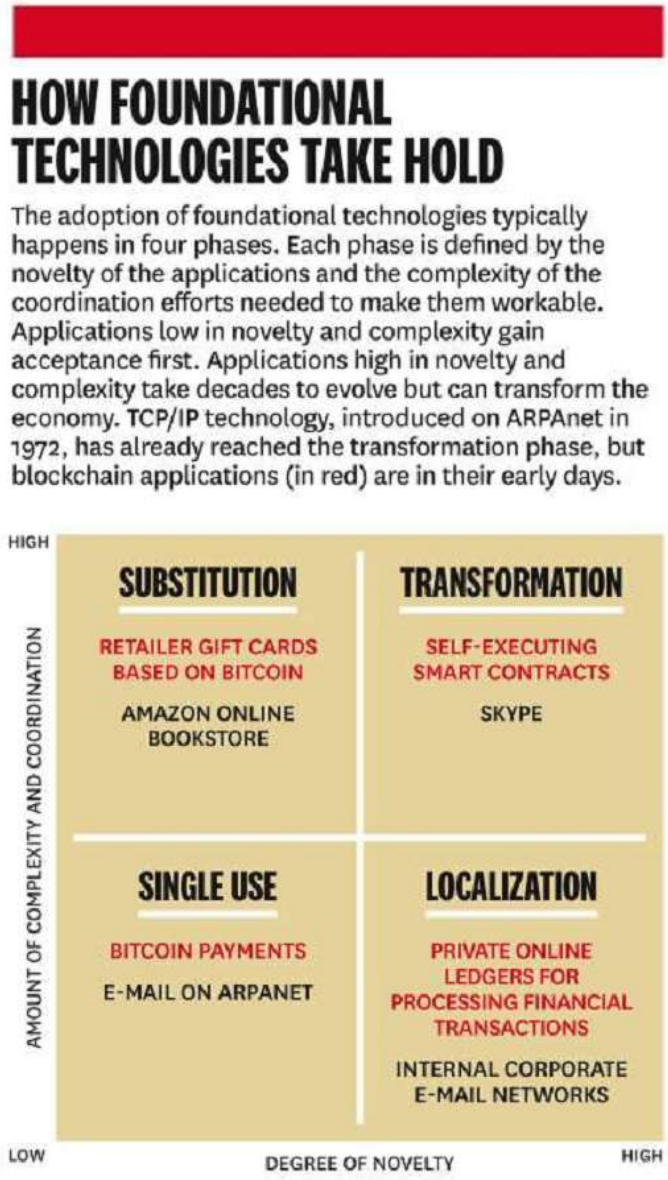


Figure 6. How foundational technologies take hold. Source: Iansiti et Lakhani (2017).

5.2 … or disruptive ?

On the contrary, IBM specialists see the blockchain as a disruptive technology with multiple applications ranging from logistics to financial transactions (see Figure 7).

Vectors of disruption	Liquification of the physical world
Unlock excess capacity of physical assets	Instantly search, use and pay for available physical assets
Create liquid, transparent marketplaces	Real-time matching of supply and demand for physical goods and services
Enable radical re-pricing of credit and risk	Digitally manage risk and assess credit, virtually repossess and reduce moral hazard
Improve operational efficiency	Allow unsupervised usage of systems and devices, reduce transaction and marketing costs
Digitally integrate value chains	Enable business partners to optimize in real-time, crowdsource and collaborate

Figure 7. Five factors of disruption: How the IoT will increase our leverage physical assets. Source: Brody and Pureswaran (2014).

5.3 Analysis

The TCP / IP protocol is both similar to the blockchain from a certain point of view and different from another. Indeed, the TCP/IP protocol is an open protocol, as is the public blockchain. On the other hand, the TCP/IP protocol was initially only known to a handful number of specialists in a world where personal computers were still rare, whereas the bitcoin and the second generation of blockchains have been very quickly adopted by millions of users (see Figure 8). Overall, the blockchain represents more a disruptive technology that will be adopted massively than a slowly spreading technology. But there are nevertheless some issues that need to be resolved (that we present in the conclusion).

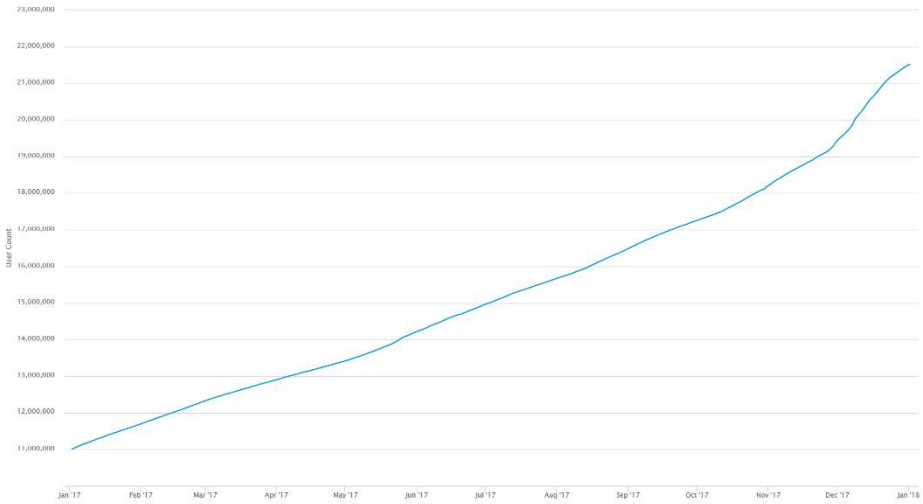


Figure 8. Number of bitcoin blockchain wallets. Source: blockchain.info (last accessed on January 2, 2017).

6 Case study: an economic analysis of the bitcoin blockchain

The bitcoin network is the first public blockchain network to have been developed in a massive way. In May 2017, there were nearly 7,000 nodes on this network. Each of these nodes can hide pools (shared resources) and farms with several thousand ASIC (Application Specific Integrated Circuit) units developed to mine new blocks. The main pools and farms are located in China.

A crypto-currency has value only if it is considered as a currency by all the participants in the monetary system. It therefore needs to be rare, in the sense that it cannot easily be copied (a problem equivalent to that of counterfeit notes for traditional currencies). This property is satisfied by the blockchain network, which guarantees the absence of double expenses. In addition to this value related to acceptance, the bitcoin has value through various economic mechanisms that are not exclusively monetary. We analyze the demand and the supply of bitcoins. We begin with the analysis of the cost of validating blocks and then move on to demand analysis.

6.1 The supply of bitcoins

The monetary creation is divided by 2 every 210,000 blocks to arrive at a total of bitcoins in circulation (except for lost ones) of 21 million. This monetary rule depends on the bitcoin protocol that can be modified by the Bitcoin Foundation, as we will discuss in Section 7. Moreover, for a given demand, this downward trend in the supply of new bitcoins automatically increases the price of the bitcoin. Ultimately, as the supply becomes inelastic, the price of the bitcoin is essentially determined by demand. A continuous increase in the value of the bitcoin could lead to a situation where people prefer to keep bitcoin for themselves rather than spend them (making them useless) and to a decrease in the price of goods and services denominated in bitcoins, generating a deflationary pressure in the economy (people expecting prices to drop further). The deflationary issue is the subject of debates in the bitcoin community. Anyway, the fixed monetary rule can be modified to respond to fluctuating market conditions, at the risk of a hard fork.

Electricity is the main component (between 90% and 95%) of the total cost of a mining farm. Böhme et al (2015) evaluated that the consumption of the bitcoin network to more than 173 megawatts of electricity on a continuous basis. This accounted for about 20% of the production of a nuclear power plant and $ 178 million annually (at the price of residential electricity in the United States). This amount may seem important, but Pierre Noizat estimates that it is not more than the annual electricity cost of a global ATM network (estimated at 400 megawatts) (http://e-ducat.en/2015-11-28-cop21-and-blockchain/ last checked on May 2017, 2018).

This cost could increase substantially in the future. Indeed, the proof-of-work consensus based blockchain plans an increase in the difficulty of the cryptographic problem to be solved according to the global hash-power of the network. This negative externality could raise the electricity cost for all miners validating blocks in the bitcoin blockchain.

The bitcoin can also be bought and sold on a trading platform in the secondary market. The value of the bitcoin is then closer to the value of a financial investment for which investors anticipate gains. Speculation may lead to an appreciation of the bitcoin.

6.2 The demand for bitcoins

The demand for bitcoins results from several user concerns that we analyze in this section, starting with the positive factors and concluding with the risks.

6.2.1 Financial privacy

Governments are increasingly limiting the use of cash to show their anti-money laundering efforts and to stop the development of black markets. Cash is the only 100% anonymous payment method. The bitcoin and the other crypto-currencies come second. Indeed, the system of pseudonyms used by the protocol bitcoin makes it possible to mask the identity of the persons making transactions. Some crypto-currencies, such as the Zcash, can also mask the metadata of a transaction.

Why use an anonymous payment instrument? There are many reasons. First, the use of an anonymous payment instrument makes it possible to avoid leaving traces, which can be used for surveillance by a government, by employers and by certain enterprises (in particular banks, insurance and Internet companies). Indeed, Internet companies and banks practice price discrimination strategies that can sometimes turn against consumers. Leaving traces through payment data can also push companies to solicit more customers on new commercial offers and targeted advertisements that can be considered as nuisance by consumers. Secondly, paying with an anonymous payment instrument also limits monitoring by family members and relatives (little sisters or sousveillance). This will be the case for a payment made from a common account. Thirdly, people want to remain anonymous when they make gifts, or at least they want to keep private the amount that they paid for the gift. Anonymity makes it possible to limit the externalities linked to the traces left during a purchase; it has therefore an economic value. The bitcoin, by using pseudonyms, also creates economic value by masking the meta-data of transactions.

6.2.2 Bitcoin operates in times of crisis and thus avoids capital controls

Bitcoin emerged just after the financial crisis of 2008. This is not a coincidence. This period witnessed the power and the will of governments and central banks to control cash withdrawals and money in circulation. There are very few ways to escape these two institutional constraints. The bitcoin is one. Indeed, even if cash withdrawals are prohibited, owners of bitcoins can still pay using their private key.

6.2.3 Network externalities related to improved security

First, the level of security increases with the number of nodes in the network, because more computational power is required to threaten the security of the blockchain (through a 51% attack, double spending or DOS attacks). Moreover, a DOS attack is more difficult to carry out because it is more difficult to guess who is the winner of the mining process. There are therefore positive network externalities: the value of the bitcoin increases with the number of nodes participating to the network.

6.2.4 Indirect network externalities related to the payment instrument

Bitcoin is a payment instrument, in the same way as cash, bank cards or Visa / Mastercard / American Express cards. The bitcoin can therefore be analyzed using the theory of multi-sided markets, which consider situations in which two groups of economic agents benefit from positive cross network externalities. Indeed, a consumer values a payment instrument if it is accepted by the merchant with whom he makes a transaction. Conversely, a merchant proposes a payment instrument used by many customers. Consequently, the dynamics of the multi-sided markets create virtuous cycles, which can start with a slow deployment phase followed by an acceleration phase. If the bitcoin were to experience such a phase, its value could rapidly increase. Moreover, the commission paid by the consumer or the merchant is not controlled by a platform serving as an intermediary. Finally, the bitcoin can be used for international money transfers without paying exchange fees to banking institutions.

6.2.5 Bitcoin can discipline governments

The bitcoin (the same is true for the other crypto-currencies) can be considered as an alternative currency not controlled by a central bank. Some economists, such as F. Hayek, consider that these alternative currencies, which compete with the official currency, can discipline governments that would be tempted to finance their debt by inflation. In this case, consumers and investors would turn away from the official currency to buy the alternative currency and thus create deflationary pressure on the official currency.

6.2.6 Risks

Among the factors reducing the demand for bitcoins, the risks related to regulation are particularly strong. On the one hand, a State could request that the capital gains generated by the purchase and sale of bitcoins be declared. In addition, bitcoins can be used in regulated sectors (such as insurance or banking) and their use could therefore also be regulated. Finally, there is always the risk of losing the data on the hard disk on which the private key is stored, and thus losing associated bitcoins, or that a state imposes access to private keys for security reasons.

Part 3 – Forks and Oracles

7 Forks: the governance of the Bitcoin network

The issue of governance is crucial to understand the future of crypto-currencies. Indeed, if nodes of the network disagree over the evolution of the communication protocol, the network faces the risk of being split into several networks (hard fork) with currencies incompatible with each other. The most important issue is the choice of the consensus rule for the validation of new blocks. There must be consensus on consensus, which technology alone does not seem to be able to provide.

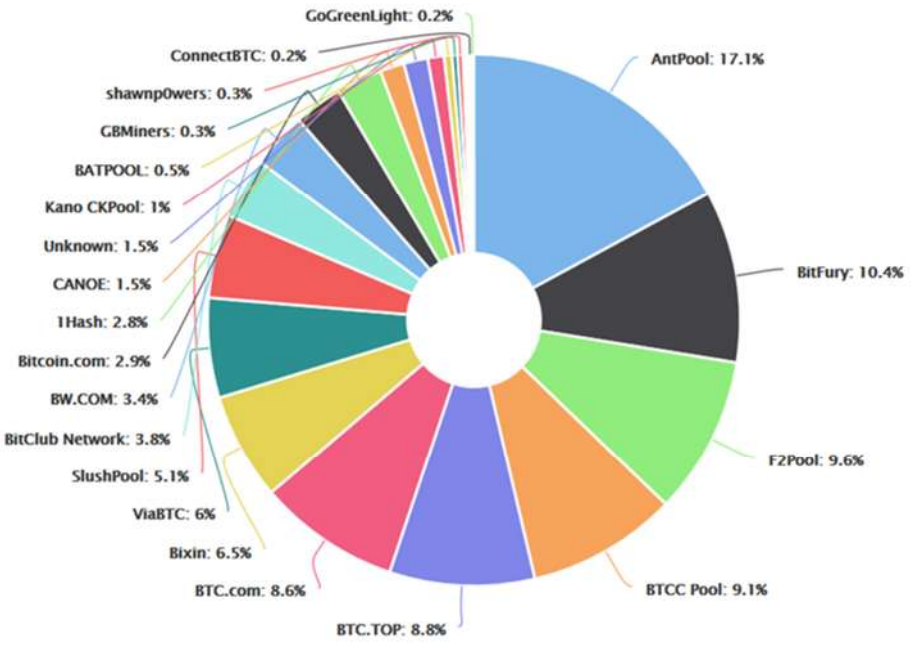


Figure 9. Principal mining pools and farms on the Bitcoin *blockchain*. Source: blockchain.info (checked on May 22, 2017)

It should be noted that the distribution of pools clearly indicates that hash-power is concentrated in the hands of about ten pools, which therefore have an important weigh in the decision-making process with respect to changes in protocol rules (see Figure 9).

A protocol is the equivalent of grammar for a spoken language. We can add or remove rules, but it is at risk that people can no longer understand one another. In the case of the bitcoin network, one speaks of soft fork and hard fork when we want to qualify these changes in the rules.

There are several implementations of the bitcoin protocol: bitcoin Core, Libbitcoin, bitcoin XT, bitcoin Classic. All these implementations are globally governed by core developers. For example, Bitcoin Core is governed by a meritocratic peer review process through a Bitcoin Improvement Proposal process moderated by Wladimir Van Der Laan, which significantly contributes to the code of the bitcoin protocol (see Figure 10).

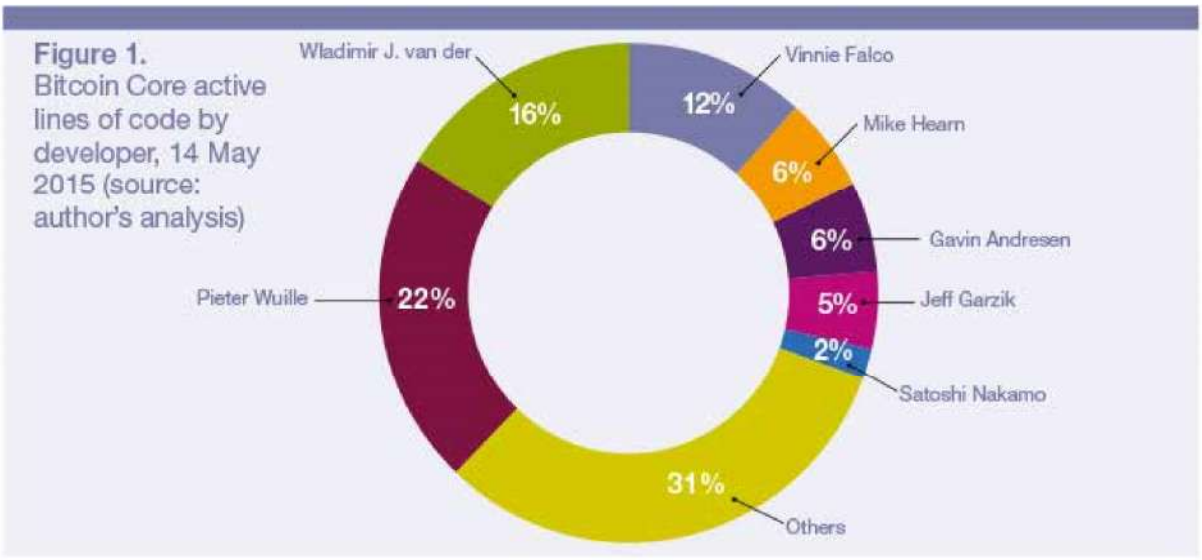


Figure 10. Major code contributors to the *bitcoin* protocol (May 2015). Source: Walport (2016).

The governance of the bitcoin protocol is adopted by the nodes of the network that decide to implement a change or not. The change of protocol can affect the four layers of the bitcoin network: the consensus rule, the P2P layer, the Application Programming Interface (API) and the applications. For the sake of brevity, we will only discuss the consensus rule.

To add a rule, a 95% majority of the hash-power is required. The old blocks become invalid and the non-upgraded nodes lose in safety and efficiency (hash-power). To force miners to respect users, a soft fork could render the mining equipment obsolete through a new mining algorithm. To remove a rule, it is necessary that all the full nodes adopt the change, otherwise there is a risk that the bitcoin network could split into two incompatible networks (hard fork).

In conclusion, technology cannot solve governance issues on its own. This is a paradox: the technology is built to secure data registers and execute tasks in a decentralized and distributed way, but the technology cannot manage its own governance.

8 Oracles

Oracles are trusted entities signing claims about the world outside of the blockchain. The need for oracles arises when smart contracts require external data generated by real-world events. Oracles can be software-based, hardware-based, or based on

human intermediaries. A software-based oracle can be programmed to search for and parse text from online sources and can check events happening on other blockchains. Hardware oracles get external data from sensors and the Internet of Things. Human oracles are necessary for tasks that are too costly or too complex to be executed by machines: for instance, reviewing a complex insurance claim, checking whether or not a scientific breakthrough has been made, convert bank notes into crypto-currencies. They can be directly liable in case of problems. Some events may be too complex to be assessed for a single oracle and may require the contribution of a network of oracles.

There are two main issues with oracles: oracles need to truthfully report the states of the world; and they have to secure data and to guarantee the privacy of transactions.

8.1 Software oracles

Software oracles extract the needed information online or in other blockchains and push it into the smart contract (for instance, temperature, prices of commodities and goods, flight or train delays, etc.).

There are some technical pros and cons for using software oracles, but trusting the source of information is the main issue. For instance, edition wars can manipulate information available on Wikipedia. Oraclize allows an auditor to verify if a specific web page was accurately retrieved (using a proof of honesty or TLS notary proof). There are many other software-based oracle solutions available in private blockchains.

8.2 Hardware oracles

There are some facts that cannot be determined through public data attestation. Some applications require to get information or readings from the physical world, where the data only exists in connected object (for instance the state of a door lock, the location of a container, the current speed of a vehicle). Hardware oracles provide a secure and non-tamperable way to collect sensor data from connected objects. To be able to securely report a reading from a sensor, hardware oracles require a cryptographic attestation of the sensor reading, authenticating the origin of the measure and an anti-tampering installation of the reader device, rendering it inoperable (by wiping the private key) in case of a manipulation attempt.

8.3 Human oracles

Human oracles are needed for validating complex requests such as the legal status of a company or tasks that are too costly to be executed by machines. For instance, startup companies specializing in peer-to-peer money wiring need “human ATMs” (sic) to deposit cash into a crypto-wallet and to withdraw bank notes from a crypto-account.

8.4 Consensus based Oracles

Decentralized prediction markets such as Augur or Gnosis rely on Oracles to settle outcomes of events. However, to avoid market manipulation, these Oracles cannot

be based on the trust of one single entity (e.g. Google or Wikipedia). The solution is to use rather complex consensus mechanisms based on reputation, ultimately building decentralized oracles who rely on the 'wisdom of the crowd'. For further security, a combination of oracles can be chosen for event resolution. For example, a market creator may select 5 oracles for resolution and require a 3 out of 5 majority for event decision. By requiring oracles to submit security deposits, consensus-based oracle systems create risk of loss for oracles who lie about event resolution or attempt to collude to do so.

8.5 Token-based distributed oracles networks

The idea of a distributed oracles network is to decentralize the process of verifying external data by using a network of oracles incentivized by tokens (for instance the PHI token for the Pythia network, the AEON token for the Aeternity network and the LINK token for the Chainlink network). In the case of the Aeternity network, there is only one consensus mechanism for adding blocks and verifying the truthfulness of oracles using “state channels”. State channels increase scalability by making groups of transactions independent of each other. This allows them to be processed in parallel.

8.6 Confidentiality of transactions

Oracles are necessary to run smart contracts based on data lying outside of the blockchain. They come with their own set of challenges. For example, an oracle needs to be able to provide a tamper-proof source of information. Confidential queries are another issue. If a smart contract needs information on a personal bank statement or a medical record, a query from the oracle to the website would need to contain login, password or other private information. To that end, researchers at Cornell's Initiative for Cryptocurrencies and Contracts (IC3) have launched an oracle service that allows ethereum smart contracts to obtain trustworthy information and to securely send confidential queries to websites.

Nevertheless, Oracles network can help solve the problem of blockchain governance. In the Aeternity blockchain, prediction markets are proposed to implement the governance of the blockchain. The communication protocol could be governed by user input. A prediction market could exist where beneficial changes to features and protocols would result in a higher token value. The incentive to increase the value of a token would allow the blockchain community to decide efficiently which changes to implement.

9 Conclusion

To conclude, the blockchain is a revolutionary technology that is not limited to bitcoin transactions. The development of an ecosystem around smart connected objects will probably not happen without the blockchain. The blockchain opens the door to the liquification of the physical world, the economy of real-time micro-transactions and smart data sharing. Smart contracts depend on reliable data from the physical world.

New oracle solutions based on markets for trust using the idea of truth as a consensus are promising.

However, a number of issues still need to besolved. First, responsibilities need to be clearly established and the laws applicable to public blockchains clearly identified. Secondly, the application of the General Data Protection Regulation (GDPR) in Europe must be guaranteed (right to be forgotten, data portability, etc.). Thirdly, it will be necessary to determine the tax and legal status of crypto-currency gains. Fourthly, it will be necessary to think about how to articulate smart data (for instance ethical coins that cannot be used to purchase weapons) coming from blockchains with the principle of Net neutrality in Europe.

10 References

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. The Journal of Economic Perspectives, 29(2), 213-238.

Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. IBM, September.

Coase, R. H. (1937). The nature of the firm. Economica, 4(16), 386-405.

Dick, P. K. (1969). Ubik. 1969. New York: Vintage

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. Harvard Business Review, 95(1), 118-127.

Karan, E. (2017), A quick guide on building a GPU Mining Rig (Edition 3.2): Best for Ethereum and Ethereum Classic, Amazon Kindle edition

Lanier, J. (2014). Who owns the future?. Simon and Schuster.

Moore, T., & Anderson, R. (2012). Internet security. The Oxford Handbook of the Digital Economy (Oxford University Press 2011).

Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

Suarez, D. (2006). Daemon. Penguin.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.

Walport, M. G. C. S. A. (2016). Distributed ledger technology: beyond blockchain. UK Government Office for Science.