Blockchains, a report

José Deodoro de Oliveira Filho
Master in Policy Economics
University of Illinois at Urbana-Champaign
dlvrflh2@illinois.edu

1. INTRODUCTION

Blockchain is an emerging information technology that allows us to create public digital ledgers to instantly records transactions between users in a network of computers (such as the Internet). It has unique properties that yield potential to reduce costs throughout the financial industry and to enable applications in diverse areas, some of them not viable using current technologies and some never imagined before.

The technology was created just prior the crisis of 2008 to power a product, bitcoin, by itself a broad and interesting subject. Bitcoin has been around for the last eight years, it has a large number of supporters and is already considered a great success in the incipient *Fintech* niche. On that account, it will be used frequently as an example throughout this report, in order to better illustrate the features, flaws and potentials of blockchains.

This report starts with a tale of mystery, the genesis of blockchains (along with bitcoin). Next, technological aspects of blockchains are briefly exposed in three sections: how it works, its properties and some shortcomings. The following three sections discuss interesting aspects of the current state of blockchains: the reward system (economic incentives in the bitcoin network), related patents, and how it is evolving. Discussion about the practical and foreseen uses for blockchains are left for the final three sections. Among these, the final two sections particularly look at the advantages and drawbacks of practical blockchain applications, by comparing bitcoin to legacy payment systems.

2. HISTORY

The history of the blockchain technology is intertwined with the creation of bitcoin. The latter it a decentralized cryptocurrency or, as defined by Wikipedia, a (decentralized) “medium of exchange using cryptography to secure the transactions and to control the creation of new units” [3]. It was first described in a research paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System”, published by a Satoshi Nakamoto on November 1st of 2008 in his site, bitcoin.org. The author himself announced its availability that same day in the *cypherpunk mailing list* (an Internet mailing list dedicated to cryptography) [4].

It is generally accepted that *Satoshi Nakamoto* is a pseudonym, some believe it was most likely used by a small group of people rather than an individual. The mysterious inventor of bitcoin and blockchain remains anonymous to this date: he was skilled enough to use safe, encrypted messages to mailing lists, and crafted enough to write texts that disclosed no personal information about their author. Nakamoto has given up communications in the spring of 2011, after announcing he had “moved on to other things”, and remains silent ever since [5].

In his paper, he describes bitcoin as a “system for electronic transactions without relying on trust”. His invention achieves goals pursued by researchers for a long time [0]: the creation of a digital currency technology which carries some of the properties of real world cash, most importantly that it would allow for anonymous and reliable transfers of assets from a subject to another [6]. Up to that point, every financial transaction effected in the Internet depended upon trust of the participants over intermediaries (such as banks), which guarantee to both actors that assets would be retrieved from payers funds and deposited in sellers account. By design, there was no way to make an anonymous peer-to-peer financial transaction in the Internet until the appearance of bitcoin. [2]

Eliminating the need of a trusted third party and allowing for secure anonymous electronic transactions had been goals of several projects since before the Internet went mainstream. Pioneers foresaw the boom of markets of digital assets which would follow its popularization, and considered this a necessary condition for the creation of those markets: people would need a way of securely purchasing products like digital music, books or movies over the network. At that time credit cards weren’t considered a viable option specially due security concerns: much of a “classical” credit card transaction depends on transmitting sensible information over the wire, such as card details and cardholder’s information (number, expiration date, cardholder name, etc) [10]. In the mid–1990s, legacy card transaction systems were adapted to the Internet using secure communications (the HTTPS protocol), minimizing security problems. Although they didn’t present all desired features, these systems have been considered good enough for applications and are used up to this date. The mechanisms within bitcoin (specifically, blockchains), on the other hand, do carry those features.

The first node came online on or about January 3rd, 2009, when Nakamoto minted the *genesis block*, the first batch of 50 bitcoins. On January 12th, 2009, Hal Finney was the recipient of 10 bitcoins in the first transaction [11]. The first transaction for tangible goods was made on May 22nd, 2010: 10,000 bitcoins were transferred from Laszlo Hanyecz (who lived in Florida) to a person in London, who ordered a pizza from Papa John’s and had it delivered to Hanyecz’s house. The arrangement was made through an Internet forum populated by the first bitcoin enthusiasts. The 10,000 bitcoins were valued at US$41 at that time [7], by today’s exchange rate that pizza cost over 4 million dollars.

3. HOW IT WORKS

A blockchain exists in a network, composed of nodes. A node may be a peer (or client), which has the keys to a unique account in the network; or a verifier (or miner), which works to validate transactions and register them into the blockchain. Transactions are records of exchange of information between accounts. In bitcoin, accounts are *wallets* and the information exchanged in transactions, the balance and digital signatures of two accounts.

Nakamoto summarizes the steps needed to run this network as follows [6]:

- A peer informs nodes a transaction is to be registered. The network has mechanisms for nodes to discover and authenticate each other. The transaction contains digital signatures that only the holder of the keys for those accounts are able to produce. Any node may verify their authenticity easily, with minimal effort;
- Transactions are broadcasted throughout the network, all miners receive a list of new and pending transactions. Each miner collects its list of transactions into a block. To make a block, a miner has to access the information of the previous chain of transactions of each account in the new transaction, plus the information of the last transaction in the blockchain. Using a digital signature of that information, the miner produces its signatures for a new block;
- Each miner works on finding a *proof-of-work* for the block it created. A *proof-of-work* is a previously unknown unique digital signature that must be applied to that block to make it a permanent part of the ledger, it relies on the digital signature of the last valid block of the network and it is promptly and easily verifiable by anyone in the network. When a miner finds a valid *proof-of-work*, it broadcasts the new block to all nodes;
- As the broadcast of a new block is received, nodes validate the block itself, its *proof-of-work* and make sure that all transactions it contains are not already spent. When valid block is accepted as new part of the blockchain, its transactions are no longer pending, and its digital signature is now elected to mint the next block. This block also contains a custom transaction that carries a pre-determined reward to the miner that minted it;

At times, more than one miner may find a *proof-of-work* and broadcast a valid block simultaneously. When this happens, both blocks are voted and the one which receives the least votes is ignored by the network. Once a block is dropped (i.e. ignored), its transactions are gathered into the next block. Therefore, the blockchain is designed to tolerate divergent copies of itself for short time spans. As nodes are programmed to considerer the largest known copy as the only valid ledger, they always reverts the blockchain back to the decision of the majority.

Thus, the blockchain may be viewed as a secure database of transactions disposed in chains. The information is distributed in a public network of computers, and is fully trusted to be authentic by design.

4. PROPERTIES OF BLOCKCHAINS

The digital ledger contains several mechanisms in order to protect its integrity. Namely, it enforces [12]:

- Distribution: all participants have unlimited access to any part or the whole of the updated ledger. Every copy carries the same properties and may be audited and certified as legitimate by any peer;
- No double spending: each transaction must carry its chain of previous transactions of its accounts. A peer would try to cheat the system by submitting different chains to different miners in the network. Since they would generate different blocks, and only one of those blocks may be voted into the blockchain, one of the chains must be contained in the winning block before the others. Once the first transaction chain is written to the ledger, all other chains are considered invalid and their transactions, purged from the system;
- Non-repudiation: the ledger can be only be added to. Thus, once a transaction is written in a block and that block elected to the blockchain, no peer is able to erase it from the ledger;
- Authenticity: all information is digitally signed using well known, public, pluggable encryption algorithms. Thus every transaction is guaranteed to be legitimate and that is easily verifiable;
- Accountability: peers access their accounts using digital keys only they are aware of. No central authority has any knowledge of which are the valid keys or of whoever holds them. But, although accounts do not hold the identity of their owners, all transactions are public (i.e. every transaction for every single account may be tracked), and the ledger may be audited at any time;

The most prevalent property of blockchains is the lack of a third party in which all peers must trust: since transactions are written by a process of certification and consensus of all participants, the network itself serves as certifying authority. This characteristic, in particular, separates blockchains of all the previous attempts of creating a truly digital currency.

On the other hand, it is important to emphasize that, contrary to popular belief, anonymity is not an inherent property of blockchains [14]. The entries in a ledger carry public account numbers for each party that participated in each transaction. Although the owners of each accounts are not of public knowledge *ex ante*, once one an account holder is identified, it is possible to track all transactions for that individual throughout all history of the blockchain. Every bitcoin transaction, for instance, is readily inspectable by anyone using one of several public sites in the Internet (such as blockchain.info). This technique was used by FBI agents to track down the owner of the illicit drug virtual marketplace *The Silk Road* in 2013 [13].

5. TECHNICAL ISSUES

Blockchain technology may be seen as a protocol: a set of algorithms, rules and communication schemas that, put together, yield the functionality of the digital ledger. When building a blockchain, coders have to decide for two parameters that characterize how the network will operate: the size of blocks and the rate of creation of new blocks. In the case of bitcoin, the chosen parameters created two well known vulnerabilities and one performance issue: opportunities for *double-spending attacks*, opportunities for *history revision attacks* (the so-called “51% attack”), and a low transaction throughput. Although these issues are particular to bitcoin, discussing them briefly will help us to understand the flexibility in the design and the evolution of the blockchain technology.

The cryptographic puzzle chosen as *proof of work* of bitcoin was designed so that miners would take on average ten minutes to mint a new block [19]. A parameter embedded in the mining algorithm, the *difficulty*, is automatically reviewed every time 2016 blocks are added, ensuring that the average time remains constant. This parameter dictates the rate of creation of new blocks of bitcoin. Since transactions are pending until new blocks are written into the blockchain, this implies that peers in this network will wait up to ten minutes to have their transactions made permanent. It has been proposed that an attacker may take advantage of this characteristic by minting a valid block containing a transaction between two accounts he holds himself, then running a new transaction with a merchant using his old balance. Once the merchant deliver the goods, the attacker broadcasts his valid block to the network, overriding the transaction made with the merchant [20]. Albeit theoretically feasible, the difficulty involved in minting a block and making a counterfeit transaction in a ten minutes window makes this attack impracticable.

A more harmful attack was described by Nakamoto himself and is regularly discussed by both bitcoin community and its detractors: the history revision, or 51% attack [12]. As described in the previous section, short lived divergent versions of the blockchain (denominated *forks*) are predicted and tolerated by the protocol as part of a correction mechanism for collisions (the time when two miners succeed in minting a new block simultaneously). *Forks* are eliminated in time as the majority votes up the *official* version of the blockchain. Thereby, by design, if any entity is able to hold more than 50% of the hashing (i.e. mining) power of the network, it would have the number of votes necessary to validate whatever blocks it may wish to promote, thus power to confirm fraudulent transactions. Any legitimate blocks minted by remaining miners would go into *forks* that wouldn't survive the voting mechanism and, in time, purged by the network. Moreover, it has been proved that this scheme is viable by the participation of colluding miners in numbers well below the 50% threshold [17].

Critics also point out that the bitcoin network suffers from a characteristic low throughput. Currently, there is a hard ceiling of 7 transactions per second, a small number compared to the average 2000 transaction per second Visa records in its network. This number is determined by the quantity of transactions a miner is able to store in a single block which, in its turn, derives from the size of each blocks. Nevertheless, according to the bitcoin community, the protocol supports a theoretical ceiling of nearly the same 4000 transactions per second Visa claims to support in its network. This limit is already achievable using the processing power of today's average workstation and consumer grade Internet connection [21].

6. REWARD SYSTEM

Miners in a blockchain enter a race: they perform a series of intensive mathematical operations to solve a cryptographic puzzle (proof of work), authenticate new blocks and obtain rewards for this effort. As discussed previously, this process is continuously calibrated to keep a constant rate of block creation. When the bitcoin network was created, a regular desktop computer had enough processing power to mint a few blocks per day. By then, a miner received 50 bitcoins per minted block. That mining algorithm was built to halve the reward at around every 4 years. Circa 2016 miners get 25 bitcoins per block, by 2017 they will receive 12.5. The system was designed to yield 21 million bitcoins until May 7th, 2140, when the last automatic reward for a block will be added to the ledger. From that point forward, miners will be rewarded per transaction. The blockchain algorithms contain provisions for changing the reward mechanism at any moment [53].

This system created a *gold rush* for bitcoin. Since more processing power yields more blocks, the rising price of bitcoins created incentives for miners adding top notch machines in search of larger rewards. By 2010, a new version of the mining software was developed for specialized hardware and raised the bar for miners: in a short time, it made impossible for ordinary desktop computers to win the race for minting new blocks. To become a miner, users had to invest thousands of dollars (or millions of bitcoins) in new, expensive, powerful computers. By some time in 2012, mining became exclusive to specialized operations: either individual firms that invest heavily in computer farms or groups of individuals that acquire and operate such farms in cooperatives [2].

As competition increases, more and more mining rigs are put to work. Greater processing power comes at the expense of electrical energy. The most prevalent result of this escalation is the rising consumption of energy to mint new blocks. Some estimate that each bitcoin amounts to US$250 in energy bills at current prices. Critics point out that the bitcoin economy is unsustainable due the considerable environment cost [54]. Enthusiast claim the numbers are overestimations, mainly because the calculations are based in consumption profile of older generation mining rigs: the latest equipments are at least four times more energy efficient than the former [55]. Interestingly enough, Nakamoto himself predicted the price of bitcoin would converge to the cost of the energy needed for mining (although we're not there yet).

Fortunately, the problem of excessive energy consumption is particular to bitcoin. Technically, blockchains are viable with much less processing power than currently spent on sustaining that network. This is a straight forward conclusion by analyzing bitcoin itself: before the competition escalated in this *gold rush*, the network was able to carry its functions accordingly with much less processing power than what it uses nowadays. If the escalation hadn't happened, the *difficulty* parameter would be in a much lower level, demanding less operations to solve the proof of work, hence less energy. Some projects of alternate blockchains also stand as evidence: both the reward system and the cryptographic puzzle of blockchains are replaceable, and both may be tailored to make the system as energy efficient as necessary.

7. PATENTS

Bitcoin is on public domain since it was invented, the source code is provided with a MIT license. Open source projects may use one of several types of licenses, each has a different set of rules about derived work. Some of these licenses, for instance, state that any project relying on modification of the original code is bound to the same rules (i.e. that derived work is as public as was the original source). The MIT license is considered the most permissible among all open source licenses: it waives any copyright claims and states that anyone may copy that code and use it for any purpose, commercial or otherwise.

Thus blockchains are not patent eligible, since they are already in public knowledge and wouldn't pass the criteria of novelty. However, innovations built upon bitcoin and blockchains are patentable if they present enough elements to be characterized as novel. This situation is somewhat similar to what happens to the diary industry: although milk itself is not patentable because it is naturally occurring, technologies that produce lactose free milk are subject to patents. [41] A quick search for bitcoin related patents using *Google Patents* in this date (April of 2015) reveals over 500 filed applications, 79 of them already issued. They range from digital wallets (software that allow users to store bitcoin credits offline) to mining rigs (high performance hardware to validate transactions).

Among these patent applications, most of the major bitcoin companies are noticeably absent. Only San Francisco based *Coinbase*, which runs a major bitcoin exchange, has filed for patents. The applications include technologies used by most of the other businesses, such as a patent for bitcoin exchanges (20150262139) and a patent for a secure storage for account keys (20150262141). As they caused immediate unrest throughout the bitcoin community, CEO Brian Armstrong was quick to assert that the applications were filed as a preemptory defense move: the company needs a portfolio to protect itself from patent trolls. To signal its intentions, it joined businesses like AirBnb and Dropbox in a pledge not use patents aggressively against companies with less than 25 employees [44].

IBM, Amazon, Bank of America, Goldman Sachs and JP Morgan are some of the other applicants. IBM filed a patent in 2012 for tacking digital currencies, it describes a system which keeps track of coins that are used for illicit purpose in order to keep them out of official ("good") markets [45]. Amazon was awarded a patent that describes a mechanism to enable users to pay for their cloud services using bitcoin. [46] In 2015, Goldman Sachs filed a patent for a cryptocurrency called SETLcoin, which would be used for settling securities [47]. Bank of America filed for 10 patents that amount to a complete wire transfer system using cryptocurrencies [48]. And JP Morgan Chase was denied a patent for a digital payment system that closely resembles bitcoin. All 174 claims of this application were rejected because of the *On the Sale bar* rule, meaning the invention had been on sale for more than a year prior, therefore it is non-patentable. The general feeling is that JP Morgan's application was rejected because it carries too close resemblance to bitcoin [49].

These applications stirred the bitcoin community, which fears the whole business might be jeopardized by some companies holding key patents. Since bitcoin and blockchains are not eligible, the threat lies in patents for key technologies, including some not directly related to blockchains. For instance, QR Codes are subject to a patent by Denso Wave Inc., granted in 1999. The company chose not to exercise their rights, but it would make payments via QR Codes unviable were Denso Wave to revert that decision [50]. QR Codes are used for most mobile applications to identify transaction accounts, without them the consumer market for *cryptocurrency* would vanish immediately. The same reasoning applies if a single company acquired a patent for digital wallets, for instance, a key technology used by all bitcoin exchanges.

A viable solution is the creation of a coalition to apply for patents of common interest. This device has been used before to protect another famous open source project: the Open Invention Network was founded in 2005 by a group of companies such as IBM, Novell and Red Hat, all holding products on top of the Linux operating system. OIN's mission is to acquire patents related to this technology and license them royalty free to its members which, in turn, agree not to assert their own related patents [51]. In 2007, it helped the defense of Novell and RedHat when Xerox sued both companies for their use of Linux. The prior art search assembled by OIN was considered a key point for the jury to find Xerox's patents invalid. As of today, though, the creation of a similar organization to defend the blockchain technology seems unlikely due to lack of consensus and trust between the main players in the bitcoin market. Furthermore, loath for the patent system is a strong cultural trait of open source communities like bitcoin's, every patent application listed in this section was passionately opposed in Internet forums by a number of those players [52].

8. EVOLUTION

Open source projects like bitcoin allow developers to copy and modify the source code, thus adding new properties, altering original behaviors or fixing problems detected by users (*bug* fixes). By April of 2016, the bitcoin project had 6000 *forks* (as these copies are called). Some of the changes are merged back to the official bitcoin project through a process governed by a small project team. This team is composed of a group of three individuals (as of this same date) in charge of inspecting code contributions, choosing modifications that go into the official code repository and testing if those changes cause any problems [22]. Throughout time, this staff has been composed of employees hired either by the bitcoin Foundation or by firms with special interest in the success of blockchains. Today, the effort is backed by more than 350 volunteer contributors.

However, some coders create *forks* to modify the behavior of the original blockchain and devise new ledgers, significantly different from bitcoin, using different parameters and algorithms in attempt of solving its issues. *Litecoin* is one of such projects: created by a former Google employee in 2011, it uses different encryption algorithms and has a greater rate of creation of new blocks. In the litecoin network, a new block is added to the blockchain every 2.5 minutes, yielding faster transaction confirmation than that of bitcoin. Consequently, litecoin is able to handle a much higher transaction volume [23]. At this date, it holds the second largest market regarding capitalization among the 46 active exchange markets of *cryptocurrencies*. [8] Forks of this type, that originate new currencies, are known as *altcoins*.

Ripple is worth mentioning for its similarities to the blockchain technology. It grew from a payment protocol developed in 2004 with roughly the same objectives of Nakamoto's creation: a decentralized monetary system where transactions are verified by consensus of participants. Although the underlying algorithms and protocols are different, it similarly implements a distributed shared ledger and relies on nodes of its network to digitally sign transactions and update the ledger. The main differences from blockchains is that Ripple creates a chain of trust similar to the ancient *halawa* remittance system [30]: either two users have to direct trust in each other or the system tries to find a path of trust relationships that leads from one to another. Moreover, it is managed by a single company, which keeps to itself the power of coin emission and some control of the accounts in the system [26]. Ripple Labs is a San-Francisco startup funded by Google Ventures in 2013. It targets mainly the bank market, advertising itself as an alternative remittance option with lower fees, and claims to work with 10 of the 50 top banks in the world [24].

Granted both are valuable refinements, these cases are limited to the domain of currencies and financial transactions. Nevertheless, most recent projects using blockchains expand this technology with features that have applications in areas far beyond: *Colored coins* and *Ethereum* are the noteworthy *Blockchain 2.0* projects. Colored coins are sets of extensions over the bitcoin blockchain that modify the transaction structure to include memo fields, which may hold additional information [1]. This data may be used to store assets within transactions, such as digital music or bond certificates. Ethereum, an open source blockchain project built from ground up, just released its first production version in March of 2016 [27]. It differs from colored coins mainly because it does not hold any relationship with bitcoin beyond technological principles. Moreover, it goes much further in extending blockchains: instead of simply holding data, Ethereum transactions are fully programmable. It has attracted the attention of large companies like IBM, Microsoft and Samsung, all of which have active projects and proofs of concept on top of Ethereum powered blockchains [28].

Blockchain 2.0 enables most of the applications presented in the next session.

9. APPLICATIONS

As we have seen, bitcoin was created to be a digital alternative to the traditional exchange of value (fiat currencies and traditional banking), therefore to compete with the established channels for payment systems. Blockchains were purposefully designed to serve as a better medium for transactions than current technology: they aim to be more secure, more convenient and cheaper. Although this is presently the main application for this technology, I leave this topic to the next two sections, comparing blockchains to incumbent payment systems. For the remainder of this section, let's look at some novel applications for this technology circa 2016.

In the wake of payment systems, the next application for blockchains are *digital assets* (also known as *smart properties*). In a sense, bitcoin and altcoins are assets: an account holder owns a balance, which he or she may transfer to another account by trading with others. However, the concept of smart properties move beyond currencies to include other assets, either hard (physical properties) or soft (e.g. intellectual property). For hard assets, the idea is to add digitally signed certificates of ownership to a blockchain, such as real estate or car titles. Thereby, the owner holds a verifiable record in a public registry that may be authenticated at any time by anyone, and sellers may trade assets by moving certificates to buyers within transactions. Reportedly, the Property Institute of Honduras and Fatcom, an american Startup, started building a prototype of a blockchain-based land registry in 2015 to replace the rudimentary system of that country [34]. The project was stalled in December of that same year for reasons unclear.

Meanwhile, soft assets are already being stored in blockchains. Financial assets other than currency (such as bonds and stocks), for instance, may be easily digitized by using blockchains: in July of 2015, Overstock.com, a traditional online retailer, sold a US$5 million bond registered in the bitcoin blockchain to FNY Managed Accounts LLC, a New York based trading firm. Since then Overstock.com has sought the U.S. Exchange and Securities Commission (SEC) for permission to issue securities through that same medium. SEC approval is mandatory for securities other than private bonds, it was granted in December of that same year [39].

Intellectual property may also be registered in blockchains by using services such as *Proof of Existence*, a website that provides means for registering a cryptographic fingerprint of any type of file into the bitcoin ledger. Once registered, the owner of the file is able to prove without any doubt that the file existed at the time it was registered and that it contains the same information from that moment. This service may be viewed conceptually as a digital notary and may be used for copyright registration, since it enables an author to provide a (sort of) notarial confirmation of authorship at a given time [37]. Although it has not yet been tested as legally binding proof of intellectual property, it is hard to envision that any court would deny the merits of this authentication mechanism.

Similar devices enabled more innovative types of soft assets, like digital art. For instance, a startup based in Madison-WI, *23VIVI*, uses a blockchain to trade digital artwork: collectors acquire images (or animations) from the website, download a special version of the purchased artwork (high definition files without watermark) and receive the keys for a certificate of authenticity registered in a blockchain. Through technology, 23VIVI's creators were able to give digital art the quality of scarcity: each piece has a version number, incremented at each sale. Once a piece is sold 23 times, it may be bough exclusively through a resale market. Hence, otherwise non-excludable goods (digital files) are made excludable.

Smart contracts are another application for blockchains, enabled by features provided in projects such as Ethereum. They mitigate asymmetric information and reduce costs of intermediation by design [31]. A smart contracts is a self-enforced agreement between two parties. It runs in a ledger with no manual intervention, thus removing the need of trust among those actors. It is both defined and executed by code written specifically for the agreement. It is autonomous, meaning once initiated, the agents involved in the contract need not and cannot make any intervention; it is self-sufficient, for it is capable of acquiring and spending resources on its own to achieve its goals; it also is decentralized, since it exists in a decentralized space by principle, a blockchain. Moreover, a smart contract is *technically binding*, while classical contracts are *legally binding*: code is not subject to whims, unable to deny executing its instructions as programmed, and can't be forced to perform otherwise by anyone [1].

A clear case for smart contracts are loans backed by collateral. In this example, a lending transaction would contain assets given as collateral (for instance, a digital, transferable title for a property) and embedded code would be capable of enforcing the agreement. A program would monitor payments from borrower to lender and, in case of default within conditions specified in its instructions, transfer immediately collaterals to lenders without any human intervention. A second application for smart contracts are for enforcing *last wills*: a digital will would be uploaded to a blockchain, wait for the time of its fulfillment and execute itself. It would be able to look up obituaries and registries, acquire knowledge of the demise of its author and bestow the inheritance upon heirs as determined. The *digital will* would also be able function as a trust fund: it may automatically move assets between investments to preserve its value while not fulfilled, and wait for a due date to transfer those assets to rightful owners (e.g. to heirs that become of age) [1].

The concept of such institution is tied to that of *Distributed Autonomous Organizations* (DAOs). Both smart contracts and DAOs are not fully leverageable yet: legal consequences of digital institutions enforcing human agreements are unclear at this date, mainly because those automata would control assets but would not hold any themselves that could be used as reparation for disputes in courts, hence they are not liable before the law [32]. Wether the deterministic and definitive characteristics of the execution of smart contracts may be good or bad for society is yet to be decided, though it is certain that its adoption will require heavy accommodation [1]. Regardless, several companies currently develop products related to smart contracts: IBM is known to be experimenting this concept in its blockchain trials [33], and startups like Hedgy Inc. and RSK Labs recently raised more than US$1Mi each in venture funds to develop their smart contract platforms.

The most innovative application for blockchains might be *electronic voting*: anonymous, fraud free, resilient elections of all kinds. In a simplified scheme, voters would receive *cryptocurrency* from a central authority (the federal government, for instance) and transfer those coins to the account of his or her inclination at the time of election. Each votable option would have a unique account: an account for every running candidate or, in a referendum, an account for a “yes” and another for a “no” vote. At the end of election, a winner is determined by looking at the balance of each account. The cryptographic features of blockchains prevent votes (transactions) from being tempered by interested parties or attackers, and each individual voter can easily audit that his or her vote was cast as intended by simply checking the blockchain. Several companies and non-profit organizations have ongoing projects in this area, such as the *V initiave*, *BitCongress* and *Liquid Feedback*. Although it needs major law reviews to become mainstream, some have already tried this type of voting successfully in countries like Denmark and Spain. [40]

At this point, the bitcoin ledger is the only active blockchain hosting live applications. However, most of the applications discussed here will run in alternate blockchains, for which parameters may be chosen accordingly (for instance, in order to keep low energy costs). There are two distinct cases for new blockchains: public blockchains, such as bitcoin and altcoins; or private (permissioned) blockchains, ran by individual companies or pools of companies, such as those tried by Bank of America or IBM. For most private blockchains, the default reward scheme will certainly be replaced for charging fees directly over transactions. In some cases, such as for electronic voting, electronic ledger networks are likely to be composed exclusively by trusted nodes of a public institution (e.g. computers belonging to a federal government), where there will be no use for a reward system.

10. PAYMENT SYSTEMS

Traditional non-cash payment systems use a central ledger, operated by a central authority, usually a Central Bank. Large institutions hold accounts in this central ledger. These institutions, in turn, maintain their own ledger to register accounts for its clients. A larger institution may hold smaller institutions as clients. At some level, institutions have consumers as clients. This hierarchical construct is denominated a *tiered payment system*. Blockchains payment systems are flat, all participants are connected to a single network and there is no hierarchical relationship between them. These systems have two major advantages compared to tiered systems: immediacy and decentralization.

Blockchains are capable of registering and broadcasting transactions in nearly real-time, twenty-four hours a day, seven days a week; whereas tiered systems gather transactions in the central ledger and periodically perform account procedures to settle transactions, subject to inherent delays. For instance: in the US, transactions in the ACH system take from 24 hours up to 60 days to reach its destiny; the usual credit card transactions take 2 days to settle (although merchants may, under certain conditions, get next day funding); some state-of-the-art systems throughout the world settle transactions as fast as in a few minutes (e.g. banking system in the UK). In all these cases, transactions are processed only during business days. The actual gains of an instantaneous payment system are uncertain at this point [63]. Regardless, the European Central Bank (ECB) is currently promoting the construction of a pan-European instant payment system for trials [61].

Centralized, tiered payment systems carry three major risks with them: credit risk, that a bank may become insolvent and default; liquidity risk, that a bank may be solvent but still not have funds to settle its payment at a given time; and operational risk, that infrastructure may fail and operations cease temporarily or permanently. The two former risks make necessary that participants in the payment system contribute up front for hedging them. For larger systems, this contribution is substantial and creates an entry barrier that hinders competition. The resulting equilibrium implies excessive transaction fees. [60]

These risks don’t apply to blockchains, mainly because of its decentralized nature: since there is no delayed procedure for settlement (balances are adjusted as transactions are registered), there is no way for participants to become insolvent, either temporarily of permanently; and since there is no single point of failure, a blockchain infrastructure is much more resilient than those with a centralized model. In fact, the blockchain network design is similar to that of the Internet itself. One of the main characteristics of this type of architecture is that it continues to operate even if most of its nodes are taken offline.

As risks are eliminated and their costs are purged from the fee structure, one may expect transaction costs of a blockchain payment system to be less than that of a traditional tiered systems. Although a broader investigation is needed, there is a general perception that blockchains might be more cost-effective than tiered payment systems. Currently, the R3 consortium is actively running trials in search for a definitive answer. This group is composed by major banks such as Bank of America, BBVA and HSBC, and tech giants such as Microsoft and IBM. [64]

11. PAYMENT SYSTEMS (CONSUMER MARKET)

In this section, bitcoin is uses as a reference point to briefly compare blockchains to payment systems in the consumer market, since it holds a somewhat developed market of its own.

When two agents (a payer and a payee) perform a transaction, two entries (a debit transaction for the payer, a credit transaction for the payee) are registered by their institutions and transmitted throughout the upper tiers until they reach the top level (the central ledger). These transactions are settled in a clearing house, where the actual values are exchanged by the institutions. In general, the Automated Clearing House (ACH), credit card, debit card, and most national payment systems follow this model.

Credit card payments of a network like Visa and Mastercard, for instance, happen in this sequence: a consumer swipes his card in a point of sale at the merchant’s store; a debit transaction is registered by the cardholder’s bank (issuer bank); a credit transaction is registered by the merchant’s bank (acquiring bank); at a given time, all transactions (consumers’ and merchants’) go into the settlement pool and banks have their balances adjusted accordingly; only then the consumer is charged and the merchant receives his due. The latter is charged a fee at the moment of settlement, which is shared among both banks and the associated network in proportions previously agreed. For credit cards, specifically, Schul et al demonstrate that fees ultimately fall on consumers and their aggregate value is subsidized by those who use cash. They conclude that credit card transaction fees have a considerable negative effect on consumer welfare [56].

Bitcoin transactions are much simpler: a consumer receives an account address for the merchant (by reading a QR Code, for instance), and transfers a value using a program, possibly in a smartphone. The *app* creates and digitally signs a transaction and broadcasts it the network, where it is validated by miners. There is no need for settlements, since transactions are immediately registered in the blockchain. And, specially considering identity thefts, this process is vastly more secure than credit card transactions, inasmuch as no information of any party is exposed. Consumers also receive a cost advantage due to the systematic cross-subsidization of the reward system. These are actually the main claim of bitcoin activists: transactions are more secure, and they carry near null cost, whereas credit card networks usually charge 2% to 3% of the transaction value.

Matters are not so simple at this point in time, though. Consumers and merchants have to interface the “real” economy and the bitcoin economy. People receive US$ salaries, merchants pay suppliers in US$. Bitcoin exchanges charge from as low as 0.2% up to 3% to convert dollars to credits in the ledger, depending on volume and payment method, since they are themselves subject to the customary fees to transfer money from bank accounts or to process credit cards. Services like Bitpay and Coinbase charge 1% per transaction to convert bitcoins spent by customers immediately to dollars in the merchant’s account. These services help the latter to deal with the exchange rate volatility, since they don’t have to hold bitcoins themselves. Summing it up, it is reasonable to conclude that bitcoin transaction fees are at best similar to those of credit cards in aggregate for the moment being. It certainly is more expensive than debit cards, which reportedly charged an average flat rate of US$ 0.31 per transaction in 2014 [59].

Furthermore, considering total welfare, the cost of bitcoin is likely to be too high. Beer and Weber claim that too many resources are wasted by the race to mint new blocks, since various competitors are trying to solve the same problem. In their opinion, the end result is that the marginal cost of transactions in this network is probably higher than that of centralized systems [57]. Plausibly, their statement is precise due to the “gold rush” of bitcoin, though they don’t present numbers to subsidize these claims. Nevertheless, as seen previously, this is a particular problem of the bitcoin ledger, not of blockchains in general.

Lastly, whereas bitcoin concerns with transactions only, most of traditional payment systems provide additional services. Banks usually offer services like fraud protection, chargeback facilities and proof of payment to their cardholders. For bitcoin, those are unbundled services provided by third party at a cost. And storing bitcoins is similar to storing cash: users must take security measures to keep private keys safe, or keep wallets in services providers. In any case, once security is violated or a service provider is hacked, losses are irreversible. Once a value is transferred to another wallet, it is definitive: there is no mechanism to dispute or reverse a purchase if a consumer is unsatisfied. [57] Therefore, users are subject to greater risk by holding bitcoins than bank accounts.

Overall, facts presented in this section hint that, currently, the maturity of blockchains (or at least that of bitcoin) is unfit for this technology to challenge incumbent payment systems in the consumer market. It presents itself, however, as a good choice for replacing the underlying tiered infrastructure of credit card networks for reasons exposed in the previous section [62].

12. CONCLUSION

Blockchain is a revolutionary technology, with great potential to change society by getting rid of the need for trusting third parties in several types of exchanges, may it be for financial intermediation, for agreements between two individuals or even for replacing anachronistic institutions, such as public notaries. Furthermore, it is capable of strengthening security for these transactions and empowering governments and individuals at the same time, giving the former means to easily overview transactions, and the latter, a higher degree of privacy.

It is based on well known technological principles, such as internet communication protocols and asymmetric cryptography, and it is test proven by the millions of transactions registered in the cryptocurrency markets. Albeit its considerable success in this niche, adopters are still in the process of tweaking it to find the best format for each application.

As time advances, private and public institutions are just discovering that it may be used to solve a wide range of problems. A new blockchain related headline appears in major news outlets virtually every day. As companies and governments have just begun to assess its potential, the next few years will certainly bring major developments and the creation of countrywide blockchains throughout the world.

13. REFERENCES

[1] Swan, Melanie. 2015. Blockchain: Blueprint for a New Economy. O’Reilly Media, Inc.

[2] Vigna, Paul. & Casey, Michael J. 2015. The Age of Cryptocurrency: How Bitcoin and DigMoney Are Challenging the Global Economic Order. St. Martin’s Press.

[3] https://en.wikipedia.org/wiki/Cryptocurrency

[4] http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

[5] S., L. (2 November 2015). “Who is Satoshi Nakamoto?”. The Economist explains Economist).

[6] http://www.bitcoin.org/bitcoin.pdf

[7] https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

[8] http://www.cryptocoincharts.info/coins/info

[9] Chaum, David. 1982. Blind signatures for untraceable payments". Department of Computer ScieUniversity of California, Santa Barbra, CA.

[10] Patent US5671279 A. Electronic commerce using a secure courier system

[11] http://historyofbitcoin.org

[12] Barber, Simon et al. 2012. Bitter to Better — How to Make Bitcoin a Better Currency.

[13] Bitcoin fallacy led to Silk Road founder’s conviction. http://money.cnn.com/2015/0technology/security/bitcoin-silk-road/index.html

[14] Reid, Fergal; & Harrigan, Martin. 2012. An analysis of anonymity in the bitcoin system.

[15] Okamoto, Tatsuaki. 1995. An efficient divisible electronic cash scheme.

[16] Sompolinsky, Yonatan; & Zohar, Aviv. 2013. Accelerating Bitcoin’s TransacProcessing: Fast Money Grows on Trees, Not Chains

[17] Eyal, Ittay; & Sirer, Emin Gün. 2014. Majority is not Enough: Bitcoin Mining is Vulnerable

[18] http://www.newsbtc.com/2015/12/18/bitcoin-to-overtake-paypal-and-established-financompanies-in-transaction-volumes

[19] https://en.bitcoin.it/wiki/Difficulty

[20] https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384

[21] https://en.bitcoin.it/wiki/Scalability

[22] http://motherboard.vice.com/blog/whos-building-bitcoin-an-inside-look-at-bitcoins-open-sodevelopment

[23] https://litecoin.org

[24] https://ripple.com

[25] https://ethereum.org

[26] http://bitcoinist.net/not-decentralized-ripple-freezes–1m-user-funds/

[27] http://www.coindesk.com/ethereum-blockchain-homestead/

[28] http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enatransactions-that-rival-bitcoins.html?_r=1

[29] http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/

[30] https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.cite>

[31] http://firstmonday.org/ojs/index.php/fm/article/view/548/469

[32] http://www.coindesk.com/how-to-sue-a-decentralized-autonomous-organization/

[33] http://www.wsj.com/articles/ibm-adapts-bitcoin-technology-for-smart-contracts�

[34] http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-whnot-know-or-trust-each-other-build-dependable

[35] https://23vivi.com/about.html

[36] http://swancoin.tumblr.com

[37] https://proofofexistence.com/about

[38] http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchacite>

[39] http://globenewswire.com/news-release/2015/07/31/756843/10144107/en/Overstock-com-and-FNY-CapConclude–5-Million-Cryptobond-Deal.html

[40] http://motherboard.vice.com/read/bitcoin-could-change-voting-the-way-its-changed-money

[41] http://reedjessen.com/bitcoin-suppression-via-the-patent-system/

[42] https://github.com/ethereum/wiki/wiki/Licensing

[43] https://github.com/ripple/rippled/blob/develop/LICENSE

[44] http://motherboard.vice.com/read/are-the-bitcoin-patent-wars-about-to-begin

[45] http://www.coindesk.com/ibm-files-patent-track-value-digital-currencies/

[46] http://www.coindesk.com/amazon-awarded-bitcoin-related-cloud-computing-patent/

[47] https://bitcoinmagazine.com/articles/goldman-sachs-files-patent-application-for-securisettlement-using-cryptocurrencies–1449000967

[48] https://www.cryptocoinsnews.com/bank-of-america–20-more-cryptocurrency-blockchain-patencite>

[49] http://www.m-cam.com/sites/www.m-cam.com/files/JP-MorganMonopolyMoney.pdf

[50] http://www.qrcode.com/en/patent.html

[51] http://www.openinventionnetwork.com

[52] https://www.reddit.com/r/Bitcoin/comments/3lxbp0/coin-base_files_9_patents_for_bitcoin_products/

[53] https://en.bitcoin.it/wiki/Controlled_supply

[54] http://www.abc.net.au/news/2015–10–06/quiggin-bitcoins-are-a-waste-of-energy/68

[55] http://kernelmag.dailydot.com/issue-sections/staff-editorials/11336/how-much-electricity-bituse/

[56] Schuh, Scott; Shy, Oz; & Stavins, Joanna . 2010. Who Gains and Who Loses from Credit Card PaymeTheory and Calibrations.

[57] Beer, Christian; & Beat, Weber. 2015. Bitcoin – The Promise and Limits of Private InnovatioMonetary and Payment Systems. Monetary Policy and the Economy. Q4/2014, 53–66.

[58] https://www.cryptocoinsnews.com/what-bitcoin-exchanges-wont-tell-you-about-fees/

[59] https://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm

[60] Ali, Robleh; Barrdear, John;Clews, Roger; & Southgate, James. 2014. Innovations in paytechnologies and the emergence of digital currencies. Bank of England Quarterly Bulletin 2014 Q3.

[61] Mai, Heike. 2015. Instant revolution of payments? The quest for real-time payments. Deuche Bank Rese

[62] http://www.coindesk.com/visa-ad-developer-secure-scalable-blockchain/

[63] Greene, Claire; Rysman, Marc; Schuh, Scott; & Shy, Oz. Costs and Benefits of Building Faster PaySystems: The U.K. Experience and Implications for the United States. Current Policy Perspectives, Federal Reserve Bak of Boston.

[64] http://www.forbes.com/sites/laurashin/2016/03/03/bitcoin-technology-tested-in-trial-by–40-big-bacite>