Zeszyty Naukowe
Wydziału Zamiejscowego w Chorzowie
Wyższej Szkoły Bankowej w Poznaniu
Nr 18 2016 r.

Paweł Szewczyk

Wyższa Szkoła Bankowa w Poznaniu
Wydział Zamiejscowy w Chorzowie
e-mail: pszewczyk@chorzow.wsb.pl
tel. 32 227 01 07

The Potential Impact of the Blockchain Technology on the Financial Sector

Summary. The Internet itself can serve as a perfect example of a complex decentralized artifact that emerged spontaneously and continues to evolve without intervention from an overarching authority or central designer. In August 2008, an anonymous user registered the domain of bitcoin.org. At the same time, an article was published, signed by Satoshi Nakamoto, pioneering an idea of direct peer-to-peer money transactions using a currency called Bitcoin and based on a technology termed as blockchain. The system was launched with the usual framework of coins made from digital signatures that provides strong control of ownership but is incomplete without a way to prevent double-spending. To solve this, a peer-to-peer network was proposed using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of central processing units power. Nodes work all at once with little coordination, they do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. The paper tries to predict how the network can, using the Bitcoin and blockchain technologies, reshape financial services.

Keywords: cryptocurrency, Bitcoin, blockchain, peer-to-peer transactions

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads.

Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.

Based on the newest and rapidly growing literature, in this paper a review of consecutive development steps of the ideas of the Bitcoin and blockchain technologies are presented and, especially, their impact on the financial sector are discussed.

2. Continuity in technology's evolution

The first four decades of the Internet brought e-mail, the World Wide Web, dot – coms, social media, the mobile Web, big data, cloud computing, and the early days of the Internet of Things [Tapscott, Tapscott 2016: 3]. It has lowered the barriers to entry for new media and entertainment, new forms of retailing and organizing work, and unprecedented digital ventures. Through sensor technology, it has infused intelligence into our wallets, our clothing, our automobiles, our buildings, our cities, and even our biology. In this digital age, technology is at the heart of just about of everything – good and bad [Tapscott, Tapscott 2016: 4].

Table 1. Phases of the Web's evolution

Phase	Goal	Disrupting	Outcome
Communications	Reach anyone in the world	Post office	Personal communications
Publishing	Spread ideas	Print media	Self-publishing
Commerce	Trade	Supply chains and physical stores	E-Commerce
Social interactions	Connect with friends	Real world	Social Web
Asset Transactions	Manage what you own	Existing custodians	Trust-based Services

Source: W. Mougayar [2016: 17].

The Bitcoin and blockchain technologies are a new phase, focused on peer--to-peer, trust based asset transactions. The key previous mini-revolutions that the Internet has brought since 1994 were:

– Personal Communications,
– Self-Publishing,
– E-Commerce, and the
– Social Web.

Each of these four phases disrupted the post office, print media, supply chains/physical stores, and the real world [Mougayar 2016: 16-17]. On the other hand, the blockchain – based applications can replace any Web application. All of them will be threatened by new versions that rest on peer-to-peer protocols that are anchored by blockchain technologies (see Tab. 1).

3. The Bitcoin technology

In August 2008, Satoshi Nakamoto published the paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" [Nakamoto 2008] in which a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions was proposed. An outline of a new protocol for a peer-to-peer electronic cash system using a cryptocurrency called bitcoin was presented.

This protocol established a set of rules – in the form of distributed computations – that ensured the integrity of the data exchanged among numerous devices without going through a trusted third party. Cryptocurrencies (digital currencies) are different from traditional fiat currencies because they are not created or controlled by countries [Tapscott, Tapscott 2016: 5].

The following are the foundational principles of Bitcoin [Mougayar 2016: 2-4]:

– A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

– A trusted third party is not required to prevent double spending.

– It is proposed that a solution to the double spending problem consists on using a peer-to-peer network.

– The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of central processing units (CPU) power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they will generate the longest chain and outpace attackers.

The network itself requires minimal structure. Messages are broadcast on a best-effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin was introduced on 31 October 2008 to a cryptography mailing list, and released as open-source software in 2009 [Bitcoin 2016]. Transactions in the system take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain, which uses bitcoin as its unit of account. Since the system works without a central repository or single administrator, bitcoin is categorized as a decentralized virtual currency.

Bitcoins are created as a reward in a competition in which users offer their computing power to verify and record bitcoin transactions into the blockchain. This activity is referred to as mining and successful miners are rewarded with transaction fees and newly created bitcoins. Besides being obtained by mining, bitcoins can be exchanged for other currencies, products, and services. When sending bitcoins, users can pay an optional transaction fee to the miners. This may expedite the transaction being confirmed.

4. The blockchain as the new database

The technology concept behind the blockchain is similar to that of a database, except that the way one interacts with that database is different. For developers, the blockchain concept represents a paradigm shift in how software engineers will write software applications in the future, and it is one of the key concepts that needs to be well understood. One needs to really understand five key concepts, and how they interrelate to one another in the context of this new computing paradigm [Mougayar 2015]:

– the blockchain,
– decentralized consensus,
– trusted computing,
– smart contracts, and
– proof of work/stake.

This computing paradigm is important because it is a catalyst for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs. Decentralized applications are going to enable a decentralization trend at the societal, legal, governance, and business levels.

4.1. Blockchain: The new innovation for financial services

Blockchain technology basically allows everyone to hold and make transactions as strangers but in a completely transparent manner. There is no mediator in between two people making the transaction, and the entire process becomes easier and cheaper. This concept can be applied to the entire digital world making any kind of exchange/transactions secure (and not just bitcoin). The blockchain network consists of nodes, i.e., distributed servers. All the nodes can accept and process the transaction. The nodes on the network share information about the candidate transaction. As much as the logic/tech part of it sounds confusing, the business models are so much easier to understand and are really impressive [Know More... 2016].

The network of computers around the world running bitcoin software will take care of the performance and maintenance of the blockchain network. About six times per hour, a new group of accepted transactions (a block) is created, added to the blockchain and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent.

4.2. Design of the blockchain (distributed ledger)

There are various approaches to blockchains (distributed ledgers), each with advantages and disadvantages [Buterin 2015]:

Fully public systems. These are decentralized ledgers open to all Internet users. Anyone can read, submit transactions, and participate in the verification and validation of transactions. The blockchains in these systems are secured by a combination of economic incentives and cryptographic verification, using mechanisms such as proof of work or proof of stake. Participants are typically known only by pseudonyms; and the issuance of an embedded currency provides incentives for participants to verify transactions and maintain the blockchain. Examples include, Bitcoin, Ethereum, and other cryptocurrencies.

Fully private systems. Permissions in these systems are assigned by a central entity. Applications include database management and auditing internal to a single company. A private system does not need an embedded currency given that the central entity can assign computers to verify transactions.

Hybrid or consortium systems. Here, the consensus validation process is controlled by pre-selected individuals or organizations, such as a consortium of financial institutions, or the customers of a company. The right to read the associated blockchain may be public or restricted to the participants. These systems are considered partially decentralized. The identity of users can be required to conform to know your business (KYB) or know your customer (KYC) procedures.

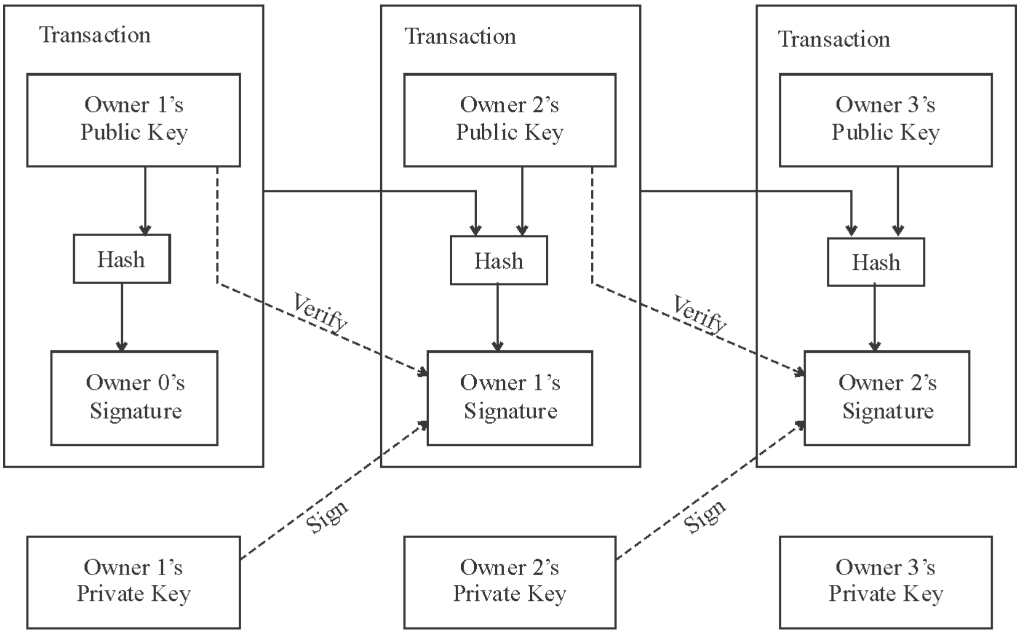
Whether these systems need an embedded currency to provide incentives would depend on the degree of trust, which in turn would depend on the degree of decentralization.

5. Bitcoin transactions

A bitcoin is defined by a sequence of digitally signed transactions that began with the bitcoin's creation as a block reward. The owner of a bitcoin transfers it by digitally signing it over to the next owner using a bitcoin transaction, much like endorsing a traditional bank check. A payee can examine each previous transaction to verify the chain of ownership. Unlike traditional check endorsements, bitcoin transactions are irreversible [Bitcoin Network].

In its most basic form, the blockchain records ownership of bitcoin and transactions involving the cryptocurrency across a wide network of computers, as opposed to a centralized ledger. Transactions are signed off by the parties involved using the software, checked by the network or the "crowd", then added to the blockchain – a long string of code that records all activity. Encryption in the software ensure these "blocks" can't be tampered with or altered. And the decentralized nature means the "crowd" police the whole system [Williams-Grut 2016].

Figure 1. Bitcoin Transactions and Block System



Source: A. Dave [2016].

The payment process from peer-to-peer may be described as follows [He D. et al. 2016] (cf. Fig. 1):

– Copies of transaction records (ledgers) are kept in multiple computers in the network and visible to anyone.

– The transaction is settled by a multitude of individual nodes (miners), providing computing resources to the network.

– Miners solve a cryptographic puzzle as part of validation process. Miners need to show proof of doing this work to the network (called a “proof-of-work” system), which is costly (computing and energy resources).

– Only the miner who finds the solution faster than any others receives newly minted bitcoins as reward for their service.

– “Trust” is created by making tampering attempts prohibitively expensive. If a miner wants to record a false transaction, she needs to compete against other miners who are acting honestly (or trying to fake a different transaction).

6. How blockchain can reshape financial services

On August 11, 2016, the World Economic Forum (WEF) released a 130-page report entitled “The Future of Financial Infrastructure: An Ambitious Look at how Blockchain Can Reshape Financial Services” exploring how the financial sector “could overcome current-state pain points through distributed ledger technology (DLT)” [The Future... 2016].

It took a year for the World Economic Forum (WEF) to research how blockchain technology could help nine financial sectors, which included global payment and foreign trading. More than 200 innovators, subject matter experts and executives from prominent institutions, such as JPMorgan Chase, Visa and MasterCard, contributed their opinions. The results was assembled in this latest report. The most significant conclusions are cited below:

1. Blockchain helps by being transparent and effective: “Distributed ledger technology (blockchain) has the potential to drive simplicity and efficiency by establishing new financial services infrastructure and processes” [The Future... 2016: 19].

2. Blockchain merges with other transformative technologies: “Distributed ledger technology will form the foundation of next generation financial services infrastructure in conjunction with other existing and emerging technologies” [The Future... 2016: 20].

3. Blockchain is revolutionary: “Similar to technological advances in the past, new financial services infrastructure will transform and question traditional orthodoxies in today’s business models” [The Future... 2016: 24].

4. Blockchain needs collaboration to succeed: "The most impactful distributed ledger technology applications will require deep collaboration between incumbents, innovators and regulators, adding complexity and delaying implementation" [The Future... 2016: 23].

6.1. Looking ahead

To date, more than 24 countries and 90 corporations use blockchain technology with many more expressing interest. The WEF notes that large banks around the world, including more than 90 central banks, have developed blockchain groups that hail its potential impact and study how to harness its technology. In fact, the report predicted that a full 80% of these banks could launch their own blockchains by 2017. Blockchain technology has "captured the imagination and wallets of the financial services ecosystem" but the WEF concluded that DLT has to resolve critical issues moving forward. These include [Zitter 2016]:

– how to develop a roadmap to achieve market collaboration and standardized regulation,

– how to structure a regulated tax framework and how to implement a cost-benefit analysis to determine the financial viability of distributed ledger technology."

According to William Mougayar [Mougayar 2016: 98-99], "from an internal implementation point of view, the blockchain's evolution in Financial Services will happen according to a progressive segmentation of major applications areas:

– Consumer facing products,

– B2B services,

– Trading and capital markets,

– Back-end processes,

– Inter-industry intermediary services".

7. Conclusions

In recent years, the term "Bitcoin" has entered the popular lexicon. It is considered a currency, a cryptocurrency, an alternative currency, and even a social movement [Talwar, Wittington 2015: 295]. The underlying technology known as the "blockchain", has the potential to disrupt the middlemen, authorities, owners, and arbiters of judgment (bankers, judges, attorneys) who make the business and economic world tick. This computing paradigm is important because it is a catalyst for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs. Decentralized applications are going to enable a decentralization trend at the societal, legal, governance, and business levels. And, first of all, it seems inevitable that the financial services sector will need to stall new regulation while simultaneously updating the existing regulation to accommodate the innovation introduced by the blockchain.

The potential impact on the financial services of the blockchain technology could be summarized in the following way:

1. A computer application, which creates some useful result for its users, can be run simultaneously on many computers around the world rather than on just one central server, and that the network of computers can work together to run the application in a way that avoids trusting the honesty or integrity of any one computer or its administrators.

2. There are three core innovations that underlie Bitcoin: peer-to-peer networking, blockchains, and consensus mechanisms.

3. Peer-to-peer networking is generally nothing new, and blockchains are merely novel ways of storing and validating data.

4. By consensus one simply means the process by which a number of computers come to agree on some shared set of data and continually record valid changes to that data.

5. The benefits of this technology are real since electronic cash promises efficient microtransactions, and enhanced financial inclusion, and finally

6. Robust digital identity may solve many of the online security problems.

Literature

Bitcoin [hasło], https://en.wikipedia.org /wiki/Bitcoin [access: 12.11.2016].

Bitcoin Network [hasło], https://en.wikipedia.org/wiki/Bitcoin_network [access: 12.11.2016].

Buterin V., 2015, *On Public and Private Blockchains*, https://blog.ethereum.org [access: 7.08. 2015].

Dave A., 2016, *How Bitcoin Works: Motivation and Design, Bitcoins*, https://thefutureofbitcoins. wordpress.com/how-does-bitcoin-work [access: 17.12.2016].

He D. et al., 2016, *Virtual Currencies and Beyond: Initial Consideration*, International Monetary Fund, SDN/16/03, www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [access: 9.11.2016].

Know More about Blockchain, 2016, *Let's Talk Payments LLC*, https://letstalkpayments.com [access: 24.07.2016].

Mougayar W., 2015, *Understanding the Blockchain*, O'Reilly Media, January 16, www.oreilly. com [access: 20.10.2016].

Mougayar W., 2016, *The Business Blockchain*, Hoboken, New Jersey: John Wiley & Sons.

Nakamoto S., 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org/en/bitcoin--paper [access: 5.07.2016].

Talwar R., Wittington A., 2015, The Decentralization of Everything? Exploring the Business of Blockchain, in: R. Talwar ed., *The Future of Business*, London: Fast Future Publishing.

Tapscott D., Tapscott A., 2016, *Blockchain Revolution*, London: Portfolio/Penguin Random House.

The Future of Financial Infrastructure. An Ambitious Look at How Blockchain Can Shape Financial Services 2016, *World Economic Forum*, August 2016, www.weforum.org [access: 16.08.2016].

Williams-Grut O., 2016, *Goldman Sachs. The Blockchain Can Change... Well Everything*, www.businessinsider.com/category/goldman-sachs [access: 4.11.2016].

Zitter L., 2016, World Economic Forum Examines How Blockchain Can Reshape Financial Services, *Bitcoin Magazine*, August 16, https://bitcoinmagazine.com [access: 16.08.2016].

Potencjalny wpływ technologii *blockchain* (łańcuch bloków) na sektor finansowy

Streszczenie. Internet jest przykładem zjawiska o ewolucyjnym charakterze, o złożoności i uporządkowaniu tworzonych spontanicznie, w sposób zdecentralizowany i bez udziału projektanta. W sierpniu 2008 r. w Internecie została anonimowo zarejestrowana nowa domena: bitcoin.org oraz ukazała się publikacja autorstwa Satoshi Nakamoto prezentująca ideę elektronicznych transakcji pieniężnych bezpośrednio między stronami o nazwie bitcoin i opierająca się na technologii *blockchain*. Na podstawie najnowszych publikacji światowych w pracy omówiony został dotychczasowy rozwój tej idei w praktyce, w szczególności w odniesieniu do sektora finansowego.

Słowa kluczowe: kryptowaluta, bitcoin, *blockchain* (łańcuch bloków), transakcje strona ze stroną