Further applications of the blockchain

Conference Paper · May 2015

CITATIONS
3

READS
10,380

2 authors:

Anna Lali Tsilidou
University of Macedonia
2 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Georgios Foroglou
University of Macedonia
4 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Further applications of the blockchain

George Foroglou
University of Macedonia, Finance and Accounting
georgios.e.foroglou@gmail.com | +30 699 416 7076

Anna-Lali Tsilidou
University of Macedonia, Finance and Accounting
anna.e.tsilidou@gmail.com | +30 698 872 9772

…

Abstract

In this research we investigate into the blockchain technology; its current use and explore other possible implementations of this protocol. In the first part a thorough explanation of the technology and the problems it is trying to tackle is attempted. At the same time a background on Bitcoin (the first application of the technology) is provided. In the second part it is examined whether the technology could be leveraged to solve problems in different fields, while some specific recommendations for the Greek economy are also made.

[Bitcoin, Blockchain, Applications]

1. Bitcoin and the blockchain technology

The first application of the blockchain technology was Bitcoin, a digital currency which was based on a protocol that allows the users of the network to perform transactions with virtual money that exist only in their computers in a fast, and secure way. A blockchain is a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. A block is the 'current' part of a blockchain which records some or all of the recent transactions, and once completed goes into the blockchain as permanent database. Each time a block gets completed, a new block is generated. There is a countless number of such blocks in the blockchain. The blocks are linked to each other (like a chain) in proper linear, chronological order with every block containing a hash of the previous block. The blockchain is seen as the main technological innovation of Bitcoin, since it stands as proof of all the transactions on the network. Each node (computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the Bitcoin network. The blockchain has complete information about the addresses and their balances right from the genesis block to the most recently completed block. To use conventional banking as an analogy, the blockchain is like a full history of banking transactions. Bitcoin transactions are entered chronologically in a blockchain just the way bank transactions are. Blocks, meanwhile, are like individual bank statements. Blockchain is kept up to date with the help of cryptography and copious computing power, provided by a global network of tens of thousands of computers. Openness helps the system remain secure: the blockchain is public so every participant can check whether a transfer comes from the rightful owner.

1.1. Blocks

Blocks are found in the Bitcoin block chain. Blocks connect all transactions together. Transactions are combined into single blocks and are verified every ten minutes through mining. Each subsequent block strengthens the verification of the previous blocks, making it impossible to double spend Bitcoin transactions (see double spend below). Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block. Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known. Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. These properties are what make double spending of Bitcoins very difficult. Honest generators only build onto a block (by referencing it in blocks they create) if it is the latest block in the longest valid chain. "Length" is calculated as total combined difficulty of that chain, not number of blocks, though this distinction is only important in the context of a few potential attacks. A chain is valid if all of the blocks and transactions within it are valid, and only if it starts with the genesis block. For any block on the chain, there is only one path to the genesis block. Coming from the genesis block, however, there can be forks. One-block forks are created from time to time when two blocks are created just a few seconds apart. When that happens, generating nodes build onto whichever one of the blocks they received first. Whichever block ends up being included in the next block becomes part of the main chain because that chain is longer. More serious forks have occurred after fixing bugs that required backward-incompatible changes. Blocks in shorter chains (or invalid chains) are not used for anything. When the Bitcoin client switches to another, longer chain, all valid transactions of the blocks inside the shorter chain are re-added to the pool of queued transactions and will be included in another block. The reward for the blocks on the shorter chain will not be present in the longest chain, so they will be practically lost, which is why a network-enforced 100-block maturation time for generations exists. Because a block can only reference one previous block, it is impossible for two forked chains to merge. The ever-growing size of the blockchain is considered by some to be a problem due to issues like storage and synchronization. On an average, every 10 minutes, a new block is appended to the blockchain through mining.

1.2. Blockchain as a public record

With Bitcoin, there is no single organization in charge of the currency, which is an enormous change when one thinks about the power a central bank has, controlling over the money supply. The idea here is to make it so everyone (collectively) is the bank. In particular, everyone using Bitcoin keeps a complete record of which Bitcoins belong to which person. One can think of blockchain as a shared public ledger showing all Bitcoin transactions. The blockchain shows every single record of Bitcoin transactions in order, dating back to the very first one. The entire blockchain can be downloaded and openly reviewed by anyone, or you can use a block explorer to review the blockchain online.

1.3 Double Spending

The blockchain technology is especially useful in addressing the problem of double spending (multiple spending of Bitcoins). When the one party registers a transaction, it is broadcasted to the entire network of Bitcoin users, and asks them to help determine whether the transaction is legitimate. If they collectively decide that the transaction is in order, then the recipient can accept the Bitcoins, and everyone will update their block chain. This type of protocol can help prevent double spending, since if the sender tries to spend his/her Bitcoin with multiple times, other people on the network will notice, and network users will notify the

multiple recipients that there is a problem with the transaction, and the transaction shouldn't go through.

1.4 Proof-of-work and mining

Some users may try to double-spend by using an automated system to set up a large number of separate identities to validate their transactions. There' s a clever way of avoiding this problem, using an idea known as proof-of-work. The idea is counterintuitive and involves a combination of two ideas: 1. to (artificially) make it computationally costly for network users to validate transactions; and 2. to reward them for trying to help validate transactions. The benefit of making it costly to validate transactions is that the number of network identities someone controls can no longer influence validation, but only by the total computational power they can bring to bear on validation. As a result, a cheater would need enormous computational resources to cheat, making it impractical. For the proof-of-work idea to have any chance of succeeding, network users need an incentive to help validate transactions. Without such an incentive, they have no reason to expend valuable computational power, merely to help validate other people' s transactions. And if network users are not willing to expend that power, then the whole system won' t work. The solution to this problem is to reward people who help validate transactions. In particular, suppose we reward whoever successfully validates a block of transactions by crediting them with some Bitcoins. The reward is used so that people on the network will try to help validate transactions, even though that' s now been made a computationally costly process. Provided the Bitcoin reward is large enough that will give them an incentive to participate in validation. In the Bitcoin protocol, this validation process is called mining. For each block of transactions validated, the successful miner receives a bitcoin reward. Initially, this was set to be a 50 bitcoin reward. But for every 210,000 validated blocks (roughly, once every four years) the reward halves. This has happened just once, to date, and so the current reward for mining a block is 25 bitcoins. This halving in the rate will continue every four years until the year 2140 CE. At that point, the reward for mining will drop below 10^{-8} bitcoins per block. 10^{-8} bitcoins is actually the minimal unit of Bitcoin, and is known as a satoshi, after the Satoshi Nakamoto mentioned earlier. So in 2140 CE the total supply of bitcoins will cease to increase. However, that won' t eliminate the incentive to help validate transactions. Bitcoin also makes it possible to set aside some currency in a transaction as a transaction fee, which goes to the miner who helps validate it. In the early days of Bitcoin transaction fees were mostly set to zero, but as Bitcoin has gained in popularity, transaction fees have gradually risen, and are now a substantial additional incentive on top of the 25 bitcoin reward for mining a block. One can think of proof-of-work as a competition to approve transactions. Each entry in the competition costs a little bit of computing power. A miner's chance of winning the competition is (roughly, and with some caveats) equal to the proportion of the total computing power that they control. So, for instance, if a miner controls one percent of the computing power being used to validate Bitcoin transactions, then they have roughly a one percent chance of winning the competition. So provided a lot of computing power is being brought to bear on the competition, a dishonest miner is likely to have only a relatively small chance to corrupt the validation process, unless they expend a huge amount of computing resources.

2. Current and future uses of blockchain technology

Blockchain is regarded as a next-generation information technology with many potential upsides in a number of fields beyond digital currencies (IEET). As said before, the first application of the blockchain technology was the digital currency Bitcoin, but the blockchain could be a much bigger opportunity than Bitcoin. The whole thing about blockchain-based

architectures is that they allow trustless transactional activity. There is no third party; there is no clearinghouse of identity information (Fred Wilson). So Bitcoin and blockchain technology is much more than a digital currency, the blockchain is an information technology, potentially on the order of the Internet ('the next Internet'), but even more pervasive and quickly configuring (Swan). Blockchain technology is one of the first identifiable large implementations of decentralization models that have the potential to "reorganize all manner of human activity" due to their ability to provide frictionless and trustless interaction between people and technology. Below more information is provided both for Bitcoin as well as the other possible uses of the blockchain technology.

2.1. Currency

Bitcoin was first described in a 2008 paper (written by someone under the pseudonym Satoshi Nakamoto) as "A peer to peer Electronic Cash System". In the beginning of 2009 the first cryptocurrency became a reality with the mining of the genesis block and the confirmation of the early transactions. The economic crisis in the Eurozone area and especially in Cyprus forced the Bitcoin price to go up to $1216.73. Since then, its price has slowed down steadily, thus the cryptocurrency was characterized by many as a financial bubble.. During 2013 and 2014, fraud incidents and hacking attacks made both investors and users question their trust to the currency. At that time, the price was a little below $300 with the daily volatility being around 3.5% when gold's volatility was 1.2% and that of other major currencies between 0.5 and 1%The reactions globally varied from country to country. Today most developed countries allow the use of Bitcoin, but consider it "private money" (USA) or "property" (Germany). However, there are some countries, most of which are in Asia and South America, along with Russia where Bitcoin is considered illegal. Furthermore, the European Central Bank has issued a statement that warns investors for the risks of Bitcoin.
You can acquire Bitcoins through mining, buy the firm another user or an exchange, receive them as payment for work or even ask donations in Bitcoins. Other notable cryptocurrencies are: Ripple, which was created by Ripple Labs and belongs to the category of pre-mined cryptocurrencies, Litecoin, which is based on the same protocol as Bitcoin but it is much more user-friendly in terms of mining and transactions, Darkcoin, a cryptocurrency that provides real anonymity during transactions, and Primecoin, whose solutions during mining procedure are prime numbers.

2.2. Contracts

An emerging use of blockchain during the last years is the creation of "smart contracts". The term "smart contracts" appeared in 1994 when Nick Szabo described a computer program with if-then structure interacting with the real world. Different developers using Bitcoin overlay protocols in order to integrate their activities further expanded this idea. More specifically, they were created platforms where the users can buy derivatives with Bitcoin (derivatives), issue their own currency (Colored Coins) and use the Bitcoin network as credit for their exchanges (Blockstream). The real revolution on this sector came from the Ethereum Project. The main purpose of this project is to create an independent platform where, using a programming language, the users can create a virtual contract between them for any purpose they want. A same project named Codius is also under developing from the Ripple Labs. The contract is executed when the loop of the commands if and then is coming into a result from real-world data. The range of the uses for these contracts is practically limitless. Every procedure that needs a third trusted party to be completed can be codified and run in the platform of their preference. That includes simple money transactions between privates, selling and buying of tangible and intangible goods and the potentiality of securing financial or not transactions that need hedging due to their instable nature. A fair example is the

agricultural market because of the products' vulnerability. The use of the smart contracts is not restricted to the financial and commercial sector though. A smart contract can be used to confirm a real estate transfer playing the role of the notary. At the same time, a user can write his/her own will on the platform and the contract will be executed after his death without the intervention of a third party (notary, judge) to confirm it. The same technology can be used for betting purposes as the need for a carrier that controls the bets does not longer exists. The procedure of a betting using a smart contract is: The users put their money on a digital account, they create a virtual contract that define the conditions of winning and losing and when a result came up in the real world, the contract get updated from an online database and execute the terms by transferring the money to winner's account.

2.3 Voting

Voting procedures remain in many countries a controversial topic, as incident of electoral fraud (invalid or inaccurate vote, multiple registration) and the big percentage of abstention often shape the final result. The adaptation of blockchain technology from any institution in any country that wants to run a voting campaign seems as an effective solution. The members could connect to a PC-based system through their computer, laptop or smartphone, using open-source code that is open to editing using a kind of authentication (biometric, written) prove their identity to the program. Then, they enter their private key to access their right to vote and using their public key to select their preference and confirm it. So far, three projects have been founded that promote voting through blockchain systems. The first is BitCongress that uses the Ethereum platform to develop its idea based on the scenario that every voter has access to one "votecoin" that enhances him to vote only one time and his vote will be recorded on the blockchain after the system verifies it. Other similar projects are Remotengrity, which provides every physical vote with a cryptographic code in order to verify the authenticity of every vote, and AgoraVoting, which uses the Bitcoin network to develop a voting blockchain-based tool that will be used in the procedures of Spanish Congress. Generally, the transformation of the voting system from paper-based to digital will increase its reliability and the convenience that offers to the voters.

2.4 Intellectual property rights.

Blockchain could be used to enforce to prove intellectual property rights. A good example of this is "Proof of Existence", a service created by Manuel Araoz, a 25-year-old developer in Argentina. The site allows you to upload a file to certify that you had custody of it at a given time. Neither its contents nor your own personal information are ever revealed — rather, all the data in the document gets digested into an encrypted number. Proof of Existence is built on top of the Bitcoin blockchain (there's a 0.005 BTC fee), so the thousands of computers on that network have now collectively verified your file.

2.5 Smart Property

A less known field that the blockchain technology could have a major impact is that of "smart property". The Internet of Things (IoT), a technology that connects every home device in the global network, is constantly growing. "Smart property" is a combination of IoT and the Bitcoin infrastructure that is defined as a physical asset whose ownership is controlled via blockchain with the use of contracts. The most famous example was described by Nick Szabo (1997) when he said that in case the debtor misses a payment in a car loan, a smart contract could revoke the digital keys to operate the car. Other examples are keys for cars (leased and

rented), homes, apartments, hotel rooms, lockers and safety deposits. A smart contract that includes physical property is easily updated when the owner changes without the need for notary's contribution.

2.6 Finance

The most widely accepted application for the blockchain technology is in the field of finance, as it ensures the much valued transparency between the trading parties. Every transaction in public or private equities, stocks, bonds or derivatives could be transcripted in the blocks and afterwards be confirmed by the local authority for its legitimacy. From this point, it's easier to detect fraud cases or money laundering through stock exchange moves. Apart from finance in the traditional form, the blockchain could also improve the contemporary forms of financing. Crowdfunding can also be improved through blockchain adaptation. Instead of a platform that collects donations and distributes them to the campaign runners, it could turn to a decentralized platform that manages the money from the benefactors and if the campaign is successfully completed gives the money to the runners or otherwise returns the donations back. This solves the trust problem that many newly established crowdfunding sites face.

2.7 Blockchain technologies in the Greek economic environment

2.7.1 Shipping management

Another service that could be redefined by the blockchain technology is the control of the containers that arrive in the Greek ports. The moment a container arrives at the port it could be labeled with a cryptographic hash that would match the last received container. The value of a system like that is that is automatically keeps track of all the containers and therefore prevents scams or mistakes like changes in specific information or incidents of industrial espionage. The most important fact it that due to the decentralized nature of the system, no information is going to be lost. In case of labor disputes or a natural disaster, the normal operation of a port is detuning due to bad control of the previous information. This can be a heavy cost for the managing port organization as the economic processes are delayed and create paralyzing effects to the port that may need several months to recover. The most recent example in the international market is the port of Oakland where the labor disputes cause a 2-month delay to complete the necessary procedures for the plain operation of the port. A system based on the blockchain technology can continue to serve the needs of the port even in extreme cases for the reason that it is independent from the labor force of the port.

2.7.2 Land titles

The digitalization of the land titles can be beneficial for a society as it reduces the bureaucracy and the corruption that is connected with the real estate industry. The users of a blockchain-based system could inspect any property record in real-time without any cost. Apart from this, the authentication of the holders would be easier and land transfer would require considerably less capital. The most important part is that the open-source system would allow its users to build applications in order to improve the way of accessing the records.

Conclusion

From this researh it is clear that the blockchain technology is yet unexplored and has much to offer in many fields. With potencial application ranging from wider banking and business to voting and international trade, blockchain could redefine many aspects of our life. Further research suggestions would include the economic implications and impact of such non-Bitcon blockchain applications.

Bibliography

- Skudnov, R. (2012). Bitcoin clients. *Instructor*, *3*(12), 32.

- Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance by Michael Mainelli and Chiara von Gunten, Z/Yen Group, Long Finance December 2014

- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. " O'Reilly Media, Inc.".

- Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. *URL https://github. com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper*.

- Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, Q3.

- Blundell-Wignall, A. (2014). *The Bitcoin Question: Currency versus Trust-less Transfer Technology* (No. 37). OECD Publishing.

- Mann, C., & Loebenberger, D. (2014). Two-factor authentication for the Bitcoin protocol.

- "SATOSHI'S REVOLUTION: How The Creator Of Bitcoin May Have Stumbled Onto Something Much, Much Bigger."*Business Insider*. Accessed April 7, 2015.http://www.businessinsider.com/the-future-of-the-blockchain-2014-4.

- "Bitcoin Series 24: The Mega-Master Blockchain List." *Ledra Capital*. Accessed April 7, 2015.http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list.

-"Blockchain Definition." *Investopedia*. Accessed April 7, 2015.http://www.investopedia.com/terms/b/blockchain.asp.

-Evans, Jon, and Columnist. "Enter The Blockchain: How Bitcoin Can Turn The Cloud Inside Out." *TechCrunch*. Accessed April 7, 2015.http://social.techcrunch.com/2014/03/22/enter-the-blockchain-how-bitcoin-can-turn-the-cloud-inside-out/.

-“Hidden Flipside.” *The Economist*, March 15, 2014.http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside.

-Lantz, Lorne. “Bitcoin Is Just the First App to Use Blockchain Technology - O’Reilly Radar.” Accessed April 7, 2015.http://radar.oreilly.com/2015/01/bitcoin-is-just-the-first-app-to-use-blockchain-technology.html.

-“Present Uses for the Blockchain.” *CoinReport*. Accessed April 7, 2015.https://coinreport.net/present-uses-blockchain/.

-“Why the Block Chain Could Be Bigger than Bitcoin | WordPress Hosting by @WPEngine.” *WP Engine*. Accessed April 7, 2015.http://wpengine.com/2014/05/19/block-chain-could-be-bigger-than-bitcoin/.

- Economics beyond Financial Intermediation Digital currencies’ possibilities for growth, poverty alleviation and international development
Dr. Saifedean Ammous
Paper presented at the Columbia University PhD in Sustainable Development 10 Year Anniversary Conference, February 28, 2014