Blockchain Use Cases: From Beyonce to Barack

Meet Patel
Meet.Patel@tufts.edu

December 14 2016

Abstract

With its meteoric rise in popularity after the emergence of Bitcoin, blockchains have been held in high regards in terms of their security and therefore their affordability. This is especially so in the financial world where the first use cases were displayed. These blockchains have not only the capabilities to revamp how banks handle money transfers but also any situation where many small time vendors are conducting business with other individuals. This includes business such as Venmo and Airbnb. Nearly any model that contains individualized information and holdings such as the stock market can use some version of a modified blockchain to store their data. Although a blockchain can be used for these models, it is not always the best option due to the various disadvantages including; large resource consumption, code integration and maintenance, and large costs. This paper will discuss the optimal use cases of blockchains taking into account the various advantages and disadvantages of the technology.

Introduction

The concept of a blockchain was originally created for a “peer-to-peer version of electronic cash”; Bitcoin (16). The goal was to avoid the middleman figure of a financial institution when conducting transfers. The Bitcoin was developed to be self-regulatory in order

to avoid the need of a trusted third party to verify each transfer and this was done using blockchains that needed heavy computing power to be created. The blockchain was an extreme success in this particular case and although this paper will look at the reasons why blockchains are so well suited for the financial market, the goal is to apply this reasoning to other use cases outside of this particular market.

To The Community

Blockchains implement a vastly different approach to storing data than has been used in the past. There is now a viable alternative to the client - server model that can be implemented securely enough to be trusted with financial transactions. Blockchains have the chance to replace many systems but a great deal of tests and proof of concepts have yet to be completed. It is often simply not enough for a new technology to be viable for it to be adopted in institutions that have already become deeply entrenched within an older technology. For financial institutions, for example, the rewards could not be greater. A Santander report suggested (17) banks could save 15-20 billion dollars in infrastructure costs per year; however it could cost in the order of billions to actually build the initial blockchain infrastructure. With billions of dollars in the balance, the technology has to be researched to a much greater extent than it has. There is no current consensus on what is possible; on what is secure; on what method of mining is optimal. Many new technology startups have been working on implementing various ideas that incorporate blockchains but very few of these products has reached a stage where it could be shipped to consumers. Many of these projects are just experiments on what the technology can accomplish and are not even being considered to be released for public consumption.

As these projects advance and continue to experiment, looking at what works and what does not for each particular case can be a useful exercise in creating more effective blockchain

based technologies. These projects also illustrate what kinds of ideas are well suited towards being implemented through the use of blockchains and what ideas would be better implemented through more traditional technologies.

Applications

What is a blockchain?

Blockchains come in various shapes and sizes but the most basic elements to the block chain consist of three parts: data distribution through peer-to-peer, data stored in blocks linking to hashes of the previous block, and the defense and consensus rules.

One of the big selling points, and also one of the big detriments, of blockchains is that information regarding new updates to the blockchain is shared through multiple nodes in the network. In this model, every participant in the network for the blockchain can have a complete copy of the blockchain and as updates get passed around from one node to another, the blockchain gets updated for every member. This decentralized system of storage makes it such that if a single node is taken offline, the blockchain can continue to function as normal. In a client - server model, all the data is held in one location or server and if that one server is taken down; the entire database becomes unusable. Although this makes peer-to-peer networks more resilient, it also means that multiple copies of the database must exist and be stored. This is further explained in the scalability section.

Data storage in blockchains is a way to both protect the integrity of the data in the chain as well as maintaining an order. A blockchain is made up of multiple blocks linking to each other (13). In Bitcoins, for example, each block contains all the transactions that were made and have not been appended to the blockchain before that particular block. The block also contains header information which contains: “some technical information about the block, a reference to

the previous block, and a fingerprint (hash) of the data contained in this block" (13). This fingerprint is essential to maintaining the integrity of the blockchain. For example, if a particular block has the hash *asd2ji* than another block with hash *bc23a2* would be built on *asd2ji*. The next block to be added to the blockchain, *jklml4v0*, would then be built on *bc23a2*. With each blockchain referencing the previous blockchain's hash fingerprint; if a single hash fingerprint is changed because the data was modified, all following hash fingerprints would also have to change in the blockchain. The need to change multiple blocks to change just one block in addition to the computationally expensive procedure of mining/creating a single block makes modifying a block that has around 6 blocks linking to it nearly impossible to change (in Bitcoin) (14).

This computationally expensive procedure is part of the third big element in blockchains; defense and consensus rules. For public blockchains like Bitcoin where anyone can write/read/mine the data, there has to be a method to trust the information provided by users. Bitcoin uses a proof-of-work model to deal with this issue. This means, whenever a user wished to update the blockchain with a new block, they must prove that they have spent a significant amount of computing power to obtain the block. In Bitcoin, this is done by requiring the hash of the block to conform to a certain pattern. This pattern requires that for any block to be deemed valid, the hash has to start with a certain number of zeroes. This is very difficult to do as it is computationally impossible to guess how a hash will behave with certain data. Modifying the header of the block until a initial hash of say *jklml4v0* becomes *000000pvd432s* is extremely expensive and, with bitcoins settings, a new valid block is only created every ten minutes. This latency can be increased for stronger security (15). Since it takes a long time to mine a single new valid hash for a particular block, if the data in a block is changed half-way through a blockchain; all following blocks would have to have their hashes recalculated and validated. If

attacker simply removes all the following nodes and emits a shorter blockchain to the nodes, the consensus rule kicks in. This rule is how conflicts are resolved on which blockchain is the correct one and which newly added blocks are to be considered as being part of the blockchain. In Bitcoin, the longest chain rule is used. As the name suggests, the longest chain rule finds the longest existing blockchain and accepts it as the valid blockchain. By combining the consensus rule and the mining expense, creating a fake longer chain to overtake the one created by the rest of the network becomes exponentially difficult (16).

Scalability Issues

One of the biggest issues with Bitcoin and other blockchain technologies has been making them scalable and a large part of this issue stems from the side-effects of having a peer-to-peer network (15). Companies like Facebook, Google, Amazon and Netflix store petabytes of data in their own distributed databases whereas Bitcoin currently only has around 50-60 GB of data. 60 GB of data is a fairly small amount of data to store in each node participating in the peer-to-peer network (15) yet there are already worries the Bitcoin network is becoming bloated. The reason the big technology companies are able to store such vast amounts of data is that they store only partial data in each individual node. In addition, Netflix for example, only stores three copies of each piece of data which means more nodes are available to store other data. With a limited replication factor and only storing small sections of the data in any given node, Netflix is able to store large quantities of information that Bitcoin, and the blockchain, could not possibly handle. There have been efforts to remedy this situation by implementing new innovations on distributed databases to add the benefits of blockchains in cases like BigchainDB (15). BigchainDB is fairly recent; it’s white paper was released earlier in

2016 so it has been yet to be implemented effectively in an actual product but this is simply one possible route to a scalable blockchain.

Proof-of-work Issues

There is no perfect solution to maintaining the integrity of the blockchain but the proof-of-work method has been effective with Bitcoin. It effectively makes attackers required to control a vast amount of computational power in comparison to the actual network which is nearly impossible for established chains. The issue with Bitcoin's usage of the proof-of-work method is that it "create[s] downward pressure on the Bitcoin price" (7). There is no incentive to keep Bitcoins and miners often immediately sell off the rewards they earned for mining a block to keep their enterprises up and running. Mining is also more efficient in groups under this framework as the more computing power you have and the faster your internet connection is, the more likely you will be able to emit a valid block and have it incorporated into chains before your competitors. By combining power and forming mining groups, rewards are more likely to come by even though they have to be shared between the group. This is because if two blocks are created at a relatively similar time, the one that has the next block linked on first will activate the longest chain rule and become valid. This will cause the other blocks created to be invalid and a waste of computing power and electricity. Since group mining is incentivised here, the top 10 mining pools for Bitcoins generate over 90% of the blocks with 60% of them coming from China (12). This creates centralization which adversely affects the ability of blockchains to preserve decentralization, security and identity. For products that rely on this like voting mechanisms, this can be hugely problematic (4).

Security Issues outside of Blockchain

Although the blockchain itself can be made to be highly secure, that does not mean the applications or the usage of the blockchain will be completely secure; one simply needs to look at the $72 million worth of bitcoin stolen from Bitfinex in August this year (3). Password theft and issues with cryptography and key management in bitcoin exchanges have led to millions of dollars of losses (8) even though no direct weakness were exposed in the security of the blockchain (3).

Notary, Proof of Existence, Escrow Applications

There are multiple startups using blockchains to create systems that could potentially eliminate the need for notaries. Notaries can be expensive and inefficient and while they often have other roles than certifying documents as official, that particular role comprises a major part of their job (5). This process can not only be extremely expensive but time consuming as well. Blockchains have the ability to "certify the existence, ownership and integrity of any kind of data, in a way that is accurate, reliable, decentralized, cheap, and counterfeit-proof" (5). This kind of Proof of Existence application of a blockchain does not even require the actual document to be stored in the blockchain - only cryptographic digest needs to be stored. This digest could than be verified at any later time to prove you had access to the file at any given time. It also prevents the document from being changed as the hash of the file would then change (2).

Others have also suggested blockchains could be used to implement Escrow services. For example escrow services are required in the real estate market when buyers and sellers need third party verification; this would not be necessary through the use of a blockchain and bitcoins where the contracts would execute automatically once an order or purchase was verified. Here bitcoins would be the escrow system but this also limits the capabilities of what escrow is as of now. As co-founder of Dyadic Security, Nigel Smart posed it "...if you're

transferring a large amount of money, if you put it into a traditional escrow account it earns interest, and if you put it in a Bitcoin account it doesn't earn interest.” (11). There could be possible solutions to allow escrow services to be completely operated using a custom blockchain but this field has not been so widely explored.

Music Sharing and Newspaper Applications

Blockchains have a huge potential in any publicly shared database and also in any industry that would require many, low cost microtransactions. These microtransactions might be too expensive with the overhead of regular models but blockchains might be able to reduce the cost of these transactions to make them a valid product. Two examples that fit into this category are music sharing and newspaper subscriptions. Newspapers could potentially offer daily subscriptions or per article payment options over the monthly subscription services currently being offered. Music sharing is already a field where blockchain technology is being utilized with moderately famous singer Imogen Heap spearheading one such product called Mycelia (9). Ms. Heap sees this as a chance to move away from an industry that very few artists have any good things to say about. She suggests there be one true version of any particular artist’s content with all the multitudes of platforms pointing to the single point. The blockchain being suggested by the creators of Mycelia is going to need systems to modify information; i.e. if a better version of the song is available and can replace the old version; and as of now this and many other problems still need to be addressed. Mycelia is still currently in the works but it is one of the blockchain technologies that is furthest along the path to becoming a viable product in the music field (9). Mycelia would definitely allow artists a much stronger control of their own music and microtransactions directly between artists and consumers could become a distinct possibility.

Voting

Some of the biggest roadblocks stopping electronic voting from becoming a reality in the US have been issues of security in the database, possible changes being made to the database after votes have been cast, and voter fraud. Nearly all of these issues could be addressed in one form or another by blockchain technology. For example, in the case of voter fraud, there are already 12 companies that are using blockchains for identification and authentication purposes (1). Some of these companies, like ShoCard, are secure enough that banks could rely on it. ShoCard has already explored using their technology to work with bank loans and other services as well as working with airlines to streamline passenger identity verification through facial recognition and data stored in blockchains (10). This technology could be easily adaptable for voting registration. In regards to other issues with traditional electronic voting: one group having too much power over the database, or the ability to censor votes based on particular information, or even to add additional fake votes; blockchains were almost created to tackle these exact problems. Follow My Vote is one organization that has made significant progress in creating a voting platform that would allow for much greater convenience in voting while also providing more transparency in the process as a whole. By creating a block to store tallies of votes, changing/removing/adding illegitimate votes becomes nearly impossible; especially when a method of verification of user voting is added to the blockchain. Implementing a blockchain based voting platform would significantly reduce the cost of elections according to Follow My Vote (6).

Multiple startups have gained a large amount of steam with technology revolving around blockchains and there are still many unexplored possibilities left. Although there are some technologies that do not currently seem feasible for blockchains; blockchains themselves are

relatively new to the world and possible improvements like BigchainDB are just now coming out. So although certain ideas might not be able to mold well with blockchains as we know them now, a successor technology might be a much more ideal option. For now, the blockchain technology has thoroughly proven itself with Bitcoin albeit many intricacies that make implementing blockchains a challenge remain. As these startups mature, we will empirically be able to see the results of the blockchain hype.

Works Cited

1. Amit. "12 Companies Leveraging Blockchain for Identification and Authentication." *Let's Talk Payments*. N.p., 07 Oct. 2016. Web. 14 Dec. 2016.
2. Araoz, Manuel, and Esteban Ordano. "What Is Proof of Existence?" *Proof of Existence*. N.p., n.d. Web. 14 Dec. 2016.
3. Baldwin, Clare. "Bitcoin worth $72 Million Stolen from Bitfinex Exchange in Hong Kong." *Reuters*. N.p., 3 Aug. 2016. Web. 14 Dec. 2016.
4. "Blockchain Comparison, A Closer Look At Bitcoin, Bitshares, and Ethereum - Follow My Vote." *Follow My Vote*. N.p., n.d. Web. 14 Dec. 2016.
5. "Can Blockchain Technology Send Notaries on Vacation... For Good?" *Medium*. N.p., 06 Nov. 2015. Web. 14 Dec. 2016.
6. @FollowMyVote. "The Online Voting Platform of The Future - Follow My Vote." *Follow My Vote*. N.p., n.d. Web. 14 Dec. 2016.
7. Graydon, Carter. "Bitcoin's Future: Proof-of-stake vs Proof-of-work." *CryptoCoinsNews*. N.p., 30 Aug. 2014. Web. 14 Dec. 2016.
8. Hornyak, Tim, and Jeremy Kirk. "10 Things You Need to Know about Mt. Gox's Bitcoin Implosion." *PCWorld*. IDG News Service, 06 Mar. 2014. Web. 14 Dec. 2016.
9. Howard, George. “Imogen Heap Gets Specific About Mycelia: A Fair Trade Music Business Inspired By Blockchain” *Forbes*. Forbes Magazine, 28 July 2015. Web. 14 Dec. 2016.
10. "Identity for a Mobile World." *ShoCard Identity for a Mobile World*. N.p., n.d. Web. 14 Dec. 2016.
11. Korolov, Maria. "Is the Blockchain Good for Security?" *CSO Online*. CSO, 01 Apr. 2016. Web. 14 Dec. 2016.
12. Lewis, Antony. "A Gentle Introduction to Bitcoin Mining." *Bits on Blocks*. N.p., 24 Nov. 2016. Web. 14 Dec. 2016.
13. Lewis, Antony. "A Gentle Introduction to Blockchain Technology." *Bits on Blocks*. N.p., 24 Nov. 2016. Web. 14 Dec. 2016.
14. Lewis, Antony. "A Gentle Introduction to Immutability of Blockchains." *Bits on Blocks*. N.p., 24 Nov. 2016. Web. 14 Dec. 2016.
15. McConaghy, Trent, Rodolphe Marques, Andreas Muller, Dimitri De Jonghe, Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto. *BigchainDB: A Scalable Blockchain Database*(n.d.): n. pag. *BigchainDB*. 8 June 2016. Web. 14 Dec. 2016.
16. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." (n.d.): 109-22. Oct. 2008. Web. 14 Dec. 2016.
17. Petrasic, Kevin, and Matthew Bornfreund. "Beyond Bitcoin: The Blockchain Revolution in Financial Services." *White & Case LLP International Law Firm, Global Law Practice*. N.p., 07 Mar. 2016. Web. 14 Dec. 2016.