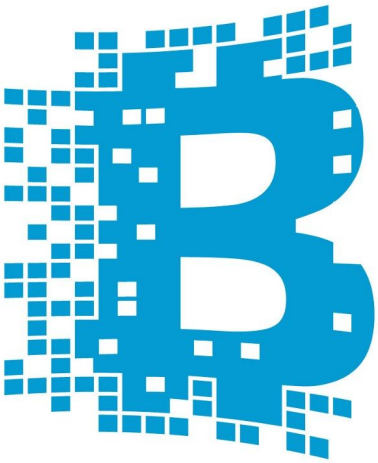
The Blockchain



CSC 462

Jakob Roberts - V00484900

Carl Masri - V00786576

Cole McGinn - V00780893

Introduction

Blockchain was first defined in a 2008 paper by Satoshi Nakamoto. Originally designed as the underlying architecture for the cryptocurrency Bitcoin, blockchain technology has been steadily growing and is now implemented in a wide variety of applications including identity management, file storage, and distributed computing. Even large institutions such as NASDAQ are experimenting with blockchain technology [1].

What is blockchain?

Put simply, a “blockchain” is a ledger of facts. These facts can be anything from monetary transactions to individual files to complete storage units [2]. A good way to think about this is to first look at a technology many of us are familiar with: BitTorrent. BitTorrent is used to exchange files of all types by members of its network; blockchain, on the other hand, is used to exchange *facts*. These facts are grouped together into sets called *blocks*, which are arranged into a “chain” (hence the name) that references prior blocks in the sequence. Once a fact is written into the blockchain, it cannot be altered without recreating all future blocks that came after. This is a fundamental aspect of blockchain and means that data can only ever be added to the ledger, never removed. It should also be noted that blockchains can be both public or private. Public blockchains (such as Bitcoin) allow anyone to read or write to the ledger. Private blockchains, on the other hand, consist of a network of trusted participants (also called an internal blockchain). In the case where a ledger's block-makers are not trusted (eg. Bitcoin), the security is provided by making it computationally expensive to add a block to the chain. The computation itself is a “guessing game” where block-makers (aka miners) need to guess a number which, when crunched with the rest of the block data contents, results in an output where the pointer to the prior block matches the prior block’s hash. This number varies depending on the number of blocks created and is relative to the difficulty of mining a new block. To summarize, blockchain is a full history of transactions where each transaction can be uniquely identified to their owner.

Why do we need blockchain?

Ever since the creation of the internet, there have been issues with privacy, security and inclusion with cryptography [7]. As our world becomes ever-increasingly connected, the microscope has become focused on these issues now more than ever before. Blockchains solve this by utilizing public and private keys so the user has privacy behind that key. Although everyone can see the public keys and signatures in the blockchain, they are meaningless because anyone can create a new public key for each transaction if they want, it’s as easy as pressing a single button. The high level of security is one of the main features of blockchain. The usage of the cryptographic chaining of the blocks allows for secure and concrete transactions.

Why can’t we just use regular databases?

Blockchain is essentially just a database, right? So what makes it so different from other centralized databases? The comparison can (and has) been made, but the major difference doesn’t come from the function so much as the execution. In traditional databases such as SQL or NoSQL, a central administrator is required even in the case where the database uses distributed architecture. In blockchain, the entire data store is distributed in such a way that every node in the network holds nearly 100% of the data. This provides a huge advantage when dealing with untrustworthy and fragile networks. It should be noted that if robustness and trust are not an issue for the system being built, there’s no advantage to using blockchain over a regular database; the data being stored and transactions being performed on that data are identical. In many systems, however, this is not the case. The ability for allowing data to be shared across boundaries of trust without the need for a central administrator completely turns the traditional client-server model on its head. Blockchain allows for reliable storage that can be verified by anyone at anytime, in contrast to traditional databases that you must trust with your data. This “trustless” type of system does not come without drawbacks, of course. The need for each node to have complete transparency with the full ledger of transactions in order to verify them means that confidentiality of the data can be compromised [9]. This problem can be mitigated somewhat using clever cryptographic methods, but not without computational cost which is compounded with every added transaction.

How Blockchain Works

Blockchain is, at its core, the very definition of a distributed system with complete reliance on the use of a decentralized peer-to-peer network. Without this, the blockchain ledger would simply be a local list of transactions with no outside verification, no replication, and no additional purpose other than that of a local database.

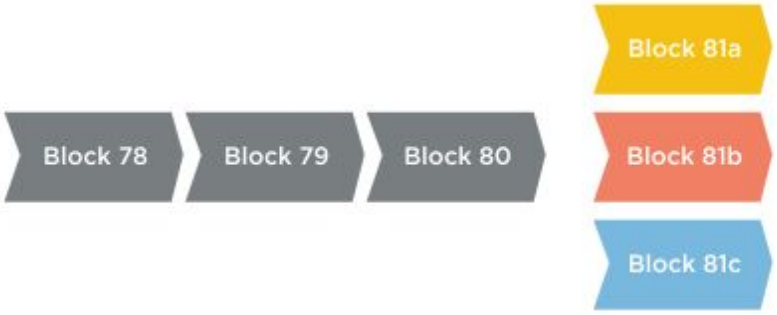
In comparison to client-server models where servers hold all of the data and the clients trust the server to be accurate, every node in a peer-to-peer network has 100% of the data (or as much as possible) and the updates are shared. As with every other distributed system, this method has trade-offs. The highly replicated data provides a very resilient and fault-tolerant storage system, however, it also needs a powerful consensus algorithm to keep that data consistent across all the nodes. In blockchain, the rules for updating the ledger (ie. ordering the facts) are provided by a special consensus algorithm called proof-of-work. The specifics of this type of consensus vary depending on the system, but the mechanics remain the same. To summarize, new blocks (the next block in the chain) are proposed by a node only after that node has solved a special mathematical problem. The problem chosen depends on the system, but it is guaranteed to be highly difficult to solve. This is what ensures the security of blockchain technology in an untrusted network; as long as no single user owns more than half of the nodes,

the network remains safe and resistant to fraudulent blocks. With blockchains, each block in the chain references the previous block. The mechanism used for identification is a hash of the block contents itself, which serves as that block's unique fingerprint.

This method of block ordering is also what makes blockchain technology so secure. The data in each block is verifiable by anyone using special algorithms. If the fingerprints are both consistent with the data and form a chain, you can be sure that the blockchain is consistent. If a malicious user decides to change some of the transactions for their benefit, they would not only need to regenerate the fingerprint for that specific block, but also for every block that has been created from that point forwards.

In terms of Bitcoin, a "miner" is someone who contributes to computing the hash for the next block in the chain. Blockchain technology provides miners with incentivisation in the form of a "block reward". Whenever a miner successfully has their proposed block accepted into the network, they receive a reward. In Bitcoin this is a set number of Bitcoins (25), but this can differ depending on the system being used. If your blockchain network is trusted there is no need to make it expensive to add blocks, and therefore the incentives for creating them can be reduced. In an untrusted network like Bitcoin, the transaction and block validation is slow and expensive by design; the intentional difficulty of generating these fingerprints makes rewriting a blockchain an exceedingly slow and computationally intensive process. Unless the malicious user has the computational means to compete with the entire "honest" network (and remain ahead forever), they will not be successful in altering any data in the blockchain.

Conflicts in the blockchain occur in the form of multiple blocks being created simultaneously by different miners. One way to resolve this is by following the "longest chain rule" (used by Bitcoin). To illustrate this, imagine you have three miners who all complete the next block (Block 81) at the same time:



[4]

For other nodes in the network, if this is the first time a miner is seeing a Block 81 it is assumed to be valid and they can begin building the next block on top. For example, if a miner sees Block 81a first, they will begin mining on that block:

[4]

However, if a second Block 81b appears and its chain grows longer than the one currently being mined the miner should ignore the previous block (81a) and focus on the longer chain, as it is considered the valid one.

[4]

It should be noted that this is only one way to resolve conflicts. On a more trusted network other options become viable, such as using a central validator which can decide which of the blocks should continue as the valid chain. Only public blockchains require a shared consensus model.

Blockchain provides an alternative to the classic client-server model that we're all too familiar with.

Pros/Cons?

Pros:

- Blockchain is resilient! As the saying going, there's “security in numbers”. Whereas traditional client-server systems will typically replicate data across a number of nodes, blockchain uses a peer-to-peer network which replicates across thousands (if not more) nodes. This adds a certain amount of complexity (most notably, consensus), but also gives more independence to each node (can continue operation in the face of network failure). There is no “central point of failure” as with many other systems.
- Can be permissionless or permissioned, depending on its usage.
- Bitcoin blockchain can be used for more than just Bitcoin!
- Security without relying on trust. The security of the cryptography makes it so you don’t have to trust how you’re making transactions.

Cons:

- Potential for fraud (although extremely unlikely/basically impossible).
- Nodes are responsible for self-updating.
- It’s big. All transactions that ever happen must be maintained. In the case of Bitcoin, all transactions ever made must be kept track of. This ledger will only grow larger.
- Centralized databases are more confidential
- Centralized databases have higher performance.

What are the applications?

Cryptocurrencies:

The most widely known application would be that of Bitcoin and other forms of currency such as Dogecoin.

Identity management:

There has been much debate and research done lately on the removal of passwords in favour of faster and easier to use technologies, such as biometric security. Another alternative to this is blockchain-based identity management. Using this technology, user profiles (called Passcards) are created with the intention of being used to replace the current username/password combo for accessing online applications.

File storage:

Peer to peer file sharing networks have many advantages over even cloud storage. The removal of the need for centralized databases (or even traditional cloud databases, which require resource-heavy consensus algorithms to remain consistent) gives rise to highly distributed resource systems that don't rely on massive server farms. Start-up company Storj.io is leading the foray into next-gen distributed cloud storage. Using blockchain technology, Storj stores information about file integrity and storage locations using structured metadata [5].

Future use:

Banks plan on using blockchain technology to simplify trade finance processes. [3] This technology will help reduce risk between importers and exporters by having a public ledger that ensures the security of their transactions as well as speeding them up. Switching to blockchaining will also save billions of dollars because blockchains are so simple and easy to distribute in a peer to peer system. Blockchain has huge potential in fraud prevention; if a company were to store its general ledger in a blockchain, there would be no way for an individual (or group of individuals) to go back undetected and alter previous entries.

Record keeping:

Basically anything that needs permanent, immutable, tamper-proof data can be used with blockchain.

How do cryptocurrencies stack up?

Let's compare Bitcoin to CAD currency. CAD currency is created and distributed by the Canadian government. They can print however much they want which can devalue it. Bitcoin is decentralized and exists because people give value to it and are willing to trade it for goods and services. It is decentralized in the sense that there is no one central node. It is distributed amongst all nodes in the system and they all keep track of the blockchain. Also, Bitcoin doesn't have the issue of losing value because people give value to it and also Bitcoin has a set limit (21 million) and is slowly releasing them until the limit is reached. Unlike CAD currency, Bitcoin is 100% digital. This make it very portable as it can be accessed anywhere with internet access. CAD currency can be spent using physical cash or a debit or credit card. Bitcoin can be compared to using a debit card. Debit card just send the money to the sellers account. This just changes a virtual number in the user's account. Bitcoin is similar. You just make the transaction and it change's the virtual number in your account by that much. Bitcoin can be used in any way a debit card could be. Bitcoin is much faster for finalizing the transactions though. Normal currency / banks can take a couple days to finalize the transaction whereas Bitcoin only take a few minutes. Once it is part of the blockchain, it is set in stone.

Why is it not more widely used?

Blockchain is not more widely used simply because it is a newer technology. Although it seems great and cheap and fast it just simply hasn't proven itself to everyone yet. Since there has been no major issues with Bitcoin yet, people are still hesitant to jump on board. It is also a lot of effort to modify a current operation to use the blockchain. It would require revamping an entire system in order to make that modification. In order for a bank to switch their operations over to a blockchain, they would need to change their core system but as well as change their user accounts and link public and private keys to each user. Another problem with this is that the current slowness of bank systems could be a good thing. It leaves some extra time to correct fraudulent usages and so on. Banking has to be a secure operation, there is no room for error because it will be very costly. Sticking with their tried and true current systems has no downsides in terms of security. They know it is secure because it has been for a long time and they can count on that. Although blockchain is secure too, it just hasn't be around long enough to convince them that it will always be secure no matter what. Also, Bitcoin just seems so good and easy it's almost magic and big banks don't like magic.[6]

The Future of Blockchain

The future of blockchain seems bright. This is really an incredible technology that will open doors and make improvements in many online operations. Blockchain technology will probably mainly make big waves in banking. Because of blockchains obvious security, it will easily improve banking. It is just much more fast than current systems. As shown in the following figure, it will greatly improve the speed of any bank system. The only problem to overcome is the sheer scale of current banking systems and if the blockchain in its current state can keep up with the demand.

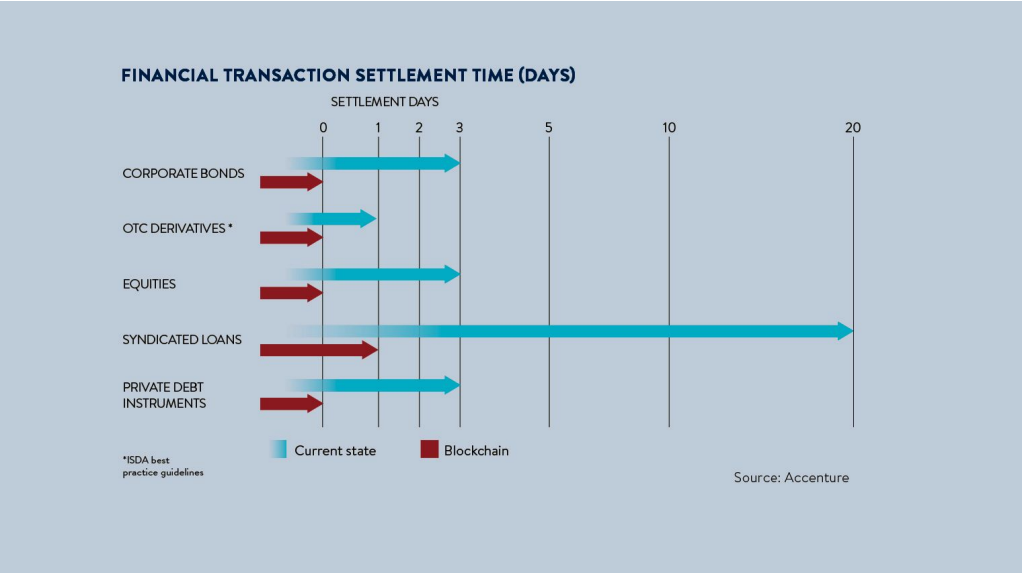


Figure X: Transaction Settlement Times [8]

The following figure describes the possible growth of blockchain. This starts with the early adoption and main use from Bitcoin. But then it leads to all the banks using it then finally a time where we wonder how we ever lived without it.

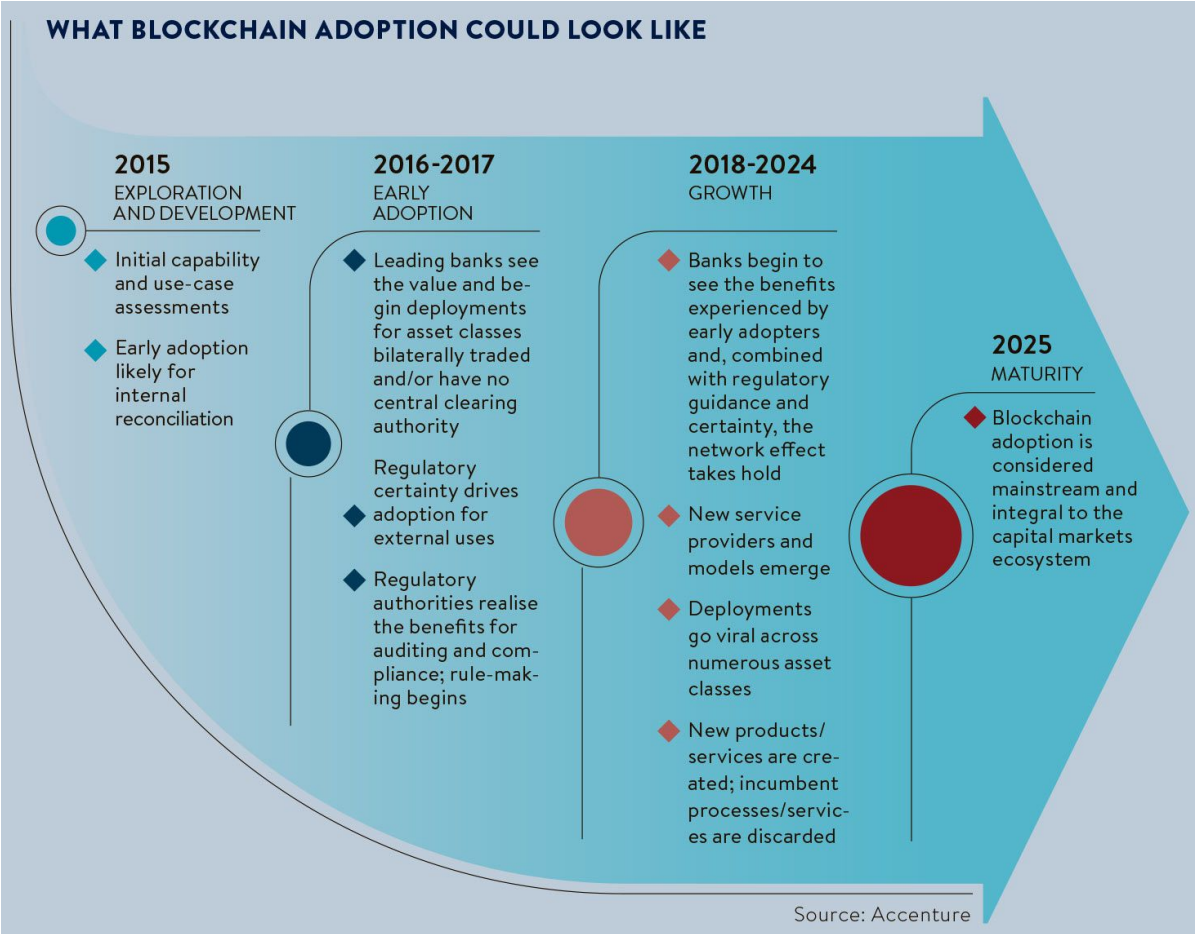


Figure Y: Blockchain Adoption [8]

Blockchain is such a powerful tool that perfectly solves the problems of security and privacy over the internet. This technology will hopefully be greatly used in the future, especially in banking.

References

[1] B. Casey, "A Bitcoin Technology Gets Nasdaq Test", *WSJ*, 2016. [Online]. Available: http://www.wsj.com/article_email/a-bitcoin-technology-gets-nasdaq-test-1431296886-lMyQjAxMTE1MzEyMDQxNzAwWj. [Accessed: 13- Aug- 2016].

[2] "Storj - Decentralized Cloud Storage", *Storj - Decentralized Cloud Storage*, 2016. [Online]. Available: https://storj.io/. [Accessed: 13- Aug- 2016].

[3] "Banks and tech firms apply blockchain to trade finance", *Reuters*, 2016. [Online]. Available: http://www.reuters.com/article/us-asia-trade-blockchain-idUSKCN10L17D. [Accessed: 13- Aug- 2016].

[4] "A gentle introduction to blockchain technology", *Bits on blocks*, 2015. [Online]. Available: https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/. [Accessed: 13- Aug- 2016].

[5] C. Marckx, "Storj: next-generation cloud storage through the blockchain - CCN: Financial Bitcoin & Cryptocurrency News", *CCN: Financial Bitcoin & Cryptocurrency News*, 2014. [Online]. Available: https://www.cryptocoinsnews.com/storj-next-generation-cloud-storage-through-the-blockchain/. [Accessed: 13- Aug- 2016].

[6] "Why B2B Pay is not using Bitcoin or the blockchain (yet) | B2B Pay powered by Barclays", *B2bpay.co*, 2016. [Online]. Available: https://www.b2bpay.co/why-we-are-not-using-bitcoin-or-blockchain-yet. [Accessed: 13- Aug- 2016].

[7] D. Tapscott and A. Tapscott, "Here’s Why Blockchains Will Change the World", *Fortune*, 2016. [Online]. Available: http://fortune.com/2016/05/08/why-blockchains-will-change-the-world/. [Accessed: 13- Aug- 2016].

[8] "The future of blockchain in 8 charts - raconteur.net", *Raconteur*, 2016. [Online]. Available: http://raconteur.net/business/the-future-of-blockchain-in-8-charts. [Accessed: 13- Aug- 2016].

[9] G. Greenspan, "Blockchains vs centralized databases | MultiChain", Multichain.com, 2016. [Online]. Available: http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/. [Accessed: 13- Aug- 2016]

[10] "Slock.it", https://slock.it, 2016. [Online]. Available: http://slock.it. [Accessed: 13- Aug- 2016]