[[1]](#footnote-1)

Blockchain Technology – A Survey and Tutorial

Steven Cocke, Daniel Davieau, Alex Salamah, Lakeitra Webb, Randall Hendrickson

*Abstract*— Blockchain, the foundation of Bitcoin, has received extensive media attention recently. Blockchain serves as a distributed, immutable ledger which allows transactions to take place in a decentralized manner. There are many challenges facing blockchain technology such as security, scalability, and legal implications. We will attempt to provide a broad overview on blockchain technology and its fundamental architecture.

# INTRODUCTION

B

LOCKCHAIN technology is increasingly being used in various industries such as healthcare, banking, supply-chain, finance, social media, and is the heart of Bitcoin. The goal of this project is to provide a survey of the current research and a tutorial on blockchain technology.

The blockchain idea was conceived back in 2008 to support bitcoin cryptocurrency exchanges. It is a very special decentralized transaction and data management technology that is critical for ensuring enhanced security and (in some implementations, non-traceable) privacy, security, and data integrity of transactions between participating parties, without going thru a 3rd party being in control of the transactions. Even though cryptocurrency such as Bitcoin, Litecoin, Ethereum, and the like, is highly controversial, the underlying blockchain technology has worked flawlessly and found wide range of applications in both the financial and nonfinancial world. Furthermore, Bitcoin uses a changeable Public Key (PK) to record the users’ identity, which provides an extra layer of privacy. Not only in cryptocurrency has the successful adoption of Bitcoin been implemented but also in multifaceted non-monetary systems such as in: distributed storage systems, proof-of-location, healthcare, decentralized voting and so forth. Recent research articles and projects/applications were surveyed to assess the implementation of Bitcoin for enhanced security, to identify associated challenges and to propose solutions for Bitcoin enabled enhanced security systems.

# Overview

Blockchain technology was invented in 2008 but came into the public conversation when Bitcoin launched. Blockchain is the digital and decentralized ledger that records all transactions. Every time someone buys digital coins on a decentralized exchange, sells coins, transfers coins, or buys a good or service with virtual coins, a ledger records that transaction, often in an encrypted fashion, to protect it from cybercriminals. These transactions are also recorded and processed withouta third-party provider, which is usually a bank. Blockchain was invented because of the perceived shortcomings of the traditional banking system. For example, when transferring money to overseas markets, a payment could be delayed for days while a bank verifies it. Many would argue that financial institutions shouldn't tie up cross-border payments and funds for such an extensive amount of time.

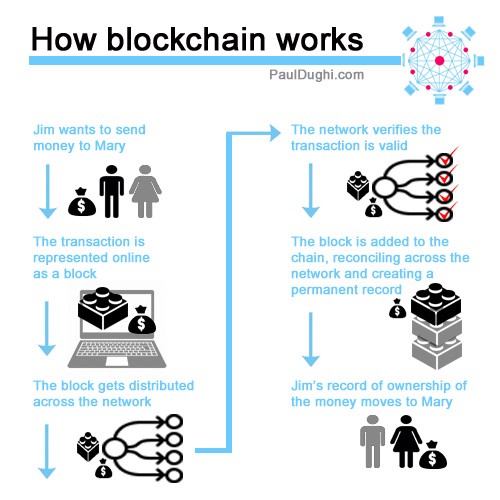


Fig. 1. A visual overview of how blockchain works

Banks almost always serve as an intermediary of currency transactions, thus taking their cut in the process. Blockchain developers want the ability to process payments without a need for this middleman. Furthermore, removing the middleman from the equation and working around the traditional banking system would allow smaller transaction fees. What's unclear is if lower fees equate to cheaper fees for the consumer, or just bigger profits for businesses to deploy blockchain technology. In addition, blockchain offers the potential to process transactions considerably faster. Whereas banks are often closed on the weekend, and operate during traditional hours, validation of transactions on a blockchain occur 24 hours a day, seven days a week. Some blockchain developers have suggested that their networks can validate transactions in a few seconds, or perhaps instantly. That would be a big improvement over the current wait time for cross-border payments.

Lastly, on a larger scale, the best real-world examples of blockchain in action are the partnership between Ripple (CCY: XRP-USD) and banking giants AmericanExpress(NYSE:AXP) and Banco Santander (NYSE:SAN). It was announced that American Express users would be able to send non-card payments to U.K. Santander accounts over AmEx's FX International Payment network and have those transactions processed over Ripple's blockchain. The allure of this partnership is Ripple's instantly settling cross-border payments, as well as the expectation of small transaction fees.

# HISTORY

The term “Blockchain” originated in a reference to a “chain of blocks” as described by the mysterious creator of Bitcoin, Satoshi Nakamoto (pseudonym) in 2008. [1] Nakamoto was describing the mechanism to solve the double-spending problem without the need of a trusted authority or central server. Three papers referenced by Nakamoto cite papers co-authored by physicists Scott Stornetta and Stuart Haber published in 1991-1997. These papers form some of the conceptual principles of Blockchain and propose a way to digitally time stamp intellectual property documents in chronological order to provide ownership protection. In 1990, Stornetta got his idea at a Friendly’s restaurant in Morristown, New Jersey. He realized his system could have many dispersed but interconnected copies of a shared ledger. The time stamp would be a hash code with each hash dependent on the ones preceding it in the chain. The block’s data could not be altered without affecting all the other blocks chained to the one in question. As an additional precaution, they advocated publicly publishing the sequence of records, so data could be reviewed and verified by any third party, effectively crowd-sourcing the verification process. Working at Bellcore, Stornetta and Haber let the patent lapse in 2004, before the inception of Bitcoin.

Blockchain is a distributed ledger software technology that forms the underlying platform of Bitcoin. Transactions are clustered into chronologically chained blocks of data using a hashing algorithm that makes the record immutable. Prior to the person or people referred to as Nakamoto, Nick Szabo designed a system in 1998 called “bit gold.” [2] It has been described as a direct precursor to Bitcoin. He said he was trying to mimic in cyberspace the trust and security characteristics of gold. The problem Szabo was trying to solve was that our money currently depends on trust in a third party for its value which is not an ideal state of affairs as evidenced with the 2007-2008 Financial crisis. Szabo has proposed using blockchains for “smart contracts” and Bitcoin provides a Turing-incomplete Script language that allows the creation of smart contracts.

In 2008, Nakamoto published the source code for Bitcoin on SourceForge. (later provide architecture for initial code and other implementations). This proliferated the use of blockchain technology and hyperledger fabric substrate in applications today. Currently there are many open-source blockchain frameworks, we will explore a few such as Bitcoin, Ethereum, RootStock, EOS.

Current use cases for blockchain include public health, financial, customs declarations, payment and digital currency, supply chain, identity, fraud prevention, trade network, insurance, clinical trail management, food safety, dispute resolution, private equity networks, distributed energy source/power grid, asset management, carbon credit management.

# Tutorial

## What is Blockchain?

A blockchain is a chain of digital blocks that contain sensitive information, typically financial. The blockchain protocol is used to transfer or exchange the sensitive information that is contained in its blocks securely between two parties without the need for a third party such as a bank or a government entity.



Fig. 2. A chain of digital blocks. The first block is referred to as Genesis.

A blockchain is essentially a distributed database that is shared across a large network with many nodes/computers. All transactions or digital events including updates that have been executed are automatically shared and downloaded to every node on the network. Each transaction is verified by consensus of most of the participating nodes in the system. And, once entered, information can never be erased.

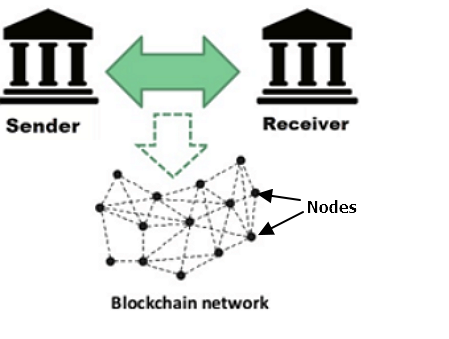


Fig. 3. Blockchain network support exchanges between two parities

The blockchain contains a certain and verifiable record of every single transaction ever made. Thus, once a transaction is executed, data is recorded inside a blockchain rendering them, i.e. the data, temper proof and impossible to hack into.

The only way a hacker may be able to make changes is to hack into more than half of the nodes that make up the blockchain. That is why it’s important to have many nodes involved in running the blockchain; more nodes means better security.

## What is not a Blockchain?

Blockchain is not Bitcoin, but it is the technology behind Bitcoin. Bitcoin is the digital token and blockchain is the ledger to keep track of who owns the digital tokens. Blockchain is the technology that is used by Bitcoin to allow secure, public and anonymous transactions to take place.



Fig. 4. Blockchain is not Bitcoin

To simplify, we can think of blockchain as an operating system (like Windows or Mac OS) and Bitcoin as an application that runs on that operating system. We can't have Bitcoin without blockchain (an application needs an OS to work) but, we can have blockchain without Bitcoin (the operating system does not need applications).

## How does a Blockchain transaction work?

Fig. 5. Blockchain transaction process

## Blockchain Architecture

As mentioned above, a blockchain is made of chained blocks, but what is a block? A block can be thought of as the pages in a ledger book where transactions are recorded. Blocks are organized into a linear sequence over time, which is also known as the block chain. New transactions are constantly being processed by miners into new blocks which are added to the end of the chain. As blocks are buried deeper and deeper into the blockchain, they become harder and harder to change or remove. This gives rise of bitcoin's irreversible transactions.

The data which is stored inside a block depends on the type of blockchain. There are mainly three types of blockchains that have emerged after Bitcoin introduced blockchain to the world.

1. Public Blockchain
2. Private Blockchain
3. Consortium or Federated Blockchain

A Bitcoin Block contains information about the Sender, Receiver, number of bitcoins to be transferred. It also contains a hash which can be thought of as a fingerprint which uniquely identify each block. So once a block is created, any change inside the block will cause the hash to change. Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it no longer remains the same block that it once was.

## Chaining the blocks for security

### Hash

The following example clarifies a blockchain. Consider a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain the hash of the previous block. Block 2 contains a hash of block 1. While block 3 contains the hash of block 2

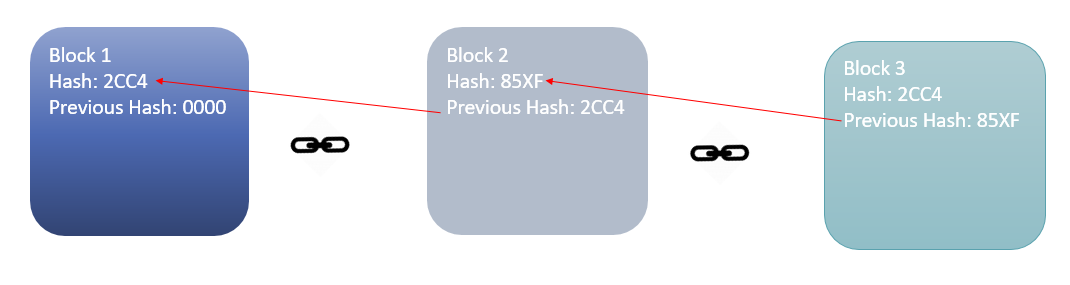


Fig. 6. Chaining the blocks via hash

Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain secure. Assume an attacker can change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have the correct hash from the previous block. Therefore, changing a single block can quickly make all following blocks invalid.

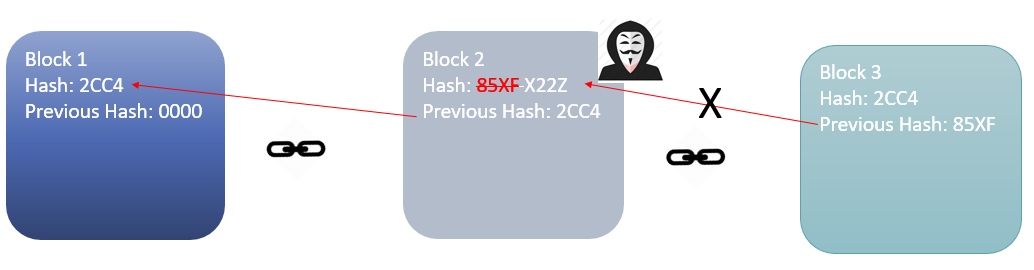


Fig. 7. Chaining anything in a clock invalidates the following blocks

### Proof of Work

Hashes are an excellent method to try to prevent changes to information found in a block, however, with the computational power of today’s computers, hundreds of thousands of hashes can be calculated per second. This allows a hacker / attacker to tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again in a matter of few minutes.

To circumvent this problem, blockchains use the concept of Proof-of-Work (POW). POW is a mechanism which slows down the creation of the new blocks by introducing a computational problem that takes significant effort to solve. The time required to verify the results of the computational problem is less than the effort it takes to solve the computational problem itself.

In the case of Bitcoin, it takes almost 10 minutes to calculate the required POW to add a new block to the chain. Considering the previous example, if a hacker were to change data in Block 2, he/she would need to perform POW (which would take 10 minutes) and only then make changes in Block 3 and all the succeeding blocks.

This kind of mechanism makes it quite tough to tamper with the blocks. Even if only a single block was tampered with, POW would still have to be performed for all following blocks. Thus, hashing and POW mechanisms make blockchain secure.

### Distributed P2P Network

There is an additional method which is used by blockchains to secure themselves, and that's by being distributed. Instead of using a central entity to manage the chain, blockchains use a distributed peer-to-peer network, which everyone can join. When someone enters this network, he/she will get the full copy of the blockchain. Each computer is called a node.

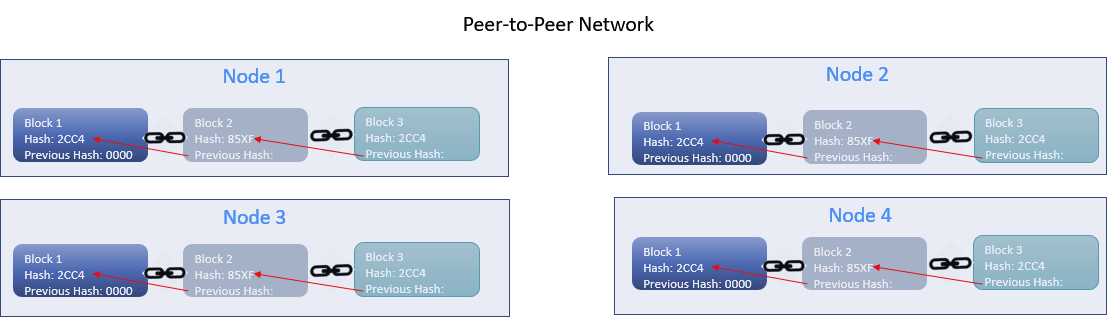


Fig. 8. Peer-to-Peer network node representation

When a new user creates a block, this new block is sent to all the users on the network. Each node needs to verify the block to make sure that it hasn't been altered. After complete checking, each node adds this block to its blockchain.

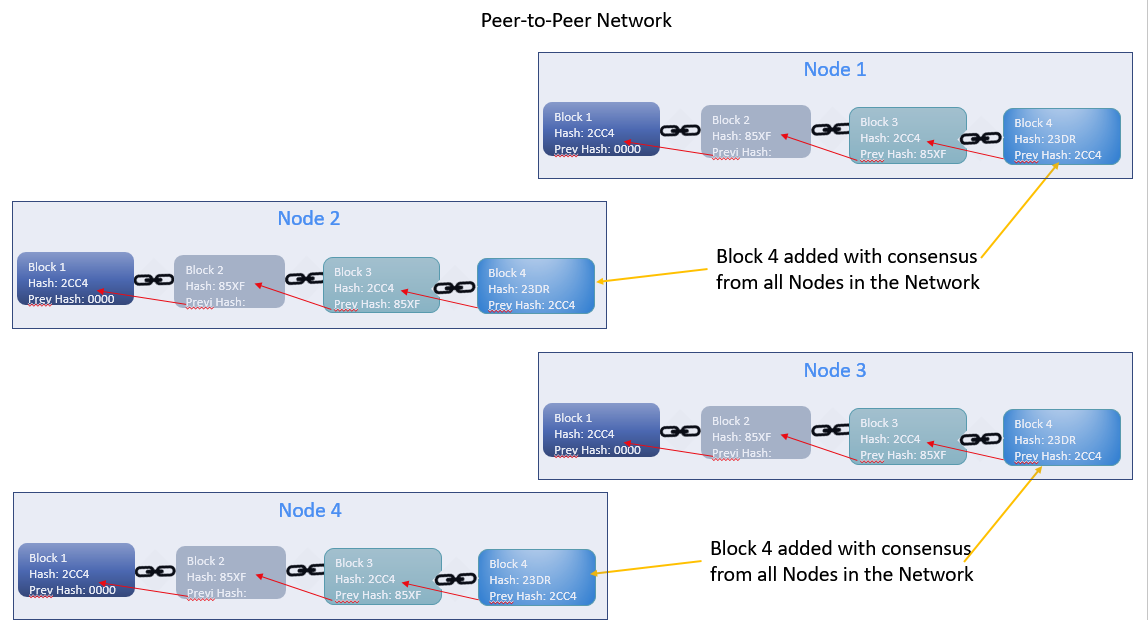


Fig. 9. Peer-to-Peer network node representation with consensus

All nodes in this network create a consensus. They agree about what blocks are valid and which are not. Nodes in the network will reject blocks that are tampered with. So, to successfully tamper with a blockchain:

1. All blocks in the chain must be tampered with
2. The proof-of-work must be redone
3. 50% of the peer-to-peer network must be taken control of

After completing these three steps, a tampered block becomes accepted by everyone else. This is a next to impossible task. Hence, blockchains are very secure.

# Future of blockchain

The potential uses for blockchain technology go well beyond financial transactions. These use cases include:

* A reliable recording of the truth
* A distributed recording with no single point of failure
* Anonymity of the participants (or not)
* Irreversibility; such as is common in financial transactions. When an error transaction occurs, the error is not deleted or removed but an additional transaction to negate the incorrect transaction is recorded.
* Automated transactions; workflows for example. Worker A completes a task and the work object is queued to worker B and so forth.

Experiments in this space tend to be in early stages, but they range from medical records, digital rights, and identity and supply chain management [4].

## Medical Records

MedRec is a proposal from M.I.T which would enable patients to own their medical records, therefore presumably removing an intermediary. Smart contracts act as an intelligent representation that link patients and providers to the addresses of existing medical records. Medrec does not ‘store’ the record directly; it rather encodes metadata that allows records to be accessed securely by patients, unifying access to data across disparate providers. The metadata contains information about ownership, permission, and the integrity of the data being requested. The full details of the smart contract structure and operation can be found in MedRec’s technical documentation [5].

## Digital Rights and Micropayments

The Brave Browser aims to “fix the web by giving users a safer, faster and better browsing experience” [6]. Brave is an open source web browser built by a team of privacy focused pioneers of the web. It aims to make browsing faster and private by blocking ads and trackers by default. They intend to enable users to opt into receiving some ads or donate to publishers. When ads are enabled they will be fewer but higher quality. Even if a user opts into receiving ads, trackers will still be blocked and privacy will still be protected.

## Identity

Uport is an Ethereum address. So if all that is needed when interacting with an end user is their Ethereum address, this is provided by uPort. However, uPort also allows apps and their users to exchange information privately, while still backed by the security of the Ethereum blockchain [7]. In more detail, a uPort identity is a complete digital representation of a person (or app, organization, device, or bot) that is able to make statements about who they are when interacting with smart contracts and other uPort identities, either on-chain or off-chain. This ability to make statements about themselves, without relying on centralized identity providers, is what makes uPort a platform for self-sovereign identity. The real power of uPort is that it makes the Ethereum app more approachable to end users. Some of the interactions enabled by uPort are simple blockchain transactions like buying shares on the Gnosis prediction market, while others include off-chain interactions, such as making private statements to other uPort users or apps. All of this is possible without end users having to endure complex key management.

References

1. Nakamoto, Satoshi. "Bitcoin: A peer to peer electronic cash system. "(2008). http://bitcoin.org/bitcoin.pdf
2. Szabo, Nick. “Bit gold”. (2005).

https://unemumerated.blogspot.com/2005/12/bit-gold.html

1. Szabo, Nick. “Money, blockchains, and social scalability” (2017).

http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html

1. C. Catalini. (2017, Mar.). How Blockchain Applications Will Move Beyond Finance. *Harvard Business Review.* [Online]. *11(7)*. Available: [https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance](http://www.halcyon.com/pub/journals/21ps03-vidmar).
2. MedRec. (2018, Oct.). What is MedRec?. *MIT MedRec Team.* [Online]. *9(4)*. Available: https://medrec.media.mit.edu
3. Brave (2018, Oct.). About Us. *Brave Team.* [Online]. *3(2)*. Available: https://brave.com/about/
4. P. Braendgaard. (2017, Feb.). What is a uPort identity?. *Uport.* [Online]. *3(2)*. Available: https://medium.com/uport

1. This paragraph of the first footnote will contain the date on which you submitted your paper for review. It will also contain support information, including sponsor and financial support acknowledgment. For example, “This work was supported in part by the U.S. Depart­ment of Com­merce under Grant BS123456”.

   The next few paragraphs should contain the authors’ current affiliations, including current address and e-mail. For example, F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

   S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

   T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp). [↑](#footnote-ref-1)