**Abstract:**

A **blockchain** facilitates **secure** online transactions. A **blockchain** is a decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. Employing blockchain also reduces the cost of online transactions while simultaneously increasing authenticity and security. These benefits are amongst the prime reasons why the technology is being extensively deployed within the banking sector. 

Blockchain technology is being used to protect sensitive records and to authenticate the identity of a user. Keyless Security Infrastructure (KSI) stores data hashes on blockchains and runs a hashing algorithm for their verification.

Public Key Infrastructure (PKI), an encryption approach which is particularly vulnerable to man-in-the-middle and DDoS attacks, is therefore deleted out of the equation. Any data manipulation can be easily spotted as the original hash is available on other nodes linked to the system, enabling banks to go beyond asymmetric encryption and caching in public keys. 

**CHAPTER 1 - HISTORY**

Many of the technologies we now take for granted were quiet revolutions in their time. We’re now in the midst of another quiet revolution: [blockchain](https://en.wikipedia.org/wiki/Blockchain_(database)), a distributed database that maintains a continuously growing list of ordered records, called “blocks.” Consider what’s happened in just the past 10 years:

#### ****Altcoins****

The first trend of experimentation saw the creation of altcoins in 2013 and 2014. Most of these altcoins were technically very similar to bitcoin, with a few tweaks, maybe a new feature, and some fresh branding.

Some of these altcoin protocols have survived and thrived over the last 4 years, while others have failed. Those that have gained and retained value have found product-market fit in two ways: either the asset has met an economic need or the protocol has met a technological demand.

#### ****Permissioned Blockchains****

In 2015 and 2016, as many altcoins lost momentum, the second wave of blockchain innovation took off. Rather than generating new assets, this wave focused on assets that already existed.

This concept of porting existing assets into new formats is at the heart of what permissioned blockchain technology attempts. Operating within a closed environment helps get us part of the way there.

This second wave of blockchain experimentation also tries to move physical assets onto a blockchain. This has been applied to everything from shoes, to homes, to diamonds, to pork bellies, to art. One illuminating point here is that the world has a major tracking problem. Maintaining a record of the existence and ownership and authenticity of physical goods, it turns out, is something we are very bad at.

#### ****Tokens****

Which brings us to the third wave of blockchain experimentation. The market has returned to a trend of creating new assets, this time rebranded as tokens. Tokens are new natively digital assets that creators attempt to imbue with value.

Tokens differ from altcoins in that their value attempts to be derived in more traditional ways. They might, for example, represent a claim on returns of a project or set of ventures. (In traditional finance, this would be called a share or an LP interest, but never mind that.) Blockchain Capital’s token and the Ethereum DAO are obvious examples here.

## CHAPTER 2- INTRODUCTION

### A blockchain is a digitized, decentralized, public [ledger](https://www.investopedia.com/terms/g/generalledger.asp) of all[cryptocurrency](https://www.investopedia.com/terms/c/cryptocurrency.asp) [transactions](https://www.investopedia.com/terms/t/transaction.asp). Constantly growing as ‘completed’ [blocks](https://www.investopedia.com/terms/b/block-bitcoin-block.asp) (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is downloaded automatically.

### Originally developed as the accounting method for the virtual currency [Bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp), blockchains – which use what's known as [distributed ledger](https://www.investopedia.com/terms/d/distributed-ledgers.asp) technology (DLT) – are appearing in a variety of commercial applications today. Currently, the technology is primarily used to verify transactions, within digital currencies though it is possible to digitize, code and insert practically any document into the blockchain. Doing so creates an indelible record that cannot be changed; furthermore, the record’s authenticity can be verified by the entire community using the blockchain instead of a single centralized authority.

### main-qimg-a603db93d8791ac9d785fc8cbeef127e

### Fig 1 : CREATION OF NEW BLOCK

### A block is the ‘current’ part of a blockchain, which records some or all of the recent transactions. Once completed, a block goes into the blockchain as a permanent database. Each time a block gets completed, a new one is generated. There is a countless number of such blocks in the blockchain, connected to each other (like links in a chain) in proper linear, chronological order. Every block contains a hash of the previous block. The blockchain has complete information about different user addresses and their balances right from the genesis block to the most recently completed block.

### The blockchain was designed so these transactions are immutable, meaning they cannot be deleted. The blocks are added through cryptography, ensuring that they remain meddle-proof: The data can be distributed, but not copied. However, the ever-growing size of the blockchain is considered by some to be a problem, creating issues of storage and synchronization.

## The idea of decentralization:

By design, the blockchain is a decentralized technology.

Anything that happens on it is a function of the network as a whole. Some important implications stem from this. By creating a new way to verify transactions aspects of traditional commerce could become unnecessary. Stock market trades become almost simultaneous on the blockchain, for instance — or it could make types of record keeping, like a land registry, fully public. And decentralization is already a reality.

A global network of computers uses blockchain technology to jointly manage the database that records Bitcoin transactions. That is, Bitcoin is managed by its network, and not any one

central authority. Decentralization means the network operates on a user-to-user (or peer-to-peer) basis. The forms of mass collaboration this makes possible are just beginning to be investigated.

## A distributed database:

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

### Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn’t stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

### home

### FIG 2: Decentralized and Distributed Ledgers

**APPLICATIONS OF BLOCKCHAIN**

Bitcoin is just one of the applications of Blockchain. Now that we have understood the basic concepts, let us explore a few of the real-life applications of blockchain.

1. **Follow My Vote** aims to change the way we vote, becoming the world’s first open-source online voting solution.
2. **Arcade City** is the groundwork for a true decentralized ridesharing service often called the ‘Uber killer’.
3. **ShoCard** stores your identity onto Bitcoin’s blockchain for easy verification.
4. **Symbiont** is a provider of smart securities on the blockchain.
5. **Bitnation**is a “Governance 2.0” initiative with a collaborative platform for DoItYourself governance.
6. **ChainLink** uses blockchain technology to verify and validate the authenticity and title of real world items.

**CHAPTER 3 – WHY BLOCKCHAIN IS SECURE**

The blockchain’s relies on 3 major pillars, consensus, distributed, and trustless, and the security is derived from a proof of work problem. This problem is design to take a large amount of computational power to complete and thus, for a single person working it may take years but for a network of computers it may take only minutes. “Proofs of work that are tied to the data of each block are required for the blocks to be accepted. The [difficulty of this work](/what-is bitcoin-mining-difficulty/) is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes.”4 Thus, the chain can be continually added to and transactions are still processed in a timely manner while securing the data from tampering.

The nature of this problem makes it mathematically impossible for someone to change the blockchain. “Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain.”5 This could theoretically be done given enough time but the formerly mentioned public ledger is chosen by a consensus, where the network of users agrees on the longest blockchain to be the recognized chain.

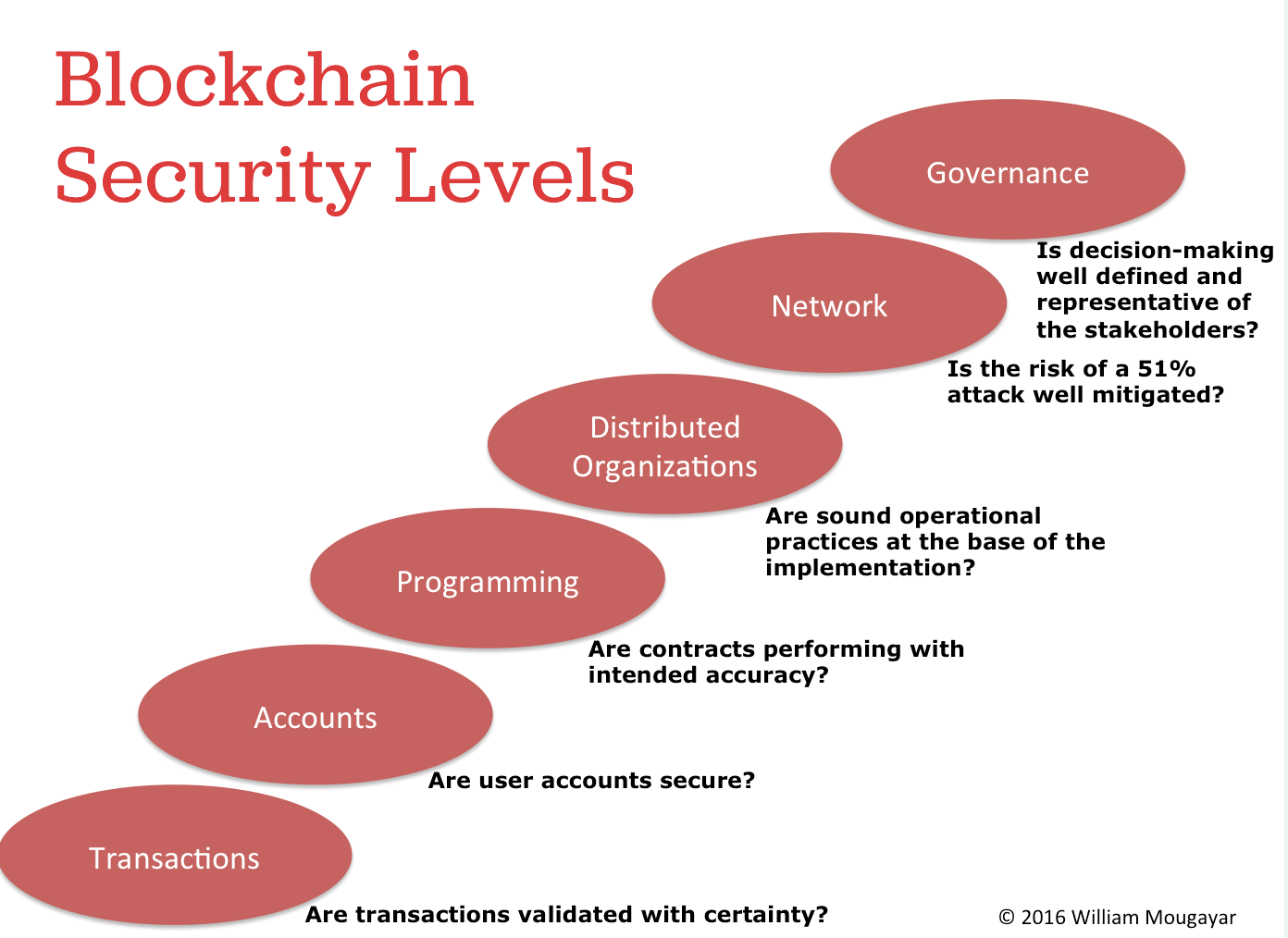
This makes up the first pillar of the blockchain. By agreeing on the longest blockchain, the only way for a user to successfully alter the chain would be to alter a block and then generate subsequent transaction blocks to make a new longest chain. However, the usage of a proof of work problem makes this mathematically impossible. Because the network of users will be adding blocks at a much faster rate than any single person could add blocks.

Thus, the security is trustless, meaning the security lies in preventing malicious parties from doing harm by nature of the protocol, without having to authenticate a transaction. Finally, the ledger is distributed, meaning that every user stores the current ledger, preventing someone from altering a single point of truth. In traditional cryptography, a single point of truth could be a certificate authority, however, if that certificate authority was to be breached, a malicious attacker could replace the stored keys with their own keys, thus enabling them to masquerade as a plethora of users. By distributing the ledger, an attacker would have to breach every member machine and replace the blockchain with their own making it functionally impossible for an attacker to alter the chain.

**CHAPTER 4 – SECURITY LEVELS**

# Six Categories of Security Layers

We should think of the various levels of blockchain security. All these layers should work together in order to deliver the highest possible security. The outcome will result in more public confidence, at similar levels as bank grade security.



**Fig 3: Security Levels**

## 1. Transaction Level

That is the minimum required level for a bonafide blockchain. A well functioning blockchain needs to validate transactions with certainty and predictability at the end of the consensus cycle. This is where the consensus method does its job of confirming the transaction finality. We have gotten pretty good at this level, but it’s in the remaining areas where more work is required.

## 2. Account Level

There are two parts to this. A user account could be self-managed via a private wallet, or it could be a hosted account at an exchange. The Bitfinex hack was an example of a hosted account hack, happened because accounts were compromised on the exchange. And on the private wallets side, the DAO replay attacks touched some DAO private wallets. This is the area where you “clients” are also vulnerable to Internet style DoS or phishing attacks. Self-managed wallets are not for the faint of heart, nor for the novice user, despite a plurality of Do’s and Don’ts that security experts will dispense. In order to deliver cryptocurrency to the masses, hosted exchanges and wallets providers have an important role to play, so they need to become really good at it. The analogy is Facebook. Facebook is not the Web. It is a walled garden, but it works well and it is arguably more secure than the Web at large.

## 3. Programming Level

This is where smart contracts or scripts could be compromised, and the DAO case was a perfect example in that category. Smart contracts could have vulnerabilities that can be exploited, resulting in a drainage or disappearance of funds. Vitalik Buterin provided an excellent explanation and classification of the known smart contract security categories, and this is an area where there is wide agreement that improvements are needed. The blockchain allowed us to program money, and we need to be careful in doing it.

## 4. Distributed Organizations Level

Think DAO here again, not at the smart contract level, but rather at the operational and organization level, and how a spaghetti topology of smart contracts labelled as “law” could become a house of cards for a Distributed Organization that wants to be autonomous.  Autonomy has its risks, but first and foremost, the organization itself must be tested and it must be sound before it gets a chance to run autonomously. The DAO tried too hard and relied only on technical curators who gave it a passing grade, but didn’t have organizational experts that could have pointed fundamental flaws in linking the operations of a company to blockchain contracts.

## 5. Network Level

A blockchain is a peer-to-peer network, physically and virtually. That network is where the consensus methods run, and this is the area where you hear of the 51% attack vulnerabilities, i.e. when theoretically, an attacker can spend enough money and hash power to “hijack” the transaction validation process in their favor. This category of security will concern itself with the soundness of the actual algorithms, protocols, incentives and consensus economics (whether mining or transaction costs related). In my opinion, the specter of “51% attacks” shouldn’t even be in our vocabulary. Imagine if a bank advertised the percentage likelihood of them being robbed as part of their marketing material.

## 6. Governance Level

I’m going on a limb in differentiating governance level security from the network level security because I’m referring here to the application side of decentralized consensus. This is an embryonic area, and we have only seen rare cases of decentralized governance. The ones we don’t hear about may be failing in obscurity, and we can’t easily extract their lessons, but the two most publicized cases are Bitcoin (block size) and Ethereum (hard fork) governance. Strategic decisions taken in the name of decentralized governance affect the long term security of a blockchain. We are still learning by trial and error as we figure out the best practices of decentralized governance. On one hand, Bitcoin could be criticized for being too rigid on governance related changes, whereas Ethereum could be perceived to have been a little too lax with their recent hard fork decision process. Maybe one day, the pendulum will swing to the middle.

Today, blockchain related robberies are more of the “cybercrime” flavor variety, because there is no physical entry into a bank or vault. It’s the hacking itself that makes these incidents possible. Crime, cybercrime, robbery, theft and hacks will continue to occur, regardless of the efforts, measures and practices of the criminal justice system. Therefore, the technology itself must do its part in being as good and as predictable as bank grade security.

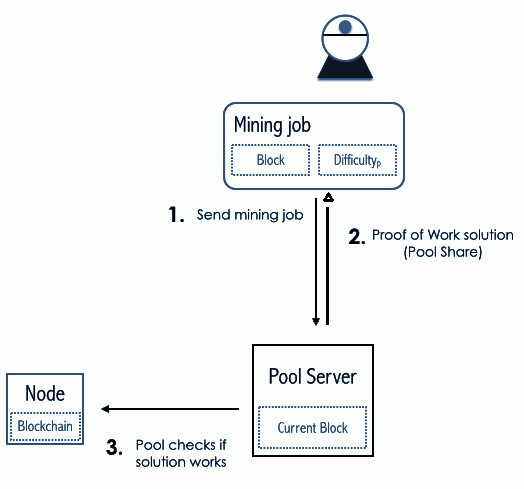
**CHAPTER 5 - MINING**

When a purchase is carried out, the ledger records it and sends it out to the entire network. Computers all over the world then compete to confirm the operation by solving complex math equations. The first to figure out the answer and validate the block receives a reward in Bitcoins this process is called **mining.**

The validated block is time stamped and added to a chain in chronological order. The entire chain is continually updated so that it’s always an accurate representation of who owns what at any given time.

Mining refers to the distributed computational review process performed on each "block" of data in a "block-chain".

This allows for achievement of consensus in an environment where neither party knows or trusts each other

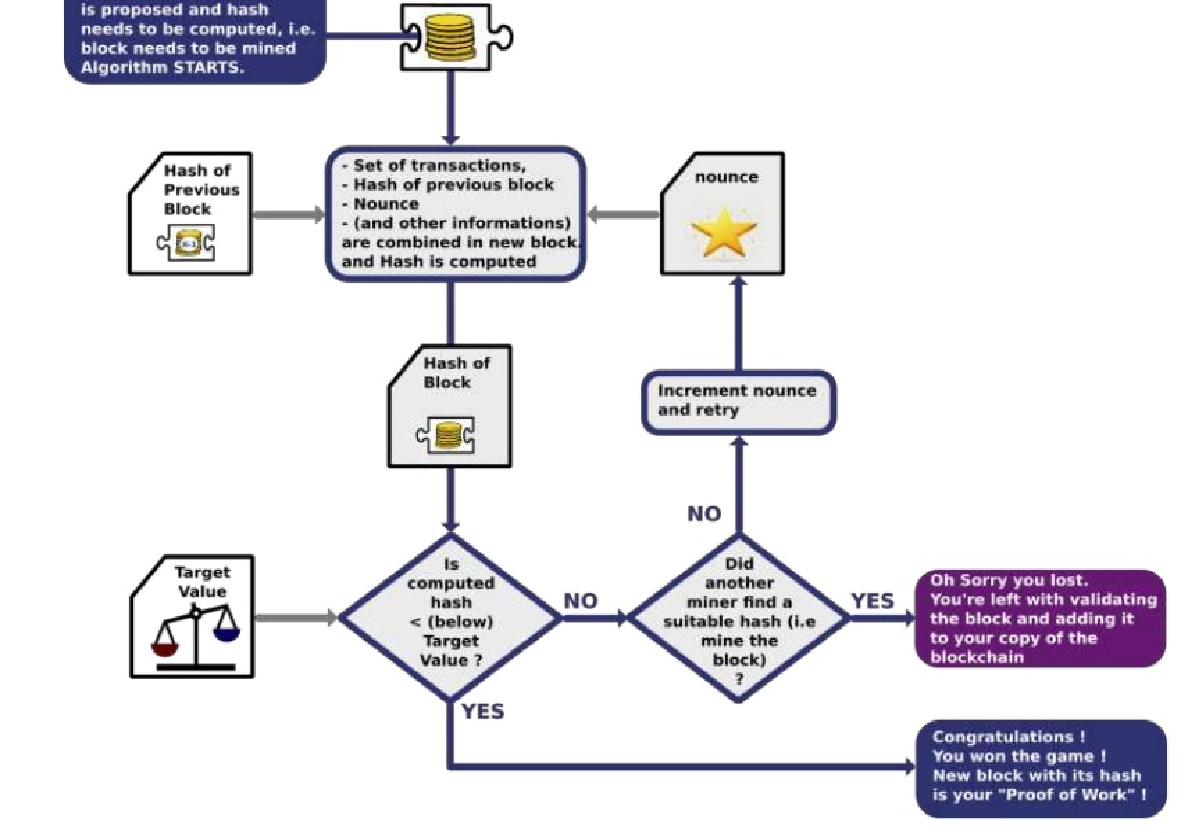
****

**Fig 4: Mining**

**Steps of mining process :**

* Central to Bitcoin is a public ledger, known as the Block Chain. for every 10 minutes, a new “block” is added to this chain or ledger.
* This ledger records all of the transaction about  what quantities of bitcoin currency are now held at different public addresses in the last 10 minutes.
* A public address is a 27 to 34 character string of uppercase, lowercase letters and the digits from 0 to 9. AKA base 58.
* Each public address has a corresponding private key. Whoever has this key, may spend the coins that are held at this private address. Private keys are 51 characters long in the same format as a public address.
* To spend an amount of bitcoin, you must use your private key to cryptographically sign the transaction and sending your bitcoin to another address.
* This message or transaction is then broadcast to the network, and the computers in the network begin working to write into the block chain or public ledger that your address no longer has the amount that was sent, but that that amount is now held  at the receiving address.
* Each new set of transaction is recorded on the block chain, every 10 minutes.
* All of the computers that are working to write new blocks to the block chain, are known as **miners.**
* These computers are all racing to solve a cryptographic puzzle, which is required to write the new block.
* The computer that solves the puzzle, and writes the new block receives an award of newly created bitcoin.
* This transparency is a large part of the value created by Bitcoin, in that the rate of creation, and current amount in existence is known.

**Mining Flow Chart:**

****

**Fig 5: Mining Flow Chart**

**CHAPTER 6 - CRYPTOGRAPHY**

## Cryptographic hash functions

A cryptographic hash function is a special class of hash functions which has various properties making it ideal for cryptography. There are certain properties that a cryptographic hash function needs to have in order to be considered secure. Let’s run through them one by one.

**Property 1: Deterministic**

This means that no matter how many times you parse through a particular input through a hash function you will always get the same result. This is critical because if you get different hashes every single time it will be impossible to keep track of the input.

**Property 2: Quick Computation**

The hash function should be capable of returning the hash of an input quickly. If the process isn’t fast enough then the system simply won’t be efficient.

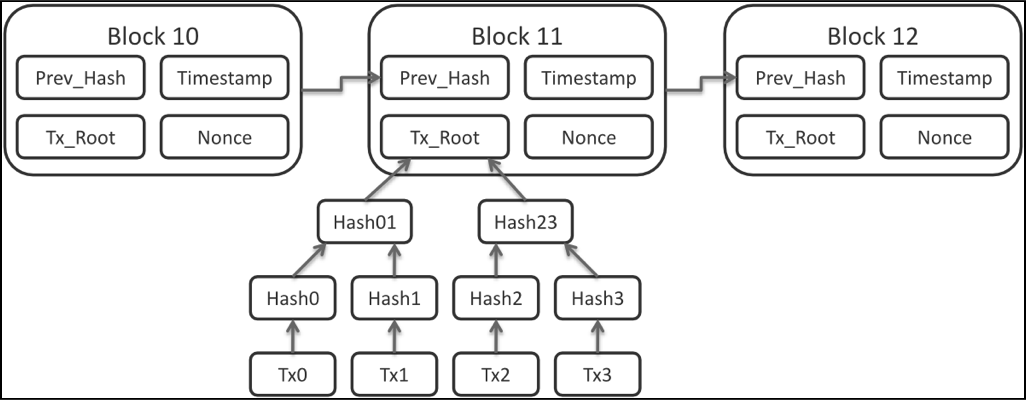
**Property 3: Pre-Image Resistance**

What pre-image resistance states is that given H(A) it is infeasible to determine A, where A is the input and H(A) is the output hash. Notice the use of the word “infeasible” instead of “impossible”. We already know that it is not impossible to determine the original input from its hash value. Let’s take an example.

Suppose you are rolling a dice and the output is the hash of the number that comes up from the dice. How will you be able to determine what the original number was? It’s simple all that you have to do is to find out the hashes of all numbers from 1-6 and compare. Since hash functions are deterministic, the hash of a particular input will always be the same, so you can simply compare the hashes and find out the original input.

**HASH RATE**

Hash rate basically means how fast these hashing operations are taking place while mining. A high hash rate means more people and software machines are taking part in the mining process and as a result, the system is running smoothly. If the hash rate is too fast the difficulty level is increased. If the hash rate becomes too slow then the difficulty level is decreased.



**Fig 6: Cryptography**

**CHAPTER 7 – PROOF OF WORK**

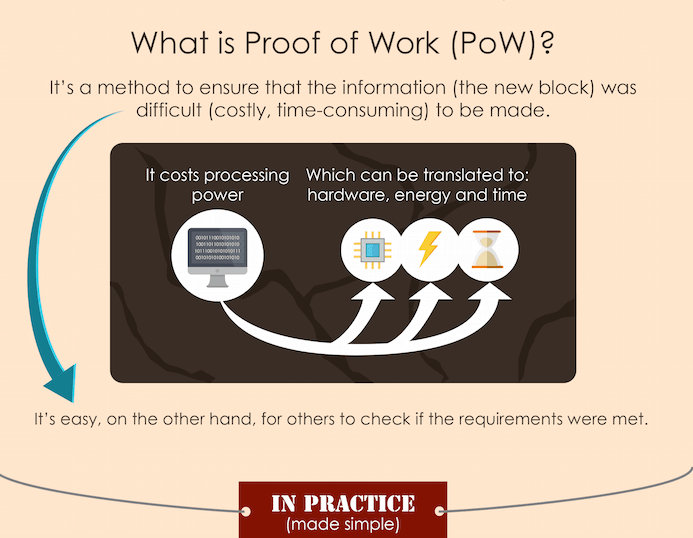
Proof of work is a requirement that expensive computations, also called mining for reasons which later will become clear, be performed in order to facilitate transactions on the blockchain. To understand the link between computational difficulty and trustless consensus within a network implementing a distributed cryptocurrency system is a serious mental feat. With this writing I hope to help those who are attempting it.

Because distributed trustless consensus is the primary innovation of blockchain technology, we start by understanding what it is. As the term suggests, there are three parts to the puzzle: (1) consensus, (2) distributed, and (3) trustless. Having explained the three terms, I will synthesize them by illustrating the problem that arises when you put all three together.

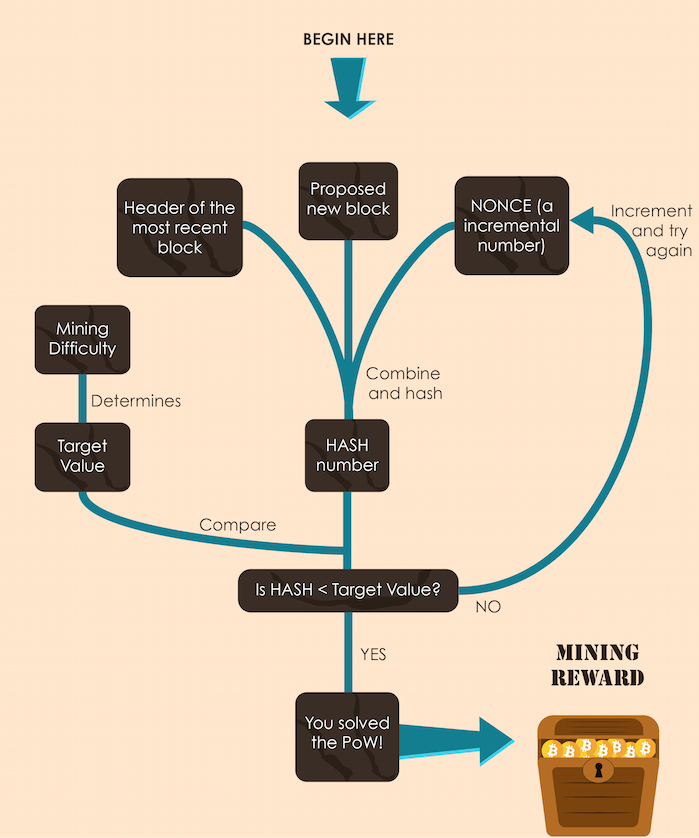
A digital transaction is some event or process whose effect is to transfer money in the sense we laid out in Cm. Putting together our understanding of consensus around money with our idea of trust, we can now list the requirements we have placed on such process so far (we will refer to them as Tx).

In order for our digital monetary system to work, the recipient of a transaction must be able to confirm that:

1. The originator of the transaction is in possession of the funds being transferred.
2. The originator of the transaction has obtained the funds by one of the means commonly recognized as valid.
3. As an outcome of the transaction the recipient will now be recognized by everyone as being in possession of the funds being transferred.
4. As an outcome of the transaction the sender would not be able to present itself as being in possession of the funds any more.

****

**Fig 7: Proof of Work**

****

**Fig 8: Mining Reward**

**CONCLUSION**

Blockchain technology can also play a pivotal role in securing internal communications, which are prone to data leaks and cyberespionages. End-to-end encryption fails to cover the metadata - something which can lead to leakage of sensitive information. In blockchain-based systems, the metadata used for communications is scattered in the distributed ledger and cannot be collected at one centralized point.   
  
Blockchain has emerged as one of the most disruptive technologies and has minimized the prevailing security issues in financial transactions. As other viable implementations for the technology are being explored, blockchains are coming to fore as top-contenders for solving an array of cyber security challenges and providing end-to-end security to banking institutions. 

Though blockchain has several advantages over other systems, there are still a few challenges in terms of compliance, regulations and enforcement that will need to be addressed. For example, regulatory issues demand clarity over jurisdictions and how to comply with KYC (Know your customer) and AML (anti - money laundering) laws. But the increasingly growing demand and acceptance by enterprises would help overcome these challenges sooner than anticipated. 

**REFERENCES**

<https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html>

<https://allquantor.at/blockchainbib/pdf/wust2016security.pdf>

<https://www.coindesk.com/information/how-bitcoin-mining-works/>