"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." – Sun Tzu, The Art of War

Cyber attacks: Availability

DDoS Attack

- Amazon Web Services
  - 2.3 Tbps
- GitHub, a software development platform (2018)
  - 1.35 Tbps
- Dyn, a DNS service provider to major websites (Oct 2016)
  - 1.2 Gbps
  - mounted by a botnet Mirai connecting 100000 IoT's

Single point of failure

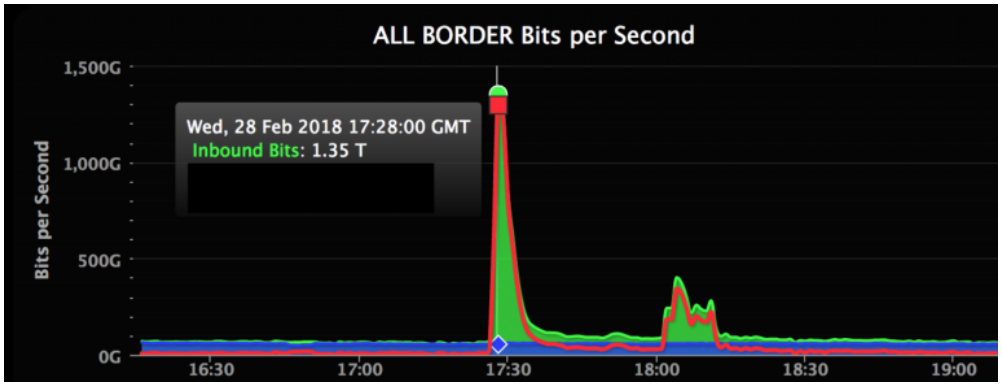
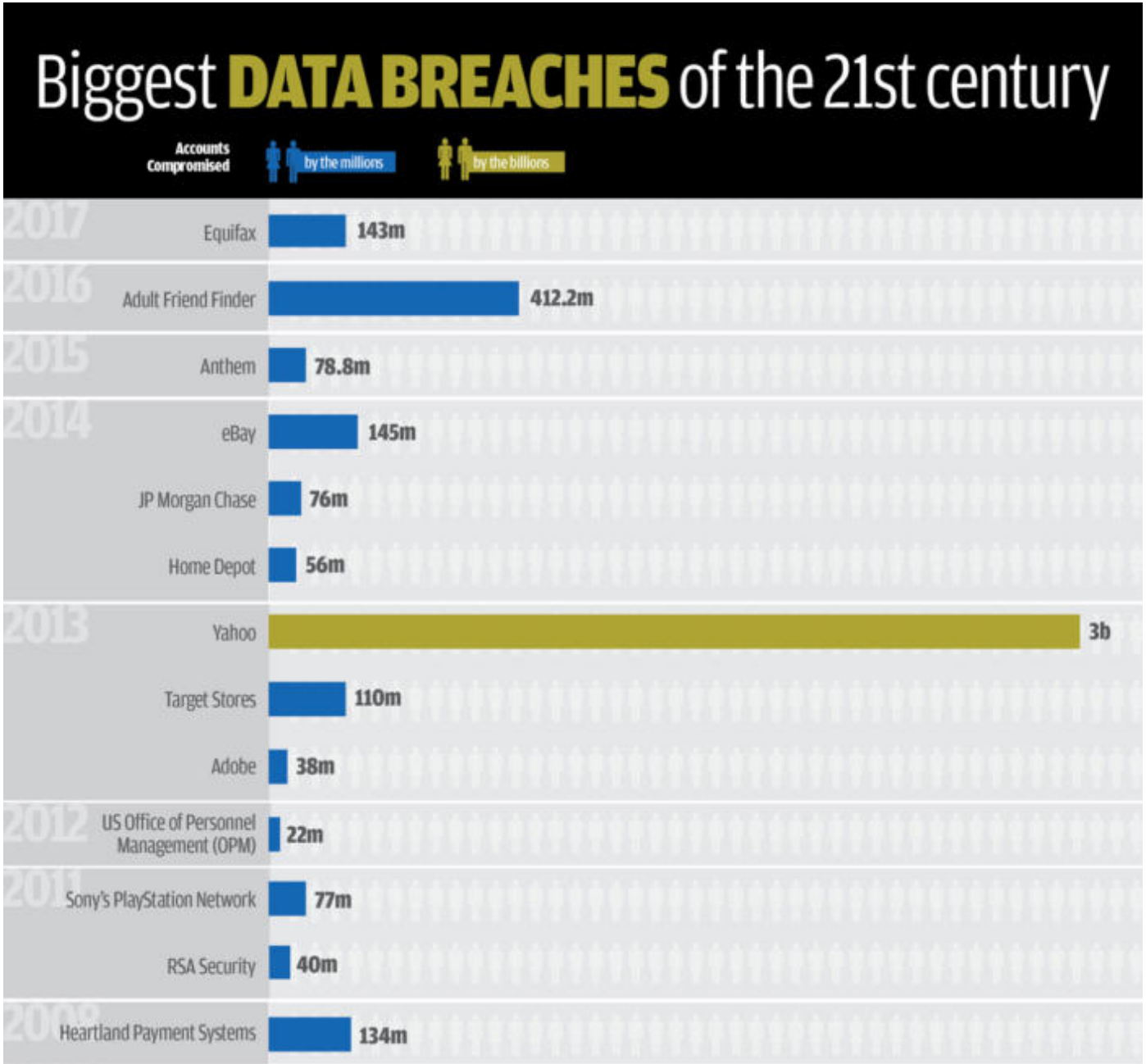


Image:https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

Cyber attacks: Data Theft



Attacks are becoming severe

Data Theft to Data Manipulation

Cyber attacks:Data Manipulation

- Hackers use the stuxnet worm to make minor changes in Iran's nuclear program in an attempt to destroy it
- Hackers infiltrate the Brazilian governments systems and inflate the logging quotas to disrupt the logging industry
- A Syrian group hacked into the Associated Press Twitter account and tweeted that President Obama had been injured in explosions at the White House the single tweet caused a 147 point drop in the Dow
- JP Morgan Chase was breached with subsequent attempts at market manipulation
- Both the World Anti-Doping Agency and Democratic National Committee are breached with hackers manipulating their data to embarrass the organisations

Blockchain

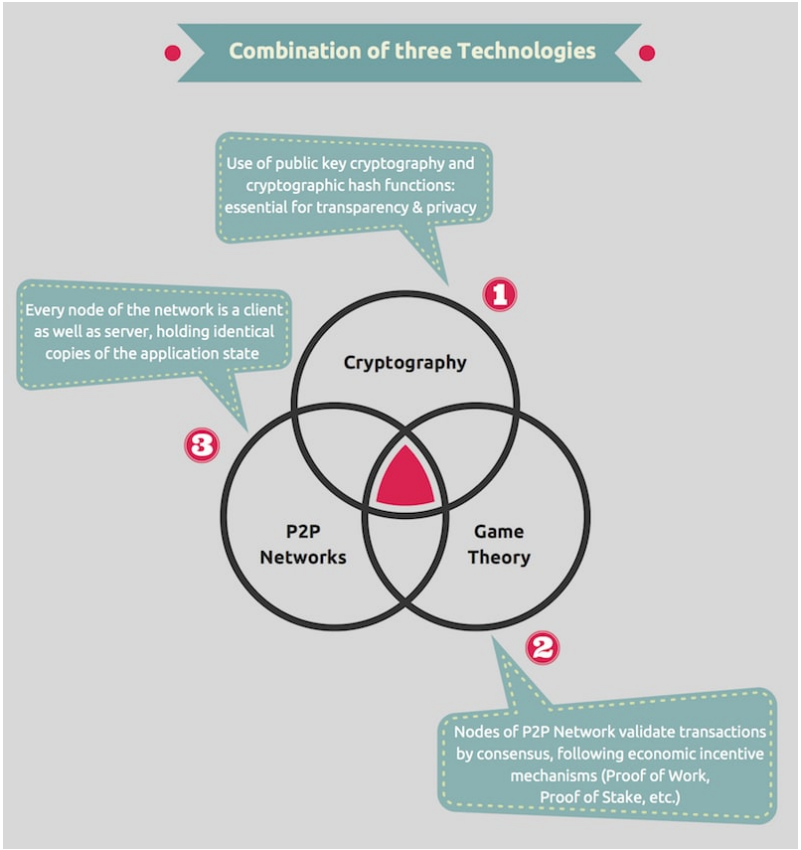


Image:blockchainhub.net

Next line of defense for cybersecurity ?

Blockchain

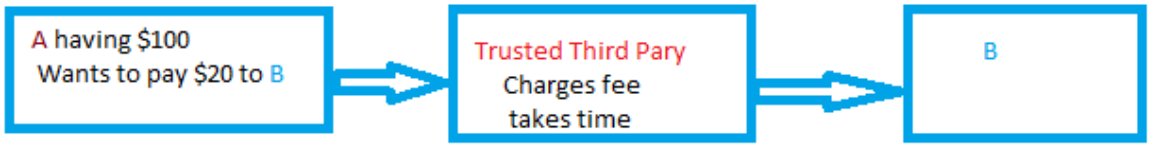
- One of the greatest innovations of the 21st century
- Operates on top of the Internet, on a P2P network of computers that all run the protocol
- Blockchain itself a file - a shared and public ledger of transactions that records all transactions from the genesis block (first block) until today.

A Solution

- Solution to the age-old human problem of Trust ?
- Allows us to trust the outputs of the system without trusting any actor within it

Distributed Ledger

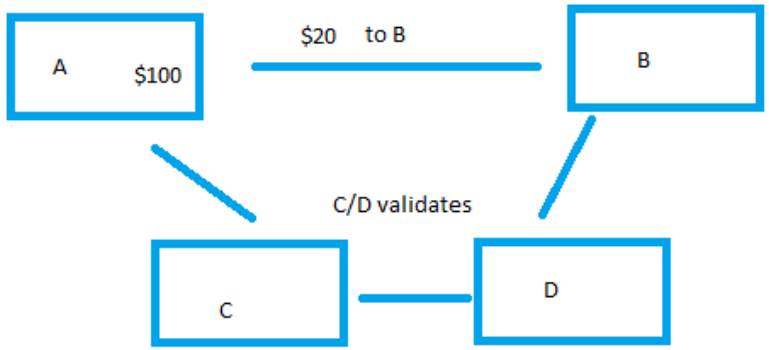
A distributed ledger allows the database of transactions to be available at multiple locations, unlike a traditional centralized database, where a central authority is involved.



characteristics of Traditional Ledgers:

- Centralization: It has a central authority that governs the data and user access permissions, thus, ensuring security.
- Single point of Failure: If the governing authority is compromised, the database is exposed to huge risk and failure.
- Validity of transactions: The central authority is responsible for validation of all transactions, thus, being the only gatekeeper of trust.

Distributed Ledger



Characteristics of Decentralised Database:

- Open and Public: Everyone in the network has access to the ledger and transaction data as it is stored at all nodes in the network. Hence, it is public and the information is easily accessible.
- Distributed risk: The power and access are distributed across all the participants in the network making it difficult for hackers to tamper with data.

Blockchain: Key Properties

- Immutable: impossible to edit past data stored in a blockchain. An append-only log.
- Decentralized: No single entity should have authoritative control over what data gets onto the blockchain.
- Distributed, typically over P2P networks

Image:https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

Chain of chronologically listed back-linked sequence of blocks denoting the changes to the state of the system

Block Creation

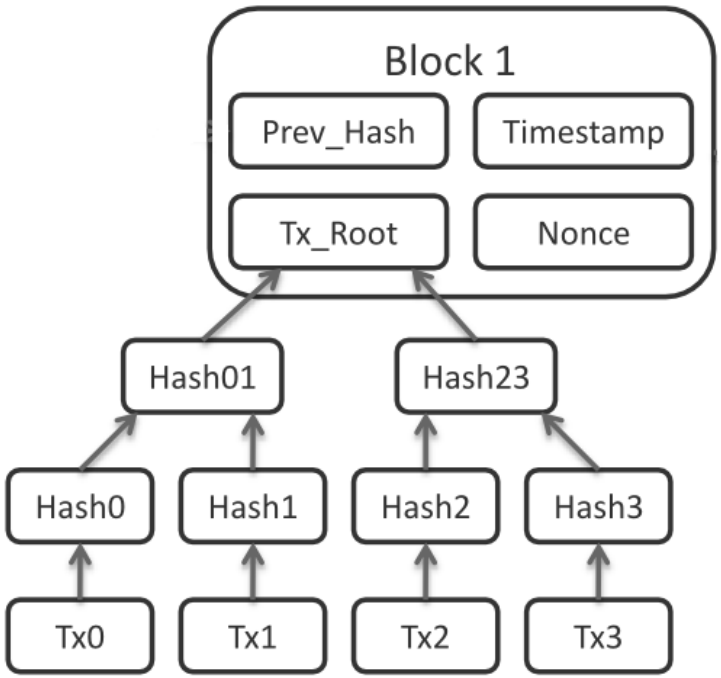
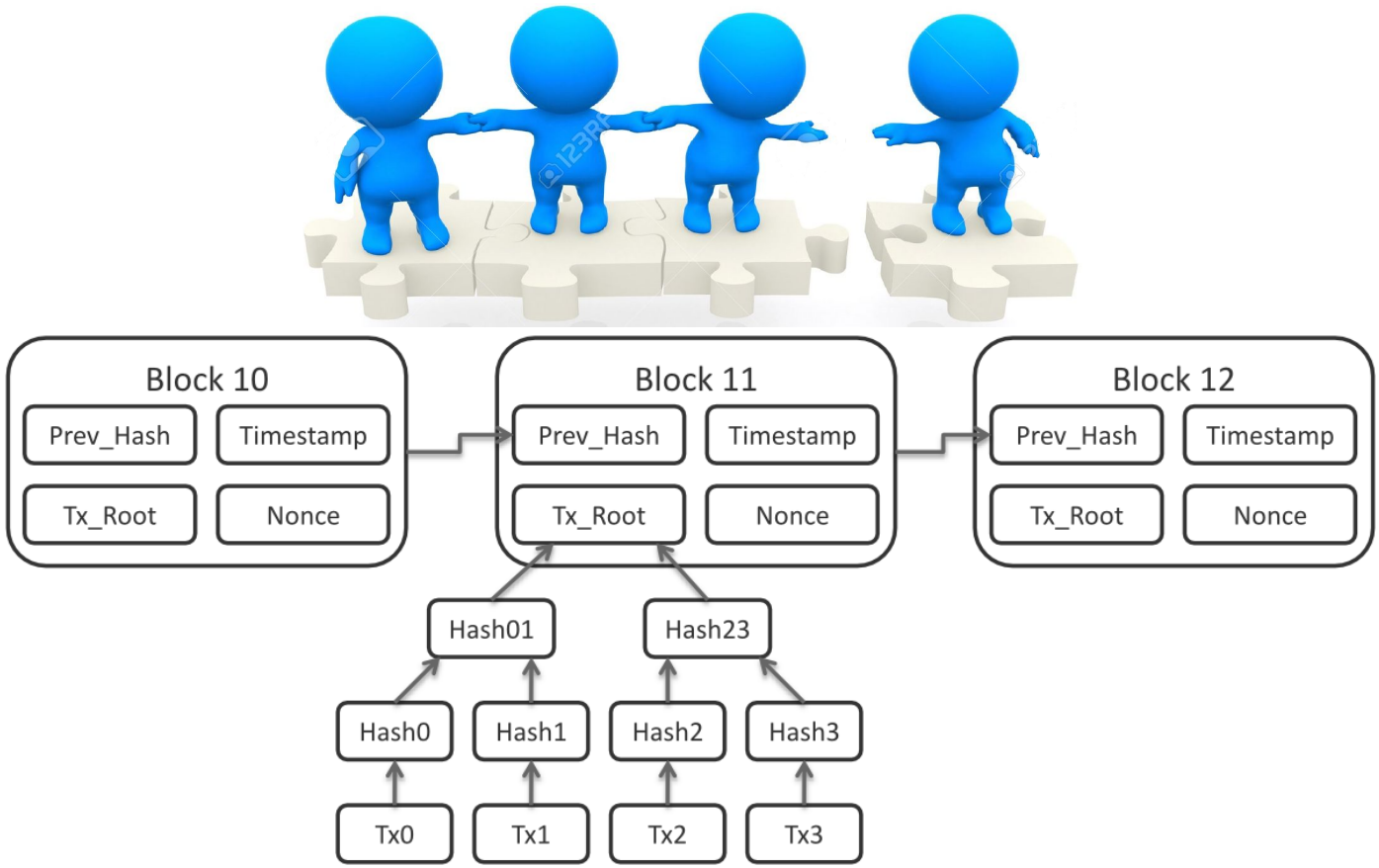


Image:Wikipedia

A linked list with hash pointers instead of ordinary pointers

Blocks forming a Chain



This is nothing new; distributed databases have been around for at least a decade before Bitcoin.

Block Creation

- easiest part!!
- a sequence of blocks
- nobody can alter the contents/order of the block
- the hash of the previous block becomes part of the next block
- onewayness property

all blockchain achieve it in the same way: Tamperproofness

Choosing the next block

Blockchain's major challenge is choosing the next block

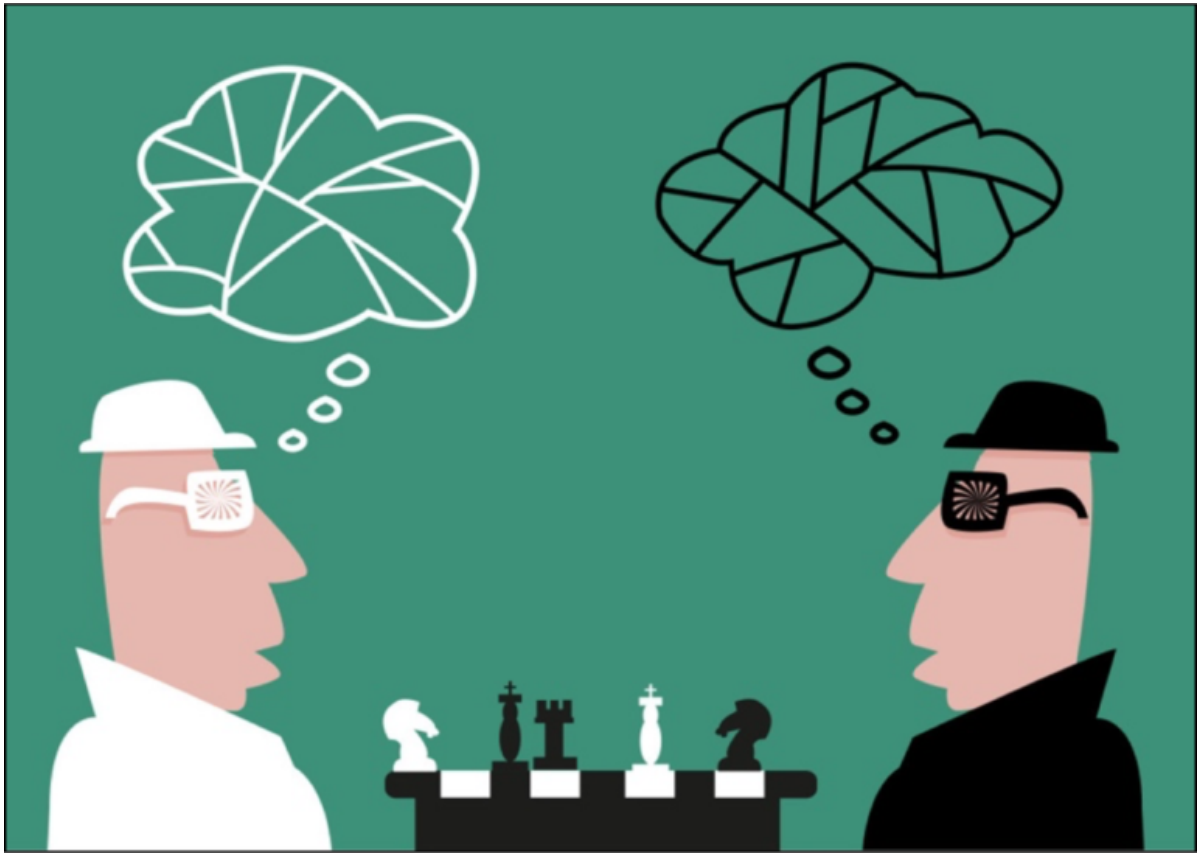
- Creation: Who can create what data?
- Dissemination: To whom the data be disseminated ?
- Storage: Who can store what data?
- Modification: Who can modify what data? (includes updating and deletion)
- Access: Who can access what data?

How to choose the next block?

- Mining: How blocks containing valid transactions are added to the blockchain??
- The magic is not in the data storage technology, but how untrusted users of the network can all reach consensus.
- The magic of "blockchain" isn't "a blockchain"; it's the Proof to achieve consensus :

Image:https://www.linkedin.com/pulse/10-elements-blockchains-ilustrated-bruno-ricardo-ferreira

- The double spending problem is the main breakthrough that Bitcoin made.



Game theory is the study of strategic decision making.

Model

The model has the following components;

- Players: The decision makers.
- Rules/strategies: The decision the players want to make to maximise their benefit.
- Payoff: Outcome of the strategies.

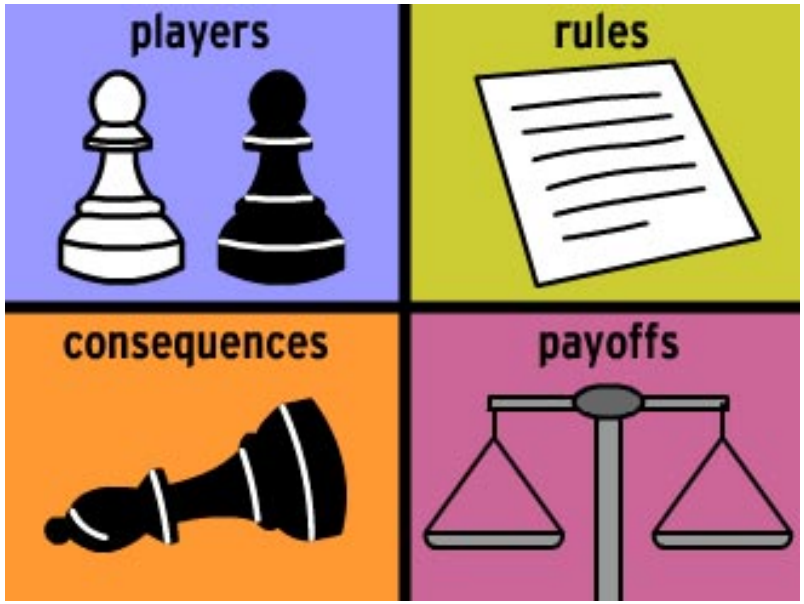


Image:http://www.exinfm.com/board

A game is any interaction between multiple persons in which each person's payoff is affected by the decisions made by the others

Game Theory Contd.

Main branches

- Cooperative
- Noncoperative or competitive: covers competitive social interactions

Types of Game

- Zero-sum game: gain of one player comes at the expense of the other
- Non zero-sum game: gain of one player doesn't come at the expense of another player.

A Thought Experiment in Competitive Game theory;Prisoner's Dilemma

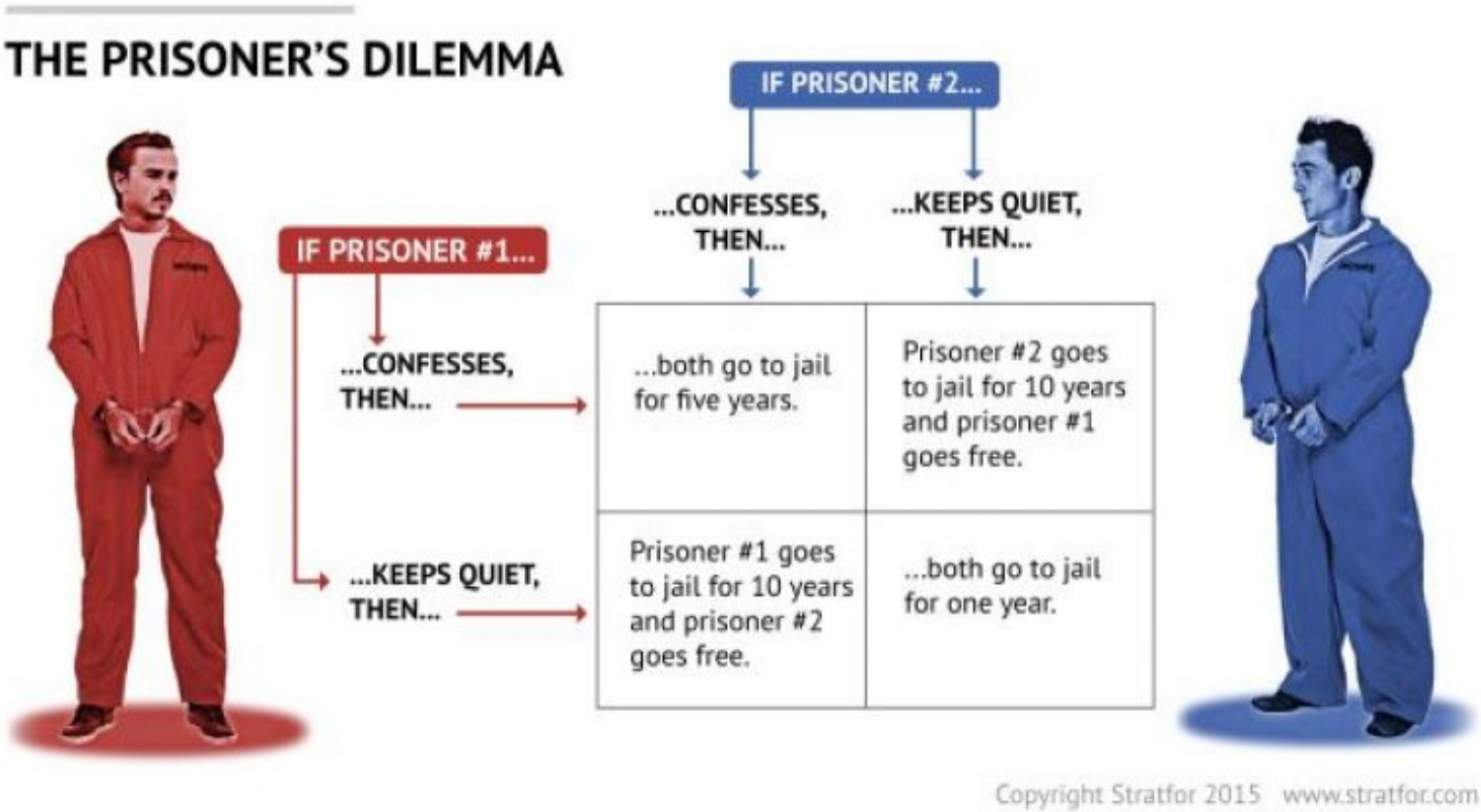


Image:https://worldview.stratfor.com/article/john-nashs-legacy-mathematic-theory-strategic-implications

Prisoner's Dilemma is a hypothetical scenario which illustrates the difficulty of deciding whether to cooperate or compete with other people.

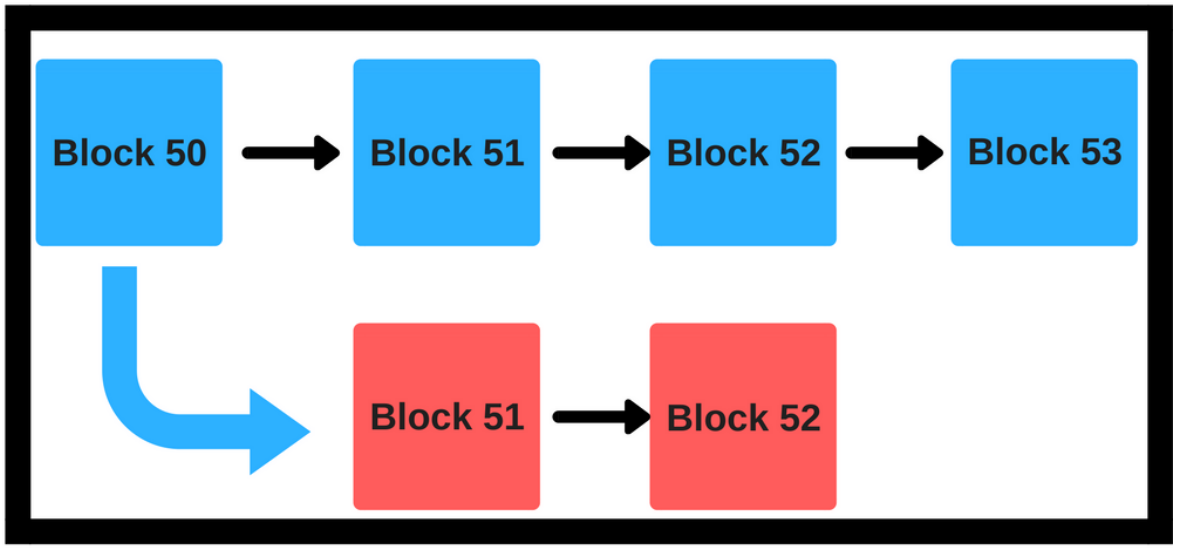
sub-optimal solution

The Nash equilibrium (NE) is a solution to a game where each player chooses their optimal strategy given the strategy was chosen by the other and they have nothing to gain by shifting their strategy.

The Beautiful Mind

Ways to cheat the Network

The blocks in blue are the main chain.



- Assume that a user, in blue block 51, spends 5 bitcoins. And now he wants to create a parallel chain with a new block 51 (red), where in he never spent?

why should the network follow blue chain instead of redchain?

This is where the true genius of blockchain comes in. The blockchain was designed in a way that it is a self-enforcing Nash Equilibrium.

- Any block added on top of the invalid block becomes an invalid block. this rules makes the network to ignore the invalid block and keep adding blocks in blue chain
- The reason why that happens is that the system has a recursive punishment system to prevent invalid blocks.
- Without a majority of miners moving to the invalid block, agents mining these invalid blocks waste resources as nothing is gained (i.e., no incentive).
- In this way, the ecosystem is rewarded for supporting itself in pursuit of the majority
- This game theoretical thinking of promoting good behaviour and deter bad is one of the strengths of this technology; its capacity to self-moderate and shift trust away from third parties.

Cryptoeconomics to achieve overall system reliability

Cryptoeconomics

- Study of economic interaction in adversarial environments
- Combines cryptography and economics to create robust decentralized P2P networks that thrive over time despite adversaries attempting to disrupt them.
- crypto for security and economics to incentivize all actors

Best Behaviour

In cryptoeconomics, you can indeed do bad stuff, you just have to pay for it.

Satoshi's implementation of a Proof of Work (POW) consensus mechanism introduced a new field of economic coordination game, now referred to as cryptoeconomics.

Types of Network settings in Blockchain

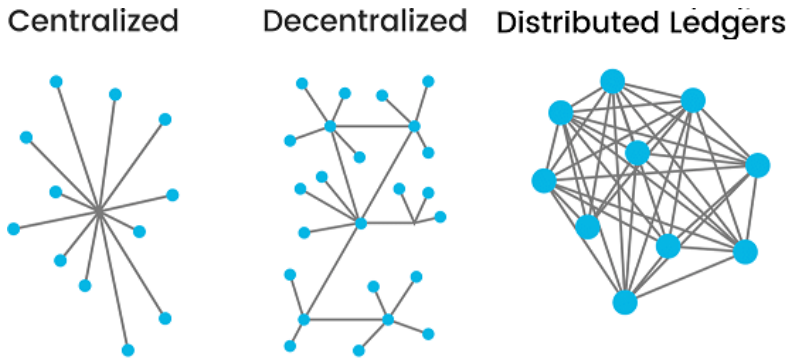


Image:https://blockgeeks.com/guides/what-is-blockchain-technology/

- Centralised - Traditional ledger, one owner writes and modifies the database they own. Ex: Traditional Bank
- DeCentralised - Permissioned Private ledger, only permissioned entities may view and validate the transactions goes into the blockchain Ex: Bankchain
- DeCentralised - Permissioned Public ledger , anyone may view the ledger contents but only permissioned entities may validate the transactions. Ex: Ethereum
- Distributed - unPermissioned Public ledger, anyone can read and write the ledger . Ex: Bitcoin

Block Creation

- easiest part!!
- a sequence of blocks
- nobody can alter the contents/order of the block
- the hash of the previous block becomes part of the next block
- onewayness property

all blockchain achieve it in the same way: Tamperproofness

Choosing the next block

Blockchain's major challenge is choosing the next block

- Creation: Who can create what data?
- Dissemination: To whom the data be disseminated ?
- Storage: Who can store what data?
- Modification: Who can modify what data? (includes updating and deletion)
- Access: Who can access what data?

How to choose the next block?

- Mining: How blocks containing valid transactions are added to the blockchain??
- The magic is not in the data storage technology, but how untrusted users of the network can all reach consensus.
- The magic of "blockchain" isn't "a blockchain"; it's the Proof to achieve consensus :

Image:https://www.linkedin.com/pulse/10-elements-blockchains-ilustrated-bruno-ricardo-ferreira

- The double spending problem is the main breakthrough that Bitcoin made.

Consensus Protocols

- Consensus is a fundamental building block for replicated databases
- to achieve overall system reliability in the presence of a number of faulty nodes.
- a set of nodes seek to agree on a (ever-growing) a unique order in which entries are appended
- Correctness is described in terms of two properties:
  - liveness/availability: the system will decide on a some value
  - safety/consistency: the system will never decide two different values
- Crash tolerance in the presence of synchronous setting is easy with a leader and followers paradigm and cope upto $n/2$ faulty nodes
- In a state machine replication protocol, a set of servers seek to agree on an ever-growing, linearly-ordered log, such that two important properties are satisfied: 1) consistency, i.e., all servers must have the same view of the log; and 2) liveness, i.e., whenever a client submits a transaction, the transaction is incorporated quickly into the log

Assumptions in Crash-tolerent systems

- Consensus to replicate the log among n number of nodes
- Paxos, view stamped replication: used in mission critical applications
- zab protocol in the zookeeper by Yahoo, a recent addition called Raft
- Tolerate atmost $f < n/2$ failures when the number of nodes is n
- The asynchronous model assume that a message broadcasted is acceptable by all nodes: nodes send/receive correct messages

The idea is to elect the leader and follow his instructions and the nodes has the mechanism to maintain the consistency even if the leader node crashes

What is Byzantine Behaviour?

Byzantine Faults

- Nodes does not follow the rules and trying to tamper with the particular state of the ledger
- faulty nodes become the majority
- include behaviours like lying, collusion with other participants, and selective non-participation

With this assumption, the system has to validate the messages it has to commit

Two-Generals' Problem: An Illustrative example

Scenario: Two generals and a common enemy: Both need to co-operate and attack inorder to be successful.

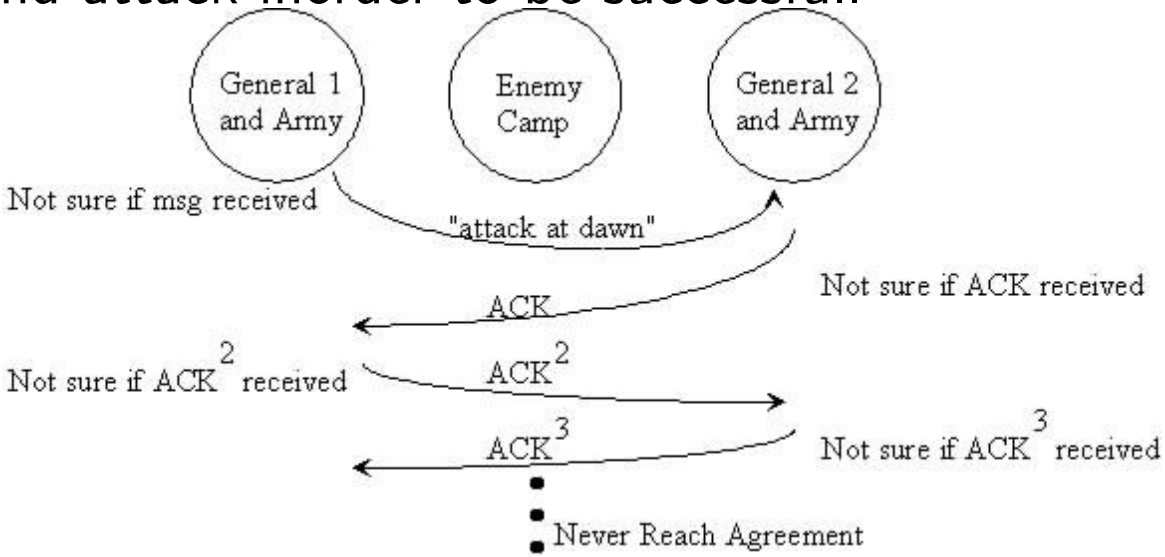


Image:https://medium.com/loom-network/

Challenge: To decide on a time

Complications:

1. enemies might capture the messenger leading to failure in delivery of the message
2. Even if (1) is not happening, General 2 has to acknowledge that he received the message and hence sending a message back

Two General's Problem

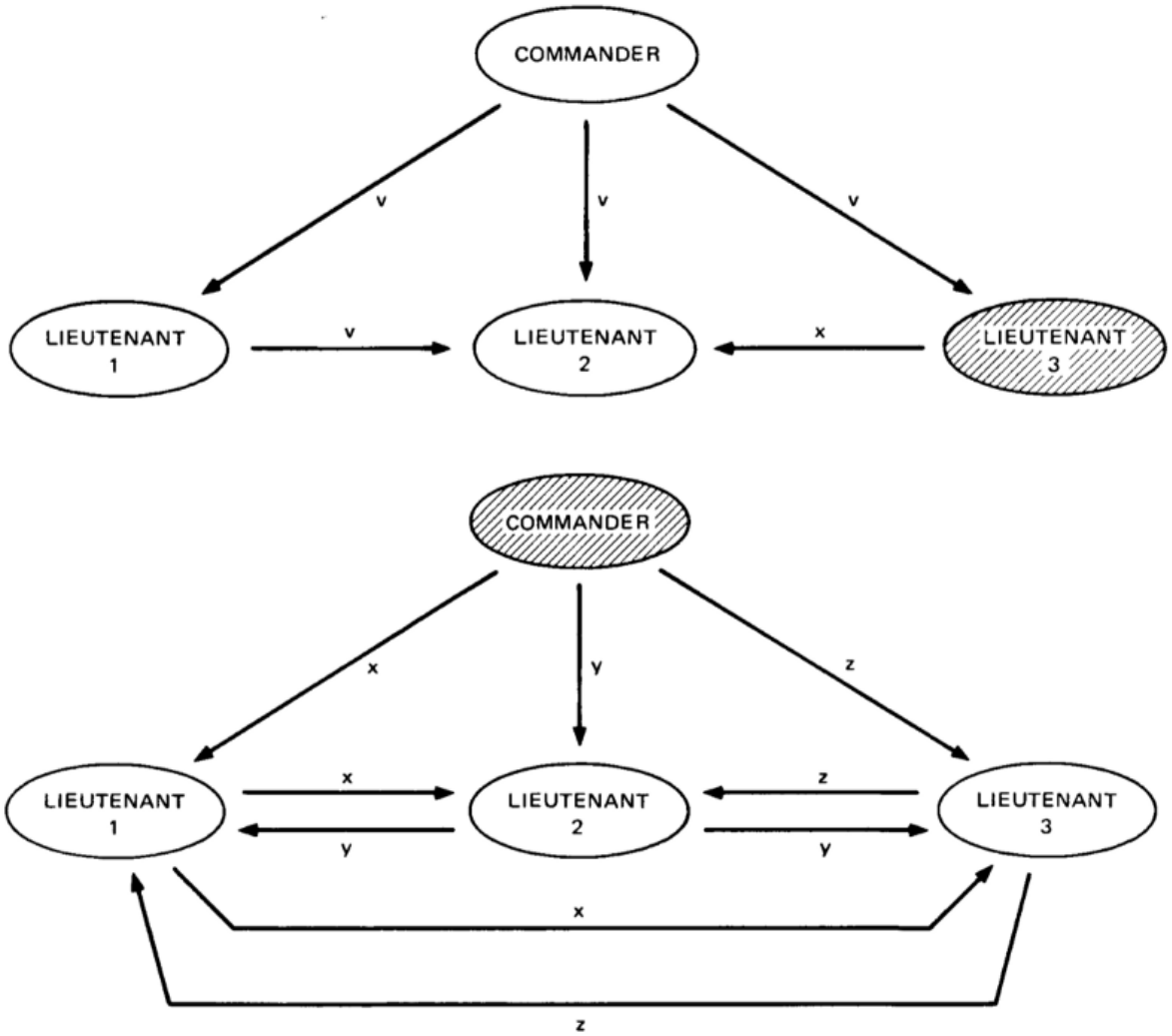
This extends to infinite ACK's and thus the generals are unable to reach an agreement.

Real World Relationships

- Generals ? processors
- Traitors ? faulty processors or faulty system components (including software)
- Messengers ? processor communications/system data bus

Byzantine Generals' Problem

A generalised problem with an additional complication: one or more generals can be traitors:they can lie on their choice



Byzantine General's Problem

- the algorithm can reach consensus as long as 2/3 of the actors are honest.
- If the traitors are more than 1/3, consensus is not reached, the armies do not coordinate their attack and the enemy wins.

Theorem

For any m, the algorithm reaches consensus if there are more than $3m$ generals and at most m traitor

To reach agreement between the loyal generals in the presence of m faults

- There must be at least $3m + 1$ processors to deal with m faults (traitors)
- Each processor must be connected to each other through at least $2m + 1$ communication paths
- $m + 1$ rounds of messages must be exchanged
- The processors must be synchronized within a known skew of each other

Such a system is called Byzantine Resilient which is a fully fault tolerant system.

Runnig time of BFT

byzantine-paxos protocol is byzantine fault tolerent where the authors introduced a mechanism to verify the messaged recieved by the node.

Constraints

- requires less than one third of the nodes is dishonest
- Message complexity
- tolerating Byzantine faults is much difficult for the large scale setting.

m	Messages Sent
0	O(n)
1	O(n^2)
2	O(n^3)
3	O(n^4)

Bitcoin Consensus

- suitable for large scale networks?
- Can we do better than the ones seen so far ?
- the result is the proof of work consensus mechanism : to elect a leader who will decide the contents of the next block. That leader is also responsible for broadcasting the block to the network, so that the other peers can verify the validity of its contents.

Bitcoin's Consensus Mechanism: Proof of Work

nonce, a random string satisfies $H(\text{prev hash, nonce}) = 0000 \cdots 0xxxxxxx$

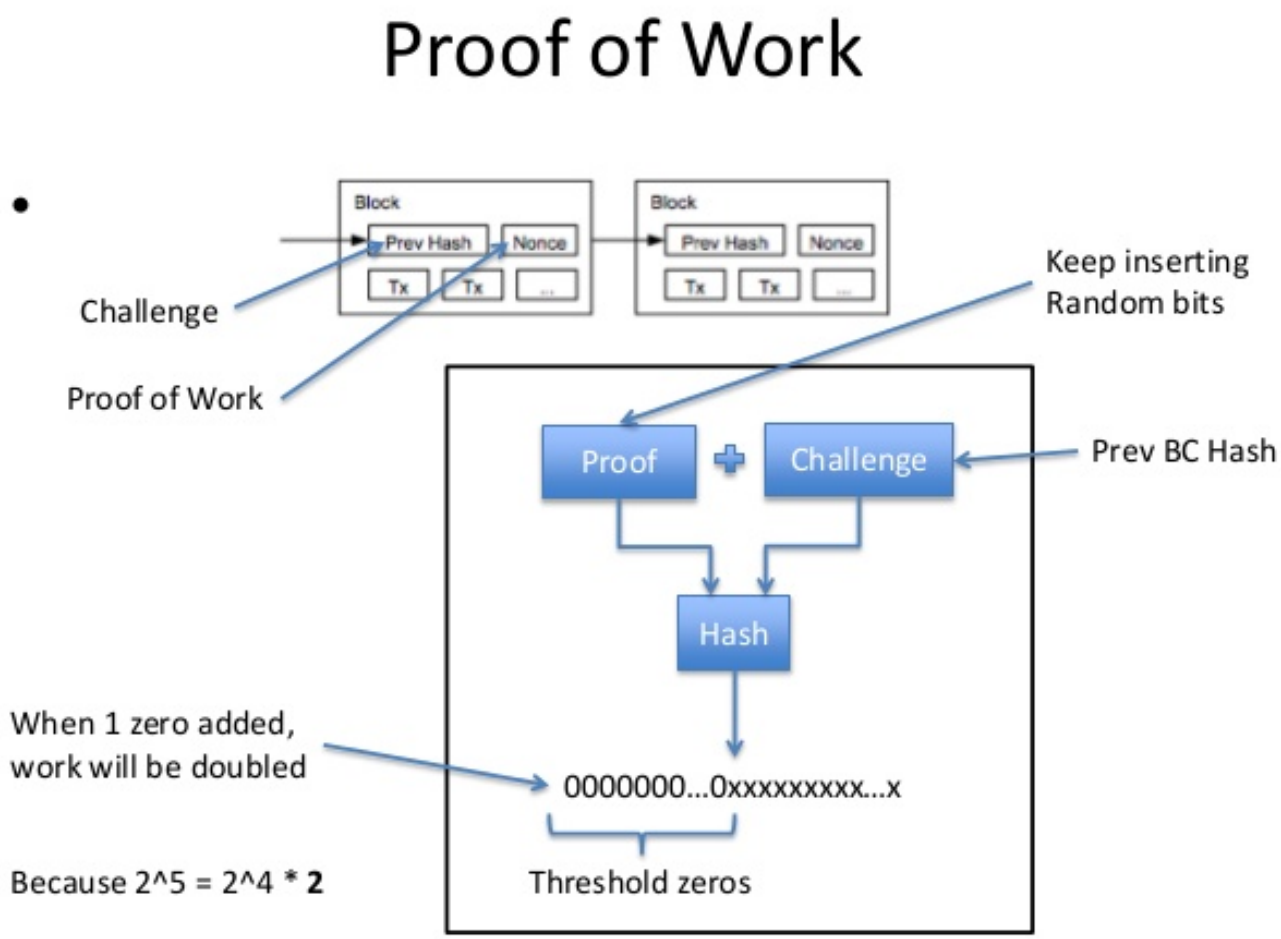


Illustration:https://steemit.com/cryptocurrency/@rrrenaldooo/what-is-hybrid-blockchain-proof-of-work-and-proof-of-stake-explained

Cheating is not possible;Tamper Resistant

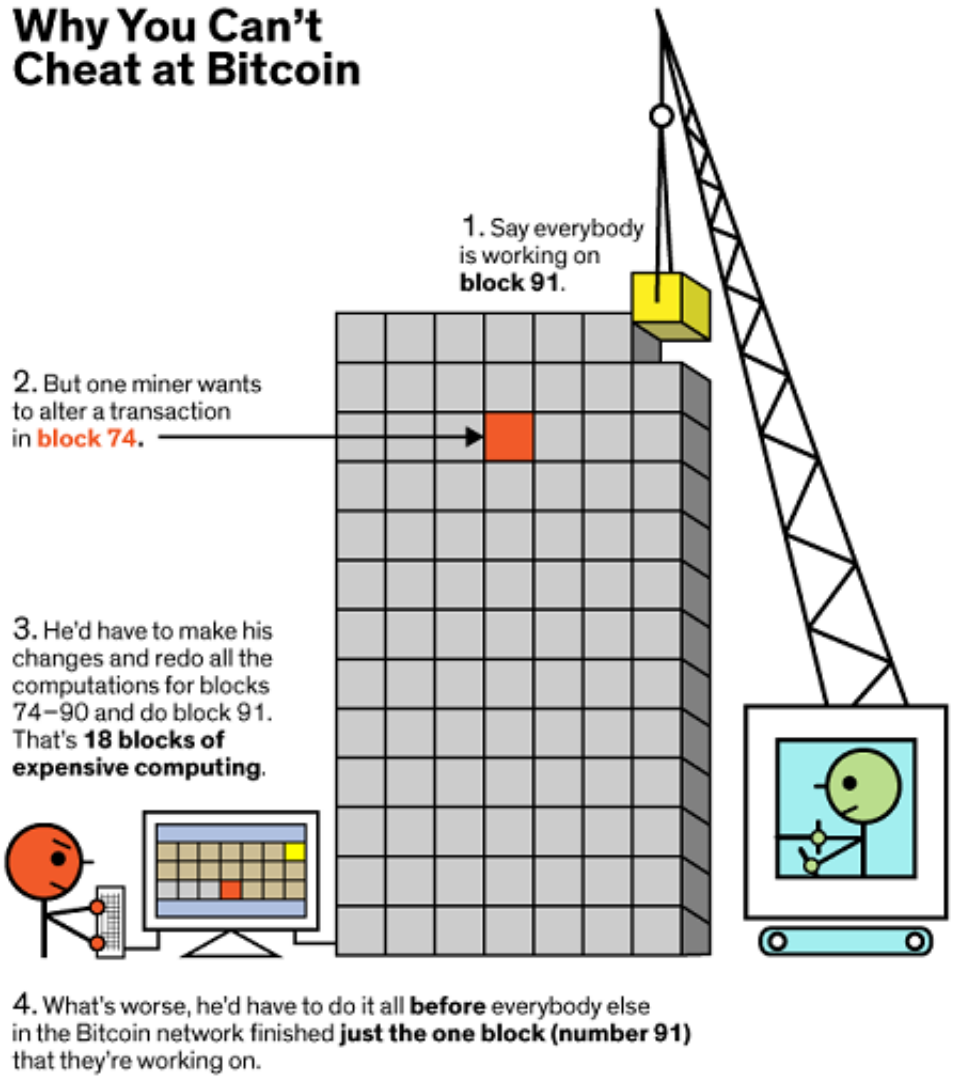
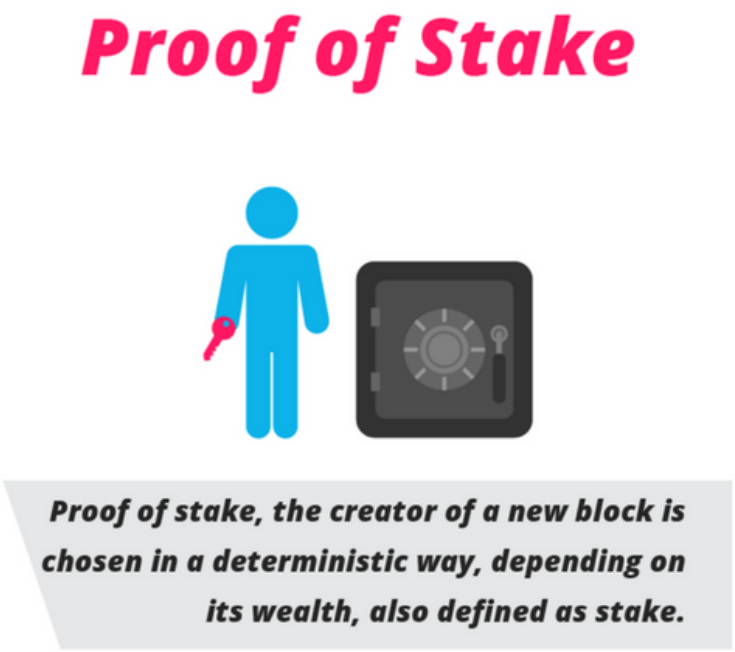


Illustration:Mark Montgomery

Consensus Mechanism used in Cryptocurrencies

- Proof of Work (PoW) is energy consuming
- Proof of Stake (PoS) replaces the energy consumption with the stake:



  - Nothing-at-stake problem
- Hybrid consensus Mechanism to take away the disadvantages of PoW and PoS: PoW-PoS

Consensus in Hyperledger: Proof of Elapsed time (PoET)

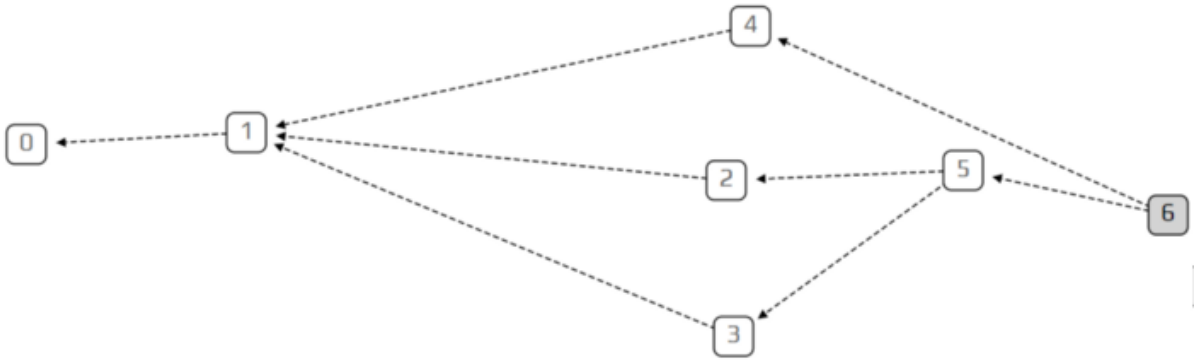
- addresses the problems in Delegated Proof of Stake (DPoS)
- randomize the leader selection in BFT using timer function
- works using SGX technology : a secure enclave
- SGX helps the node to join the network which verifies whether they are running the trusted code necessary for consensus execution
- After joining the network, nodes receive a signed timer object from the trusted code which is completely randomized.
- Each participant subsequently waits for their randomized timer to expire.
- The network participant's timer that is the first to expire propagates a signed certificate to the network indicating that they are the randomized block leader for that round. The round then restarts.
- Disadvantage: SGX is vulnerable to spectre type attacks

Algorand's Consensus

- Randomize the leader selection with the help of cryptographic sortition
- in the first phase, a node is randomly selected to propose a block
- in the second phase, a set of randomly chosen nodes validate the block proposed

The magic happens with the help of Mathematics: Verifiable Random Functions

IoTA's Tangle



- directed acyclic graph
- incoming node has to approve two transactions forming two edges
- strategy to choose two unapproved transactions is unique to this technology

Which faults are tolerated by a protocol?	**Special-node crash**	**Any $t < n/2$ nodes crash**	**Special-node subverted**	**Any $f < n/3$ nodes subverted**
Hyperledger Fabric/Kafka	.	✓	.	–
Hyperledger Fabric/PBFT	.	✓	.	✓
Tendermint	.	✓	.	✓
Symbiont/BFT-SMaRt	.	✓	.	✓
R3 Corda/Raft	.	✓	.	–
R3 Corda/BFT-SMaRt	.	✓	.	✓
Chain/Federated Consensus	–	(✓)	–	–
MultiChain +	.	✓	.	–
Sawtooth Lake/PoET	⊕	✓	⊕	–
Ripple	⊗	(✓)	⊗	–
Stellar/SCP	?	?	?	?
IOTA Tangle	?	?	?	?

Summary on Consensus

- Consensus is a fundamental building block for replicated databases
- Classical deployment scenarios are typically relatively small scale, with fast local-area networking, where crash (rather than byzantine) faults are usually of concern.
- Classical-style protocols such as Practical Byzantine Fault Tolerance or Byzantine-Paxos
  - confirm transactions quickly in the normal case
  - fast confirmation by adopting the asynchronous model
  - Complicated in a large-scale setting
- Blockchain style protocols such as PoW /PoS
  - conceptually simple and tolerate minority corruptions
  - known for slow confirmations (10 minute block interval and block confirmations after 6 blocks)
- benefits of both the world: the dream of large-scale consensus with fast confirmations

.

How Bitcoin's BlockChain works?

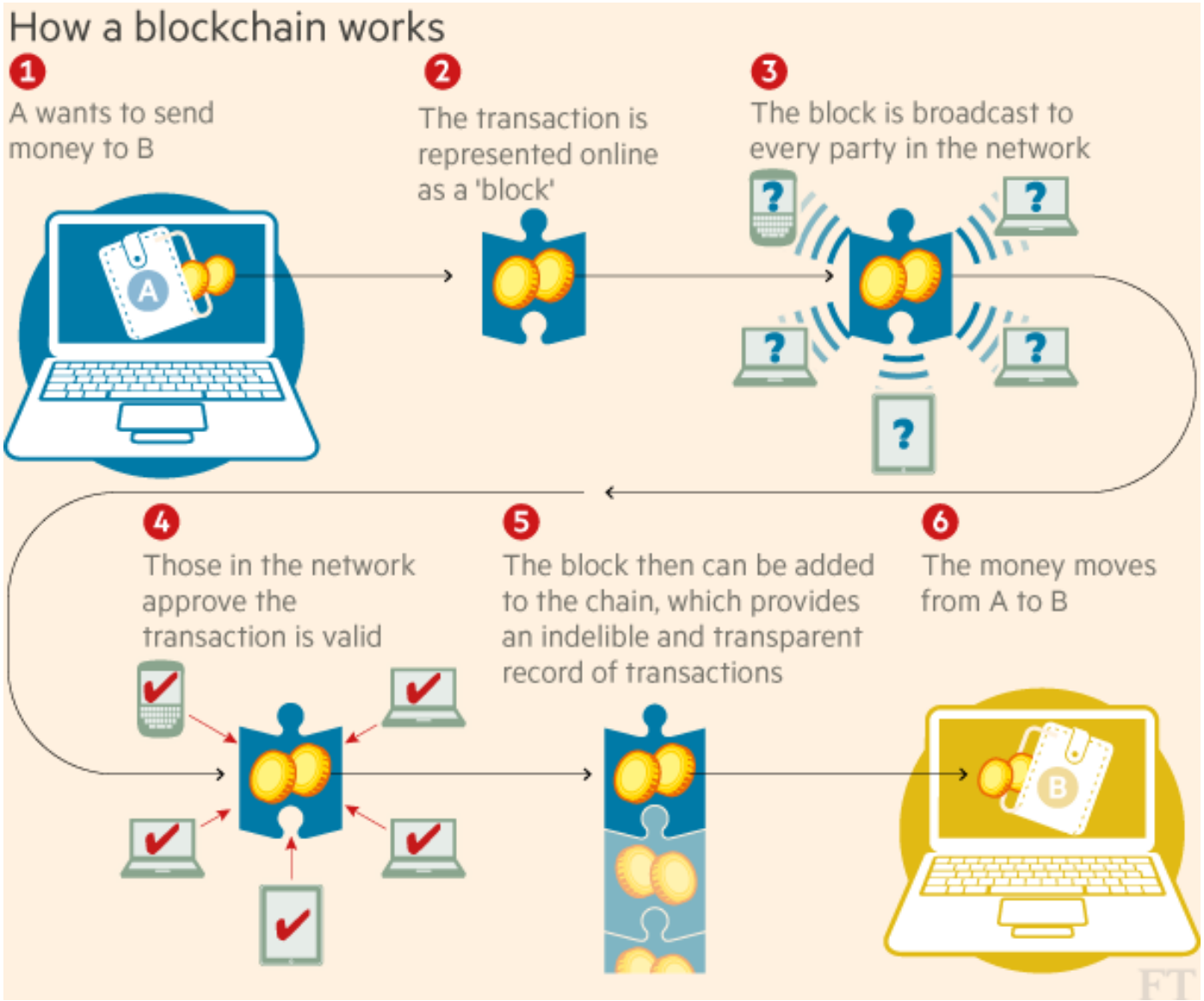


Image:Financial Times

Bitcoin's Attack Vectors

Blockchain systems enhances security and privacy that is unseen by centralized systems

- Denial of Service (DoS),
- Sybil attack
- Eclipse attack
- Routing Attack

DoS Attack

An attempt to flood the victim with bogus information

- malicious node can send many transactions with multiple address
- flood the honest nodes by sending bogus traffic
- results in the congestion of network and denying certain nodes access to some data flowing.
- stop them from updating current state

Transaction fees may slow down the attackers

ways to decrease the chances of being victims to such attacks but there isn't a way to completely eliminate them

Sybil attack:What problems can Sybil attacks cause?

A Sybil attack is one where the attacker pretends to be so many people at the same time.

- Attackers may be able to out-vote the honest nodes on the network if they create enough fake identities (or Sybil identities). They can then refuse to receive or transmit blocks, effectively blocking other users from a network.
- The other honest nodes may not be able to detect such behavior and may have fed with false information from this malicious node thinking the data is arriving from so many different sources
- In really large-scale Sybil attacks, where the attackers manage to control the majority of the network computing power or hash rate, they can carry out a 51 percent attack. In such cases, they may change the ordering of transactions, and prevent transactions from being confirmed. They may even reverse transactions that they made while in control, which can lead to double spending.

Sybil Attacks Contd.

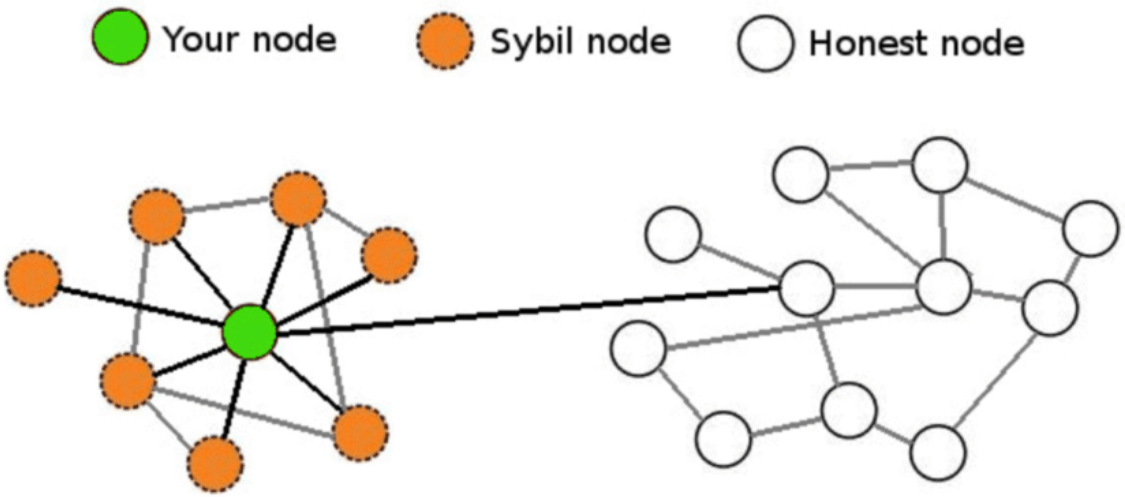


Image:coincentral

- countermeasures such as Proof-of-Work (PoW). PoW requires each node that wishes to participate in the mining process to compete in an expensive crypto-puzzle. Now, creating multiple identities is still possible, but, providing the computational power to solve this puzzle then becomes the issue.

Swiss-based company Chainalysis that provides blockchain analytics, created over 250 fake Bitcoin nodes and was trying to collect information about transactions propagating over the network.

Routing attack

Rely on intercepting messages propagating through the network and tampering with them before pushing them to their peers.

- The only way to detect is when the node receive a different copy of it from another node.
- But what if they have no other source of receiving data propagated through the network?
- what if the malicious node is able to divide the network so that it splits it into two or more partitions which cannot communicate or see each other anymore.
  - Partitioning attack: The attacker tries to split the network into two or more disjoint groups. This can be done by hijacking certain points within the network that act as the linking point between two groups.
  - Delay attack: Next, the attacker picks up the propagating messages, tampers with them and finally pushes them to the side of the network that has not seen it before.

Routing Attack Contd.

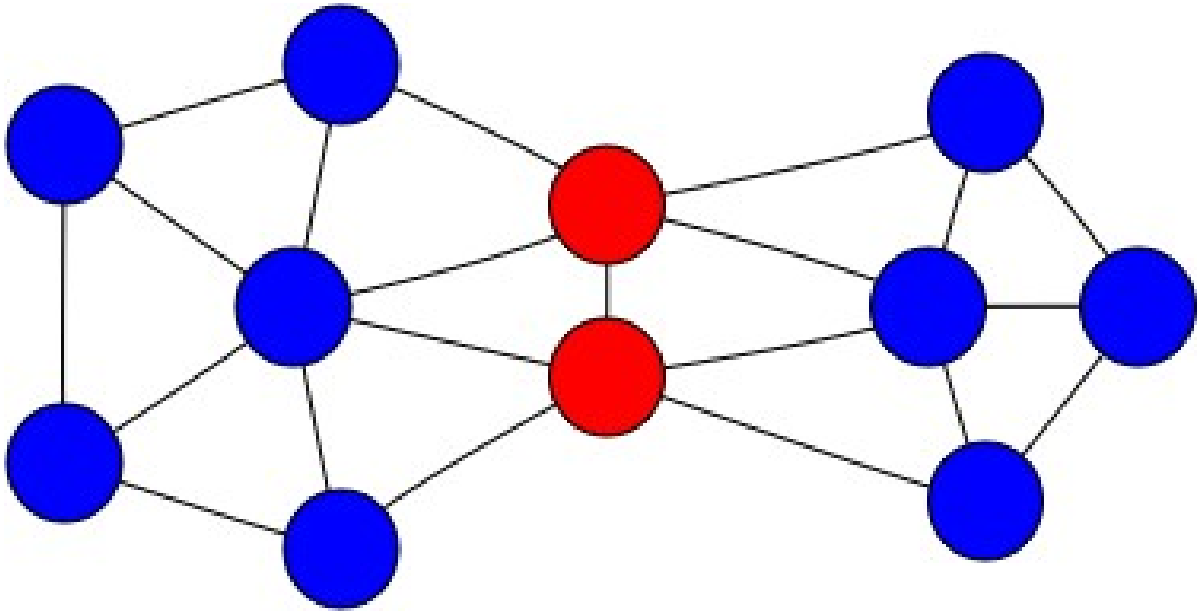


Image:medium

- continuous diversification of network connections makes attacker task much harder to find points to hijack and split the network into two or more disjoint groups.
- monitor the network parameters such as Round-Trip Time (RTT) and recognize irregular patterns. RTT is basically the time needed for nodes to share data and acknowledge its delivery. Once detected, the nodes can simply disconnect themselves and try to connect to other random nodes.

Blockchain Based Explorations

- Andhra Pradesh to become first state to deploy blockchain technology across the administration : land records and transport
- SBI through Bankchain to use blockchain for smart contracts and KYC by this year
- IDRBT to launch model platform for blockchain technology suitable for banking applications
- Dubai to become the world's first blockchain city by 2020
- Seoul to move most of its record keeping in blockchain by 2022
- Australian Government Awarded 8 Million grant to Blockchain based integrated distributed energy and water systems project ;
- chromaway :to prevent tampering on land record and stream line titles of vehicles

Blockchain for Cybersecurity

- Gladius:Preventing DDoS attack: Distributed DNS service
- Providing data integrity: Keyless signature infrastructure (KSI) by Guardtime
- Eliminating human factor from the authentication process: REMME's blockchain eases buisnesses to authenticate users and devices without password
- Estonia: health records and DARPA : US military records are protected
- Moldova eyes blockchain to end child trafficking; UN has started a pilot to fight against child trafficking
- IOTA : to identify IoT Devices and data authentication
- BankChain, a community of 27 banks, which have joined hands to explore and build blockchain solutions for banking.

Conclusion

- Blockchain technology is still in the design and planning phases: understanding BFT is crucial for applicability of blockchain beyond digital currency.
- Bitcoin consensus may not be practical for other types of blockchain applications.
  - For example, PoW to achieve consensus is inefficient where nodes are assumed to operate under real identities
- BFT is a crucial part of an effective blockchain and there are multiple ways in which it can be implemented.
- Deciding which approach to take requires weighing the nature and priorities of the community associated with the blockchain an organization wants to build.
- The solutions to BFT that have made systems like Bitcoin possible may not work well in the blockchain applications of the future