



Blockchain

Blockchain components, Blocks, transactions,
DLT, consensus, proof of work, mining,
Public vs Private Blockchain

Dr. Sarwan Singh
NIELIT Chandigarh



Agenda

- Introduction to Bitcoin
- Mining, solving puzzle
- Blockchain components - Blocks, transactions, DLT
- consensus, proof of work
- Public vs Private Blockchain



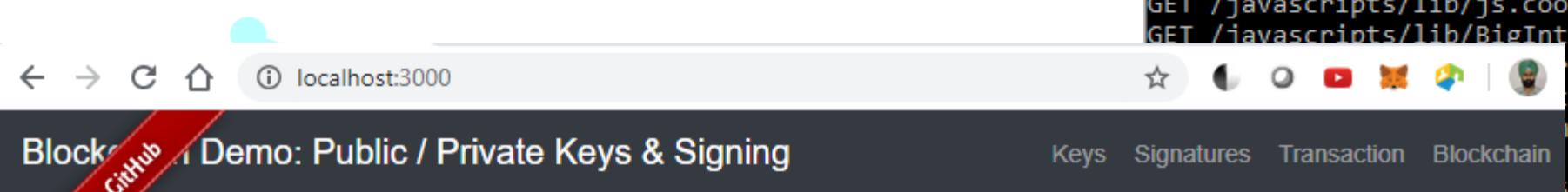
References

- Medium.com - Blockchain
- “Blockchains Architecture, Design and Use Cases” Prof. Sandip Chakraborty, Prof. Praveen Jayachandran IIT Kharagpur
- IBM Blockchain Labs
- “Conceptualizing blockchains: characteristics & applications” 11th IADIS International Conference Information Systems 2018
- blockgeeks, appinventiv
- consensys.net – Blockchain application areas, use-case
- flatworldbusiness.wordpress.com
- 101blockchains.com



Public-Private key Demo

- npm start



Blockchain Demo: Public / Private Keys & Signing

by Sarwan Singh

2019-20

sarwan@NIELIT

```
> node ./bin/www

GET / 200 1326.684 ms - 2246
GET /stylesheets/lib/bootstrap.min.css 304 9.460 ms - -
GET /stylesheets/public-key-private-key.css 304 18.051 ms - -
GET /javascripts/lib/jquery.min.js 304 19.106 ms - -
GET /javascripts/lib/popper.min.js 304 19.214 ms - -
GET /javascripts/lib/bootstrap.min.js 304 5.085 ms - -
GET /javascripts/lib/js.cookie.min.js 304 5.466 ms - -
GET /javascripts/lib/BigInteger.min.js 304 5.862 ms - -
.js 304 1.583 ms - -
ic.js 304 2.753 ms - -
in.js 304 3.166 ms - -
min.js 304 8.798 ms - -
.js 304 9.332 ms - -
.js 304 0.544 ms - -
ub-ribbon.png 304 0.829 ms - -
3392
rap.min.css 304 1.214 ms - -
-private-key.css 304 9.930 ms - -
kie.min.js 304 4.610 ms - -
min.js 304 5.365 ms - -
min.js 304 6.507 ms - -
rap.min.js 304 14.942 ms - -
eger.min.js 304 16.101 ms - -
GET /javascripts/lib/Buffer.js 304 5.175 ms - -
GET /javascripts/lib/elliptic.js 304 6.061 ms - -
GET /javascripts/lib/spin.min.js 304 9.276 ms - -
```



Blockchain Demonstration

- npm start

Fork me on GitHub

Blockchain Demo

Hash Block Blockchain Distributed Tokens Coinbase

by Sarwan Singh Chandigarh

2019-20

sarwan@NIELIT

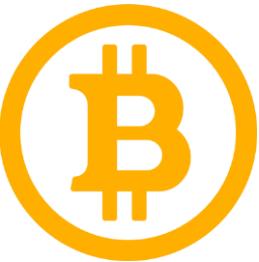
5

```
> node ./bin/www

GET / 200 2452.302 ms - 2385
GET /stylesheets/lib/ie10-viewport-bug-workaround.css 200 297.074 ms - 451
GET /stylesheets/lib/ladda-themeless.min.css 200 324.421 ms - 7717
GET /stylesheets/blockchain.css 200 328.032 ms - 632
GET /stylesheets/lib/bootstrap-theme.min.css 200 363.078 ms - 23414
GET /stylesheets/lib/bootstrap-horizon.css 200 364.527 ms - 2889
n.css 200 404.509 ms - 121205
t-bug-workaround.js 200 187.420 ms - 664
: 200 206.799 ms - 3201
n.js 200 227.678 ms - 37051
200 239.629 ms - 4123
s 200 254.457 ms - 84349
0 127.585 ms - 4624
0 63.172 ms - 2133
bon.png 200 33.845 ms - 8146
GET /stylesheets/lib/bootstrap-theme.min.css 304 3.083 ms - -
GET /stylesheets/lib/bootstrap-horizon.css 304 13.522 ms - -
GET /stylesheets/lib/ie10-viewport-bug-workaround.css 304 31.790 ms - -
GET /stylesheets/blockchain.css 304 32.750 ms - -
GET /stylesheets/lib/ladda-themeless.min.css 304 11.151 ms - -
GET /javascripts/lib/jquery.min.js 304 11.156 ms - -
```



Bitcoin



- Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: transaction management and money issuance are carried out collectively by the network.
- The original Bitcoin software by Satoshi Nakamoto was released under the MIT license. Most client software, derived or "from scratch", also use open source licensing.
- Bitcoin is designed around the idea of using cryptography to control the creation and transfer of money, rather than relying on central authorities.
- Bitcoins have all the desirable properties of a money-like good. They are portable, durable, divisible, recognizable, fungible, scarce and difficult to counterfeit.



Bitcoin Transactions are ...

- **Permissionless** and **borderless**. The software can be installed by anybody worldwide.
- **Do not require any ID** to use. Making it suitable for the unbanked, the privacy-conscious, computers or people in areas with underdeveloped financial infrastructure.
- Are **censorship-resistant**. Nobody is able to block or freeze a transaction of any amount.
- **Irreversible** once settled, like cash. (but consumer protection is still possible.)
- **Fast**. Transactions are broadcasted in seconds and can become irreversible within an hour.
- Online and available **24 hours a day, 365 days per year**.



Stored Bitcoins

Bitcoin can also be a store of value, some have said it is a "swiss bank account in your pocket".

- Cannot be printed or debased. **Only 21 million bitcoins will ever exist.**
- Have **no storage costs**. They take up no physical space regardless of amount.
- Are **easy to protect and hide**. Can be stored encrypted on a hard disk or paper backup.
- Are in your **direct possession** with no counterparty risk. If you keep the private key of a bitcoin secret



- Bitcoin uses public-key cryptography, peer-to-peer networking, and proof-of-work (consensus model) to process and verify payments. Bitcoins are sent (or signed over) from one address to another



2019-20



sarwan@NIELIT



- A Bitcoin address is a pseudonymous identity that is used to send and receive bitcoins.
- An address can be described as the hash of an **EC (Elliptic Curve) public key** and the accompanying private key is used to produce **ECDSA (Elliptic Curve Digital Signature Algorithm) signatures** to authorize payments.



Bitcoin mining - solving puzzle

The Data

- This is the hash of the latest block (shortened to 30 characters):

0000000000001adf44c7d69767585 (13 leading zeros)

The hashes of a few valid transactions waiting for inclusion (shortened)

5572eca4dd4

db7d0c0b845

the hash of one special transaction which gives 25BTC (the current reward) to yourself

916d849af76



Bitcoin mining - solving puzzle

Building the next block:

use a gross approximation of what a new block might look like (the real one uses binary format). It contains the hash of the previous block and the hashes of those 3 transactions:

0000000000001adf44c7d69767585 -- 5572eca4dd4 --db7d0c0b845 --
916d849af76 --

mining by hand! Our goal is to complete this block with a nonce (a piece of garbage) such that the hash of the new block starts with 13 zeros

(Bitcoin uses double sha256 but we use md5 for ease)

try with nonce=1 {nonce can be any random hexadecimal value},

"0000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-
916d849af76--1" | md5sum

Output : 8b9b994dcf57f8f90194d82e234b72ac

Not accepted



Bitcoin mining - solving puzzle

Building the next block ...

try with nonce=1,

```
"00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-  
916d849af76--1" | md5sum
```

Output : 8b9b994dcf57f8f90194d82e234b72ac

Not accepted

try with nonce=2,

```
"00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-  
916d849af76--2" | md5sum
```

Output : 5b7ce5bcc07a2822f227fcae7792fd90

Not accepted



Bitcoin mining - solving puzzle

Building the next block ...

try with nonce=16,

"0000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--16" | md5sum

Output : 03b80c7a34b060b33dd8fbece79cee3

Not accepted

try with nonce=208,

"0000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--208" | md5sum

Output : 0055e55df5758517c9bed0981b52ce4a

Not accepted

If you finally find a hash that has 13 leading zeroes... you're a winner!
Other miners will now build upon your block, you've just got 25BTC



Bitcoin mining - solving puzzle

Building the next block ...

try with nonce=934,224,175,

"0000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--934224175" | md5sum

Output : 0000000000005633dd8fbece79cee3 accepted

But to solve the puzzle it took 1 hour, 18 minutes, 12 seconds

There is currently no known shortcut to this process; publishing nodes must expend computation effort, time, and resources to find the correct nonce value for the target.



Bitcoin mining - solving puzzle

- For many proof of work based blockchain networks, publishing nodes tend to organize themselves into “pools” or “collectives” whereby they work together to solve puzzles and split the reward.
- This is possible because work can be distributed between two or more nodes across a collective to share the workload and rewards.
- Splitting the example program into quarters, each node can take an equal amount of the nonce value range to test:
 - Node 1: check nonce 0000000000 to 0536870911
 - Node 2: check nonce 0536870912 to 1073741823
 - Node 3: check nonce 1073741824 to 1610612735
 - Node 4: check nonce 1610612736 to 2147483647
- completed in 10 minutes, 14 seconds



Core Blockchain Architecture Components:

- **Node** — user or computer within the blockchain
- **Transaction** — smallest building block of a blockchain system
- **Block** — a data structure used for keeping a set of transactions which is distributed to all nodes in the network
- **Chain** — a sequence of blocks in a specific order
- **Miners** — specific nodes which perform the block verification process
- **Consensus**— a set of rules and arrangements to carry out blockchain operations



Actors in Blockchain solution



Blockchain Architect	A	Responsible for the architecture and design of the blockchain solution
Blockchain User	U	The business user, operating in a business network. This role interacts with the Blockchain using an application. They are not aware of the Blockchain.
Blockchain Regulator	R	The overall authority in a business network. Specifically, regulators may require broad access to the ledger's contents.
Blockchain Developer	D	The developer of applications and smart contracts that interact with the Blockchain and are used by Blockchain users.
Blockchain Operator	O	Manages and monitors the Blockchain network. Each business in the network has a Blockchain Network operator.
Membership Services		Manages the different types of certificates required to run a permissioned Blockchain.
Traditional Processing Platform		An existing computer system which may be used by the Blockchain to augment processing. This system may also need to initiate requests into the Blockchain.
Traditional Data Sources		An existing data system which may provide data to influence the behavior of smart contracts.





Blockchain Components



Ledger



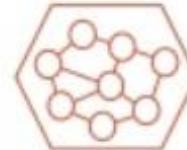
contains the current world state of the ledger and a Blockchain of transaction invocations

Smart Contract



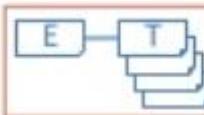
encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state

Consensus Network



a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger

Membership



manages identity and transaction certificates, as well as other aspects of permissioned access

Events



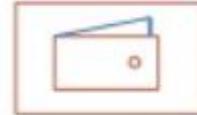
creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.

Systems Management



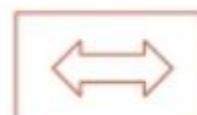
provides the ability to create, change and monitor Blockchain components

Wallet



securely manages a user's security credentials

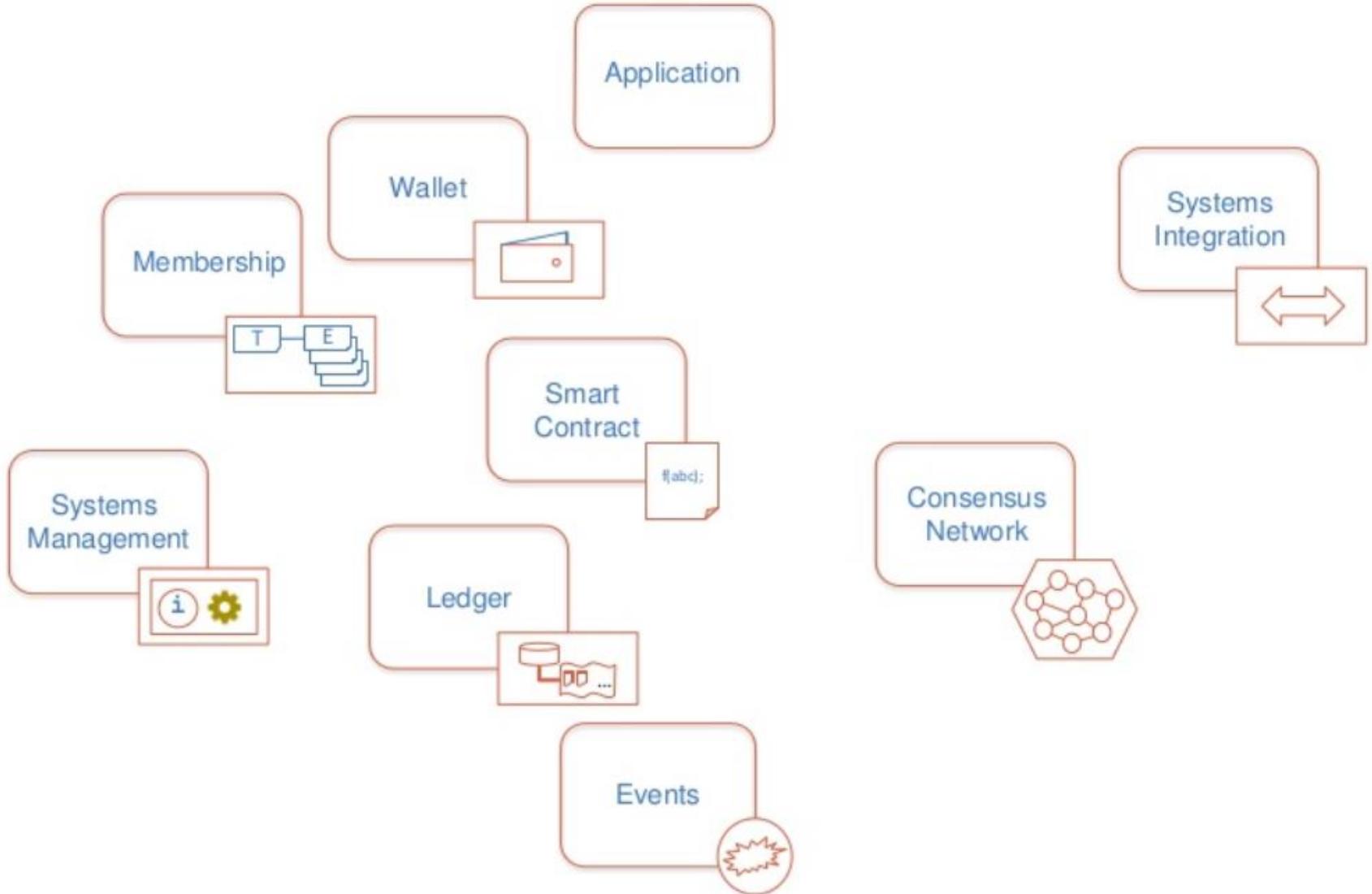
Systems Integration



responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.



Blockchain components





Consensus Model

- As blockchain is a decentralized peer-to-peer system with no central authority, which makes it a corruption free but this may be problematic in some ways:
 - How to make decisions ? “*when/how new block will be added*”
 - How to execute some job ? “*who will add new block*”
- In a centralized system, central server do this job or has this role as leader.
- In a blockchain, as there is no leader as such decisions are taken on the basis of consensus.

“Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Consensus may be defined professionally as an acceptable resolution, one that can be supported, even if not the “favorite” of each individual. Consensus is defined by Merriam-Webster as, first, general agreement, and second, group solidarity of belief or sentiment.”

wiki

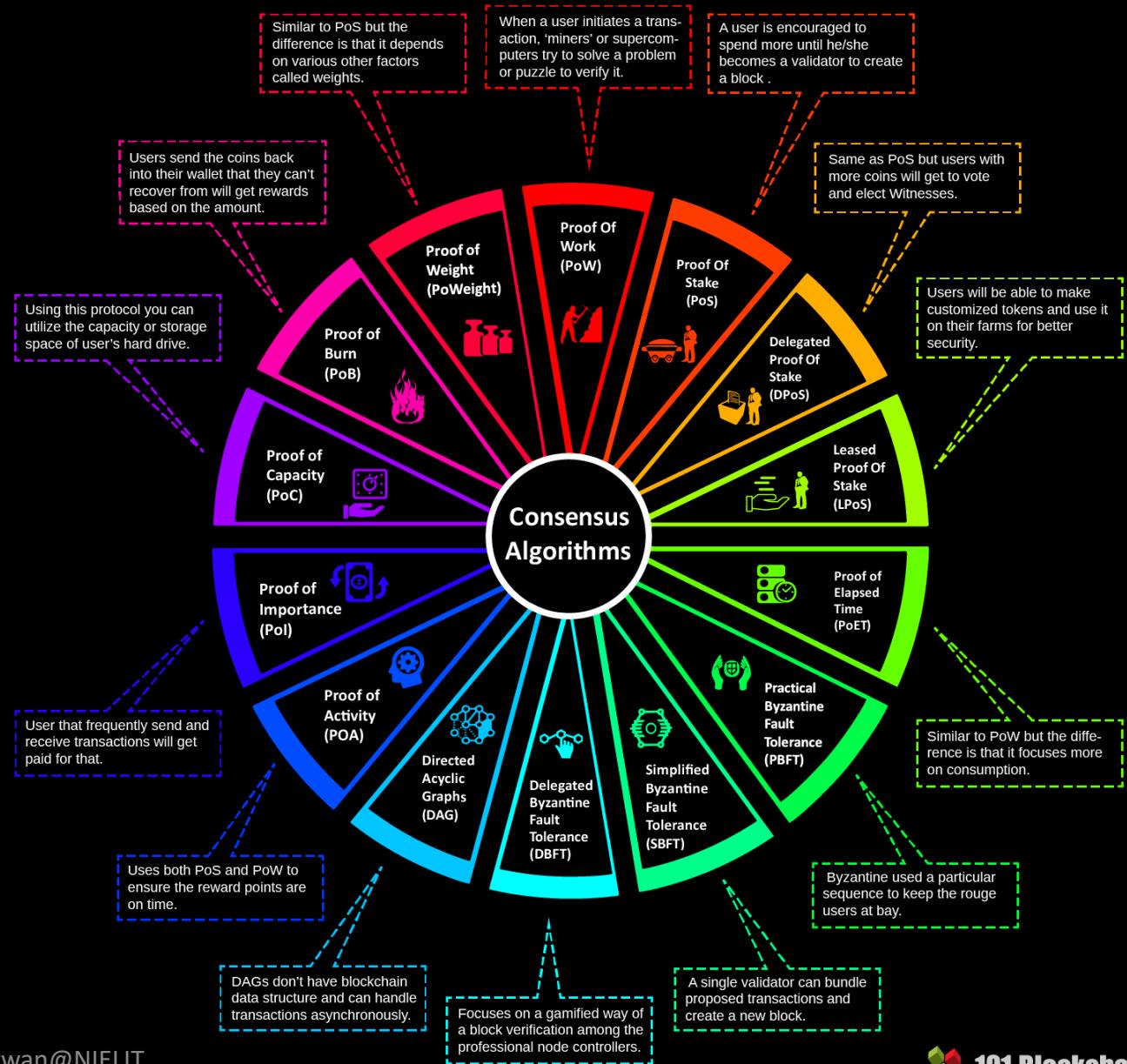


Consensus Models

- A key aspect of blockchain technology is determining which user publishes the next block.
- This is solved through implementing one of many possible consensus models.
- Consensus models enables a group of mutually distrusting users to work together.

2019-20

Different Types of Consensus Algorithms



sarwan@NIELIT



Objective of Consensus mechanism

- Agreement Seeking

- Collaborative

- Cooperative

- Egalitarian

- each and every vote has equal weightage

- Inclusive

- Participatory

Source : wiki

2019-20

sarwan@NIELIT

23

Byzantine Generals Problem

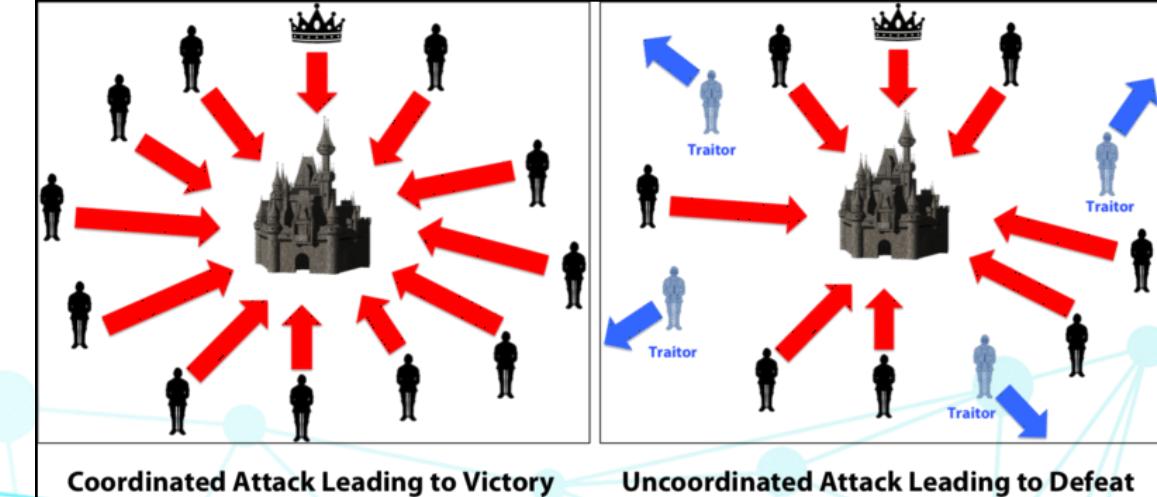
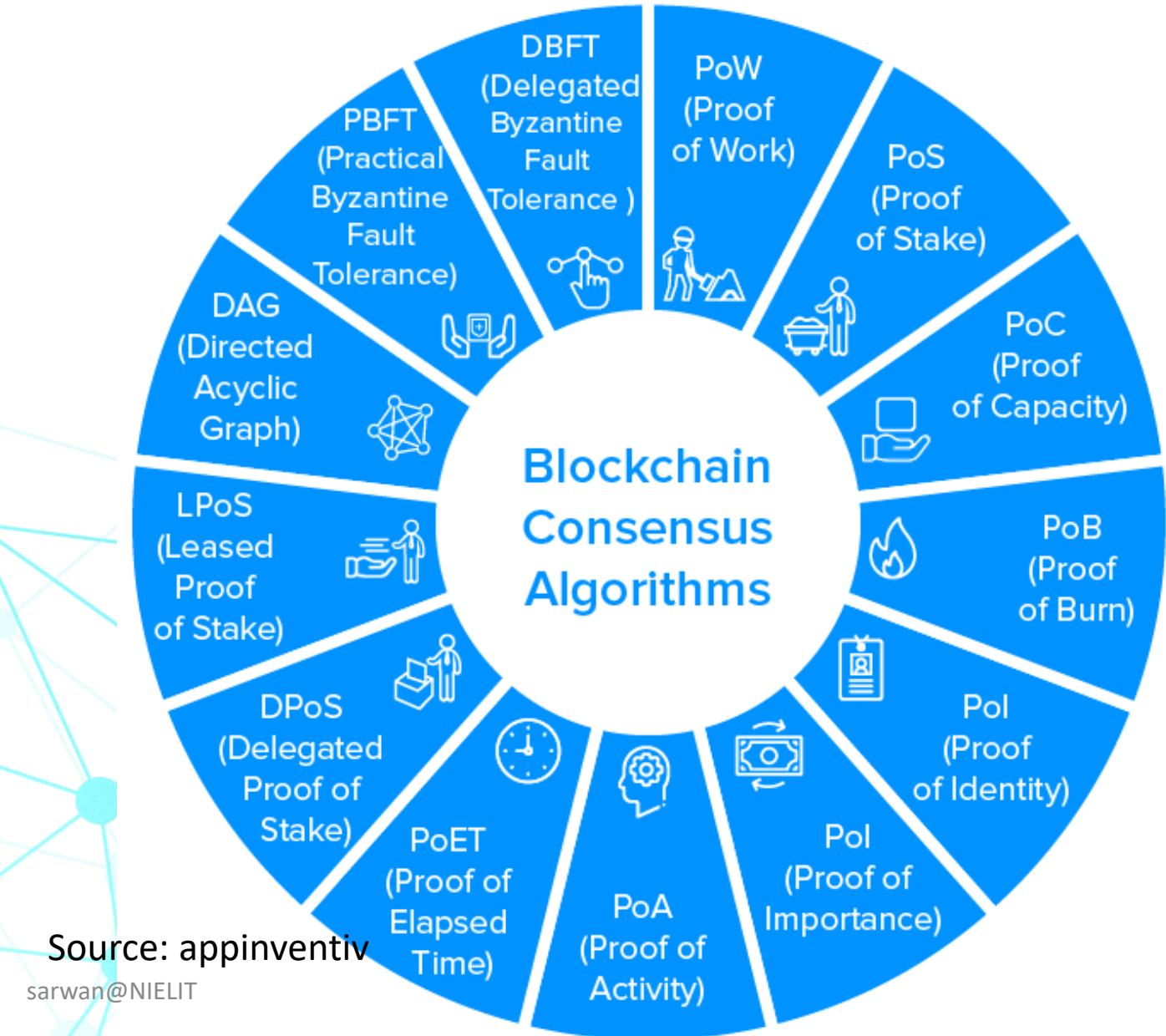


Image Courtesy: Medium



Popular Consensus models

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Byzantine Fault Tolerance (BFT)
- Direct Acyclic Graph (DAG)
- Proof of Capacity (PoC)
- Proof of Burn (PoB)
- Proof of Identity (PoI)
- Proof of Activity (PoA)
- Proof of Elapsed Time (PoET)
- Proof of Importance (PoI)





Mining Process

In a blockchain each block contains a record of many transactions on the network.

Due to large number of participants, we need to **maintain scarcity** of the reward tokens and regulate who gets right to create the next block.

Whoever solves the problem earns the right to create the next block (and gets the reward).

Creating new blocks gives out a reward, also known as the “**miner's fee**”.

To achieve this, each participant in the network must solve a complex cryptographic problem (also known as “**proof of work**”).

The disadvantage to this is, these problems are very resource intensive and take a substantial amount of computational power to solve.



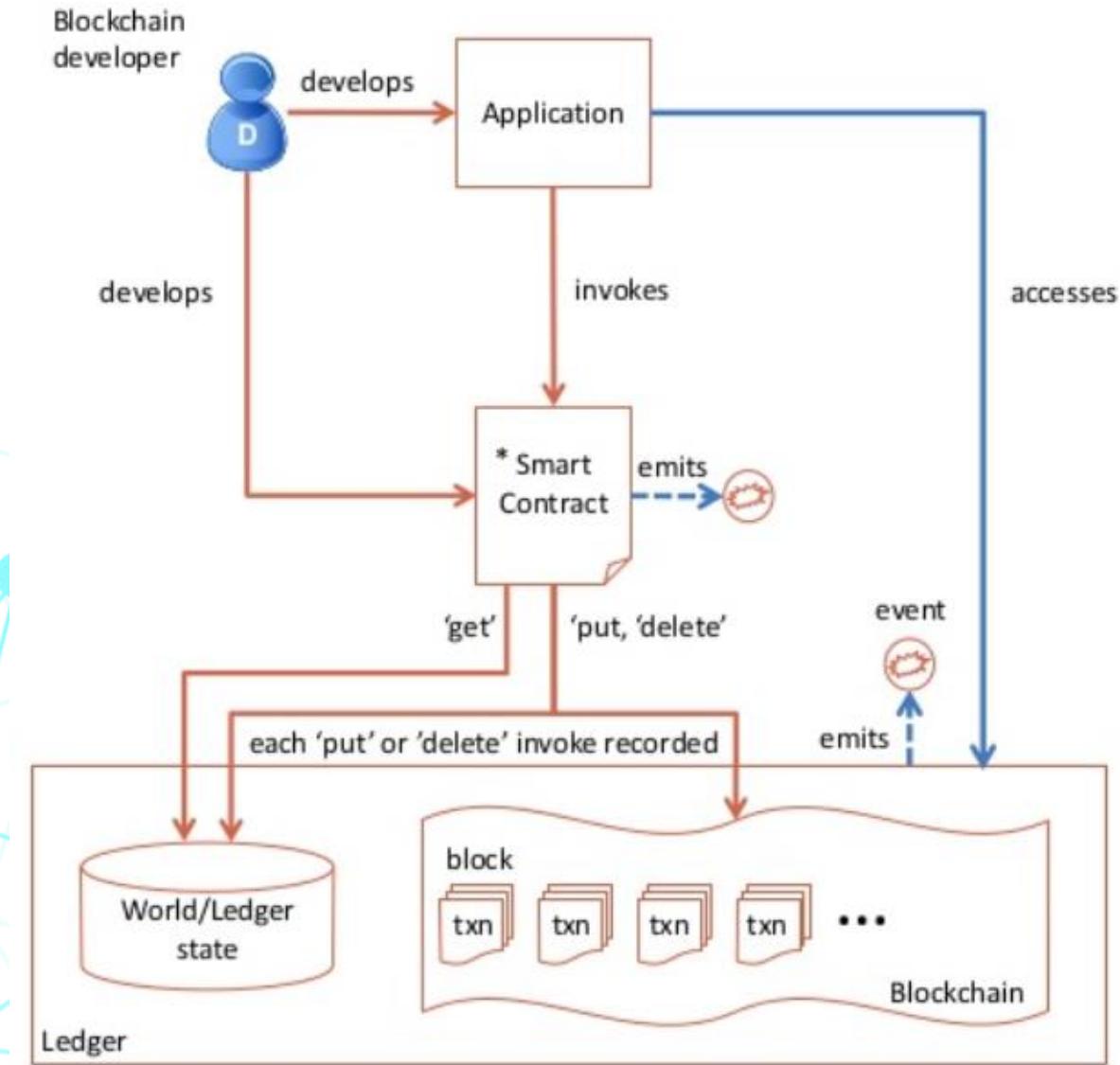
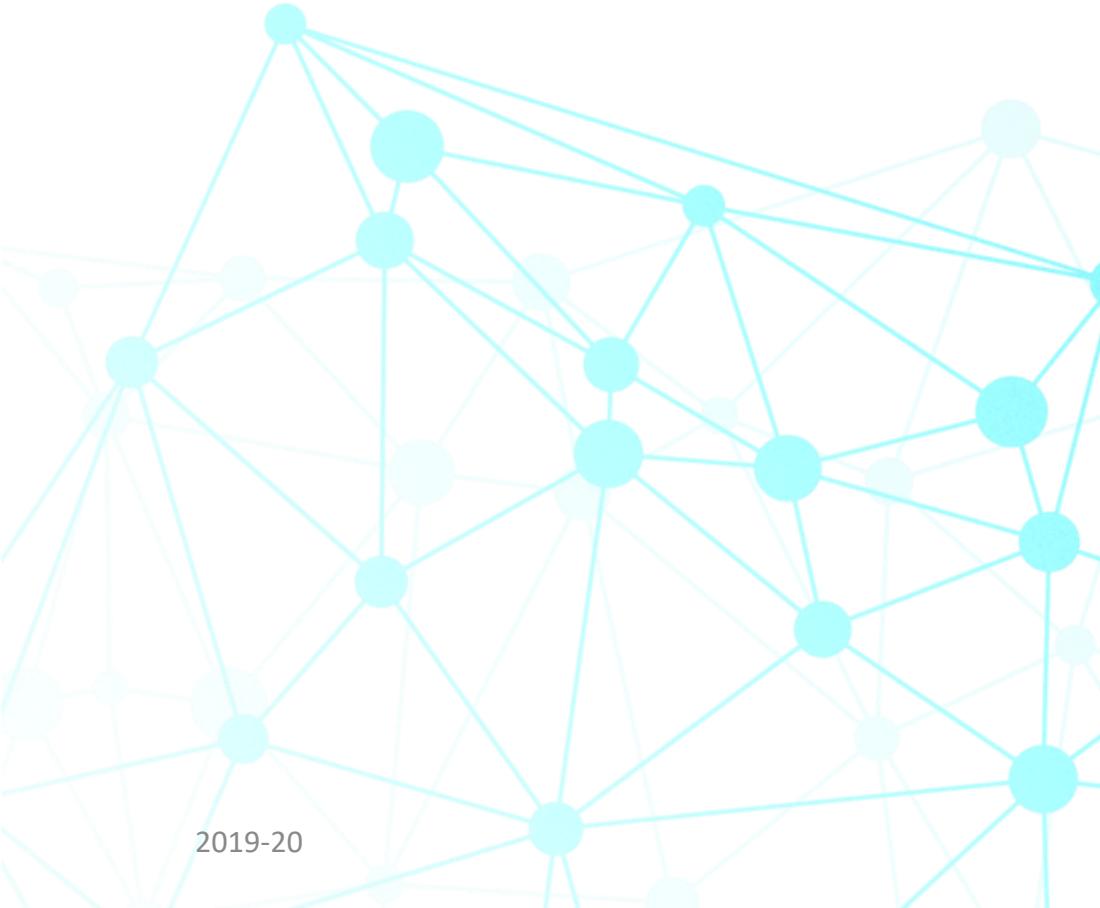
Proof of Work (PoW)

- Developed by Satoshi Nakamoto
- It is the oldest consensus mechanism used in the Blockchain domain.
- It is also known as mining where the participating nodes are called miners.
- Working : the miners have to solve complex mathematical puzzles using comprehensive computation power.
 - They use different forms of mining methods, such as GPU mining, CPU mining, ASIC mining, and FPGA mining. And the one that solves the problem at the earliest gets a block as a reward.
- This process is not that easy.

Consensus Algorithms	Blockchain Platform	Launched Since	Programming Languages	Smart Contracts	Pros	Cons
PoW	Bitcoin	2009	C++	No	Less opportunity for 51% attack Better Security	Greater energy consumption Centralization of Miners
PoS	NXT	2013	Java	Yes	Energy efficient More decentralized	Nothing-at-stake problem
DPoS	Lisk	2016	JavaScript	No	Energy efficient Scalable Increased security	Partially centralized Double spend attack
LPoS	Waves	2016	Scala	Yes	Fair usage Lease Coins	Decentralization Issue
PoET	Hyperledger Sawtooth	2018	Python, JavaScript, Go, C++, Java, and Rust	Yes	Cheap participation	Need for specialized hardware Not good for Public Blockchain
PBFT	Hyperledger Fabric	2015	JavaScript, Python, Java REST and Go	Yes	No Need for Confirmation Reduction in Energy	Communication Gap Sybil Attack
SBFT	Chain	2014	Java, Node, and Ruby	No	Good Security Signature Validation	Not for Public Blockchain
DBFT	NEO	2016	Python,.NET, Java, C++, C, Go, Kotlin, JavaScript	Yes	Scalable Fast	Conflicts in the Chain
DAG	IOTA	2015	Javascript, Rust, Java Go, and C++	In Process	Low cost network Scalability	Implementation gaps Not suited for smart contracts
POA	Decred	2016	Go	Yes	Reduces the probability of the 51% attack Equal contribution	Greater energy consumption Double signing
Pol	NEM	2015	Java, C++XEM	Yes	Vesting Transaction partnership	Decentralization Issue
2019-20				sarwan@NIELIT	Cheap Efficient	Favoring bigger fishes



Blockchain Applications and the Ledger





Blockchain applications

Application

- focus on blockchain user business needs and experience
- Calls smart contract for interactions with ledger state
- Can access transaction ledger directly if required.
- Can process events if required.



Public vs Private Blockchain



	Public	Private
Access Level	<ul style="list-style-type: none">• Anyone can participate	<ul style="list-style-type: none">• Single Organization• Participants are known and trusted
Participation	<ul style="list-style-type: none">• Permissionless• Anonymous	<ul style="list-style-type: none">• Permissioned• Identities are known
Security	<ul style="list-style-type: none">• Consensus mechanism• Proof of Work/ Proof of Stake	<ul style="list-style-type: none">• Pre-approved participants• Voting/multi-party consensus
Performance	<ul style="list-style-type: none">• Slow transaction speed	<ul style="list-style-type: none">• Lighter blockchain,• Fast transaction speed





Public Blockchain

- A Public Blockchain is a permission-less blockchain.
- Anyone can join the blockchain network, meaning that they can read, write, or participate with a public blockchain.
- They are **decentralised**, no one has control over the network, and they are secure in that the **data can't be changed once validated** on the blockchain.
- The best example of a public blockchain is Bitcoin where participants in the network (miners) are rewarded with BTC tokens.



Public Blockchain – *advantages*

- Open Read and Write
- Ledger is distributed
- Immutable
- Secure Due to Mining (51% rule)



Public Blockchain – *drawback*

- Drawback of public blockchain –
 - In a blockchain each block contains a record of many transactions on the network.
 - Creating new blocks gives out a reward, also known as the “**miner's fee**”.
 - Due to large number of participants, we need to **maintain scarcity** of the reward tokens and regulate who gets right to create the next block.
 - To achieve this, each participant in the network must solve a complex cryptographic problem (also known as “**proof of work**”).
 - Whoever solves the problem earn the right to create the next block (and gets the reward).
 - The disadvantage to this is, these problems are very resource intensive and take a substantial amount of computational power to solve.
- There is little to no privacy for transactions, nor any regulation or criteria for participants to join



Private Blockchain

- Permissioned/enterprise network, restriction on joining
- Certain restriction on transactions
- Transactional access according to participant level
- Participation rules can either be set up by existing participants, a **regulatory authority** or a **consortium**
- e.g. Linux Foundation's **Hyperledger Fabric**, designed to cater to enterprise requirements, other's **R3 Corda** and **Quorum**.
- Lighter than public blockchain, it has higher transactional throughput
- Driven by enterprises, and have the power to revolutionize many aspects of daily life



Private blockchain

- private blockchain tend to come with identity management tools or a modular architecture, where you can plug in your **own identity management solution**.
- It can be anything from a Membership Service Provider to an **OAuth solution** using Google, Facebook, LinkedIn, etc
- There are few nodes vs **12,000** nodes on Ethereum, hence lower latency and higher transactional speed.

12:38

OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.

35



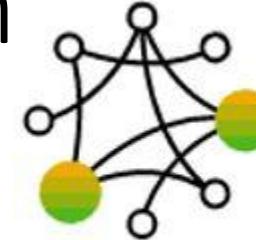
Private Blockchain – *advantages*

- Enterprise Permissioned
- Faster Transactions
- Better Scalability
- Compliance Support
- Consensus More Efficient (less nodes)



Type of Blockchain

- Public Blockchain
- Private Blockchain
- Consortium Blockchain



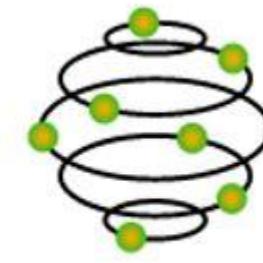
Consortium



Semi-private



Private



Public

- “trustworthy council of elders”
- *consensus process* is controlled by a pre-selected set of nodes
- it is partially private
- consolidating power is not with only one party.
- operate under the leadership of a group instead of a single entity.
- good for organizational collaboration.
- consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants. Some examples of consortium blockchains include R3 (banks) and EWF (Energy). Consortium blockchains are also referred to as **federated blockchains**.



Type of Blockchain-Semi-Private Blockchain

- Similar to private Web applications in terms of how they are managed, or simply resembles how company runs its website
- Typically target business-to-business (B2B) users.
- Users qualify according to pre-established criteria, credentials or profile, they are given access. There should not be significant discrimination for access.
- In some cases, access might be completely open. E.g. FedEx, UPS
- government entities use Semi-private blockchain, such as record-keeping, land titles, public records, etc.
- E.g. Chicago Cook County property title transfer application, or the Thomson Reuters identity tools application.



Blockchain example

