SEOULTECH

UCSLAB
Ubiquitous Computing & Security Laboratory

An Introduction of Blockchain

2019. 03. 12
Presented by
Pradip Kumar Sharma
(pradip@seoultech.ac.kr)

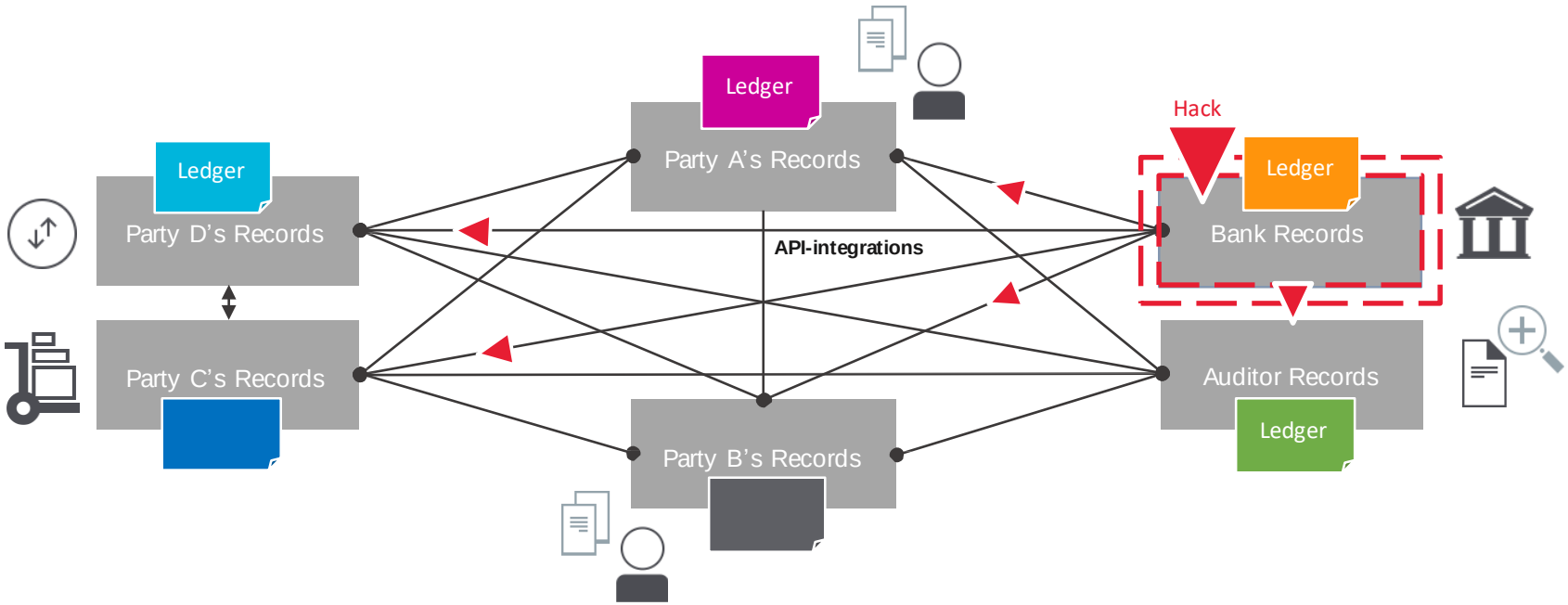
Currency

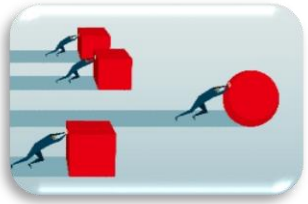
- ✓ Digital Coin
- ✓ Volatile value

Technology

- ✓ Blockchain
- ✓ Distributed shared ledger
- ✓ Cryptography
- ✓ Consensus model
- ✓ Smart contracts

Traditional Network Architecture – Separate Ledgers



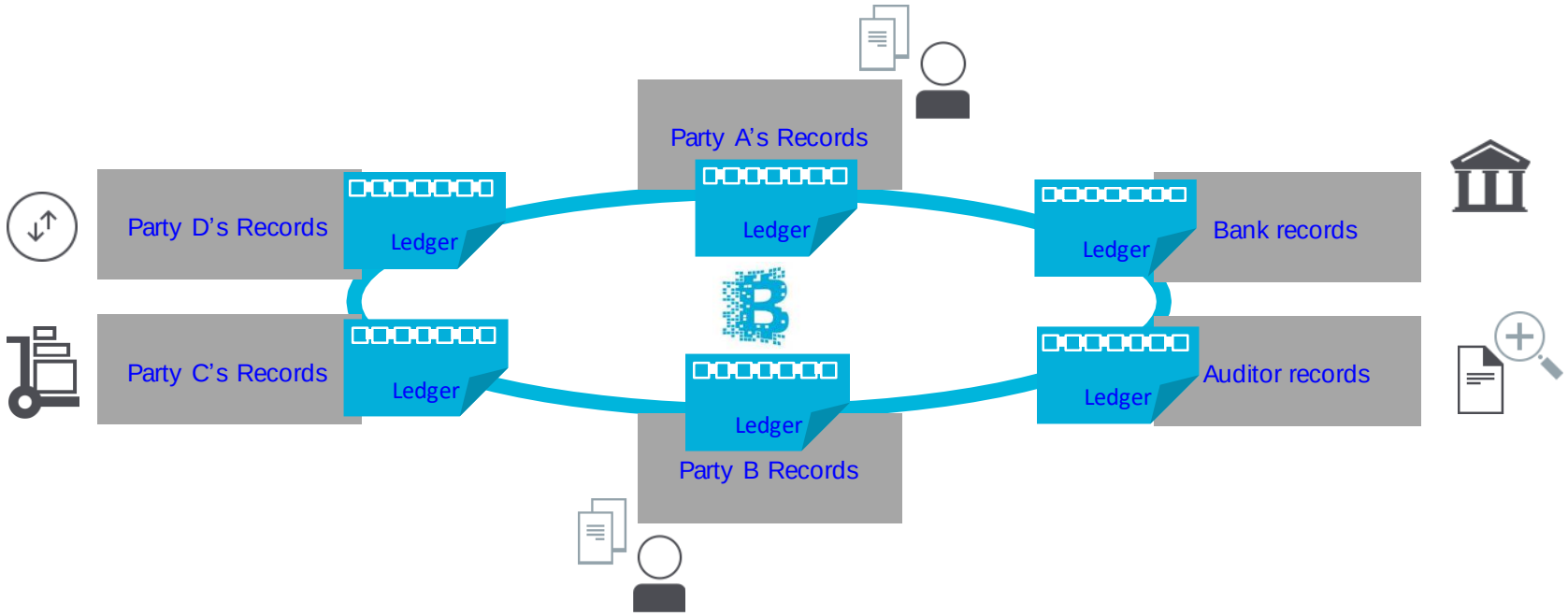


Inefficient

Expensive

Error Sensitive

Vulnerable



Consistency

Efficiency

Security

Resilience

Distributed Shared Ledger

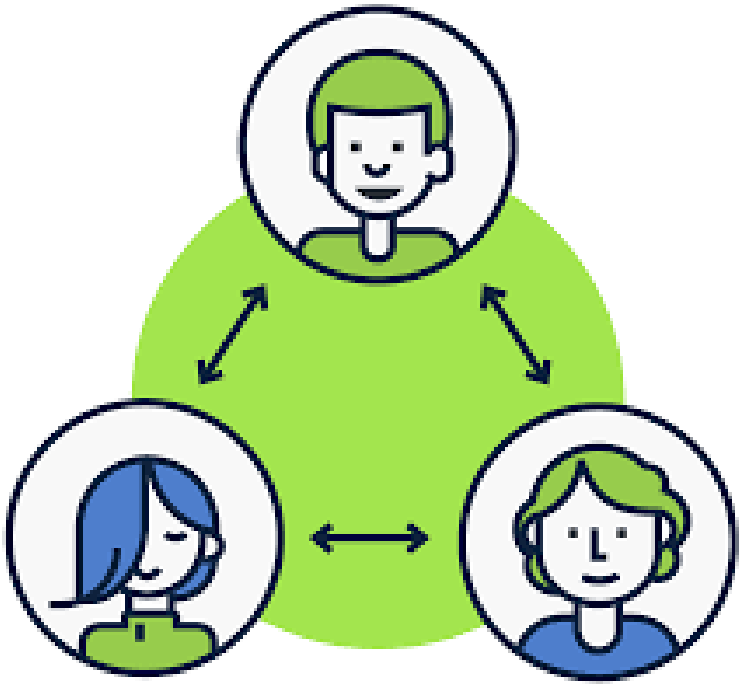
Cryptography

Consensus

Smart Contracts

A ***distributed shared ledger*** is a type of database that is shared, replicated, and synchronized among the members of a decentralized network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network.

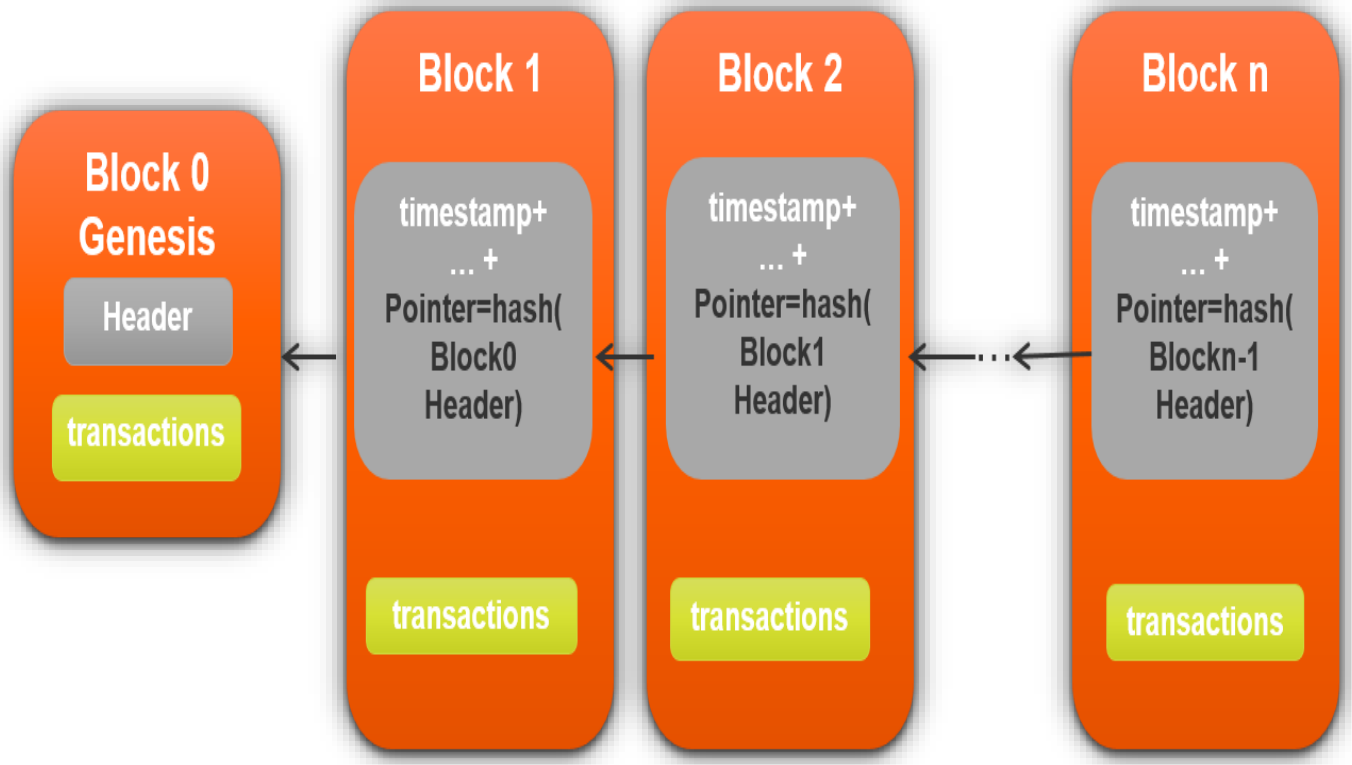
- ✓ Group of replicated logs/databases (nodes)
- ✓ Transactions distributed in blocks
- ✓ All nodes hold all transactions
- ✓ Parties identified with public key (= anonymised)
- ✓ Accessibility of transactions depending on blockchain implementation
- ✓ Resilient for failure of one or more nodes
- ✓ Group of nodes operate tamper proof



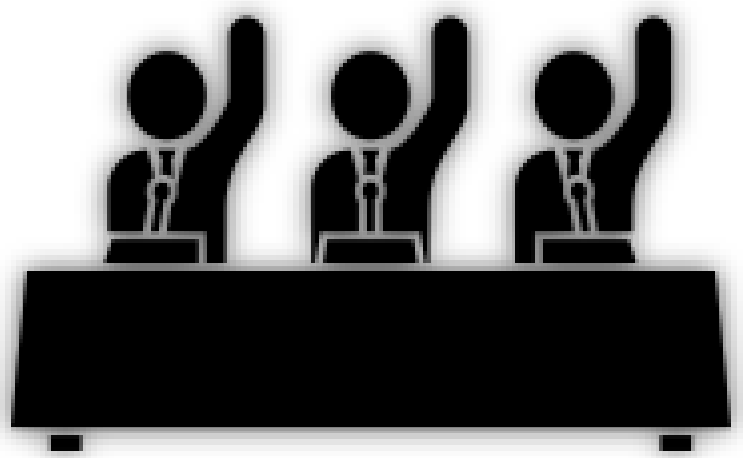
Cryptographic hashing is another fundamental piece of blockchain technology and is directly responsible for producing immutability – one of blockchain's most important features.

How does cryptographic hashing enable immutability for blockchain technology?

- ✓ The answer is that every new block of data contains a hash output of all the data in the previous block.
- ✓ Imagine a blockchain that just added its 1000th block. The data from block 999 exists in block 1000 as a hash function output. However, included in block 999's data is a hash of block 998's data, which contains a hash of block 997's data.
- ✓ By traversing the hashes backwards, every block from 1000 to 1 is linked by cryptographic hashing.



- ✓ Consensus = Majority of nodes agree on validity of transactions
- ✓ Includes validation on double-spending
- ✓ Permissionless (public) vs. permissioned (private) blockchain setup
- ✓ Proof-of-work / proof-of-stake the proof validity of node



Double spending means spending the same money twice.

Let's consider this example:

You go to Starbucks and order a cappuccino worth $10. You pay in cash. Now that $10 in cash is in the cash vault of Starbucks. By all means, you simply cannot spend the same $10 somewhere else to make another purchase.

Unless you steal it…!!!

As you paid with your $10 bill, the service provider at Starbucks instantly confirmed that you have paid, and you received your coffee in exchange for the money.

But Digital currency is ***digital*** money, not physical cash. Hence, Bitcoin transactions have a possibility of being copied and rebroadcasted. This opens up the possibility that the same BTC could be spent twice by its owner.

Types of Blockchains

	Public (eg. Bitcoin)	Private	Consortium/ Permissioned (eg. EHRs)
Network type	Decentralized	Partially decentralized	Partially decentralized - hybrid between public and private blockchains
What is it?	Anyone anywhere in the world can read and write on the network. Data is validated by every participant ("node") in the network, thus making it very secure.	Permissions to read and write data onto the Blockchain are controlled by a single "highly trusted" organisation - the owner of the blockchain.	Permissions to verify, read and write on the blockchain controlled by a few predetermined nodes. The choice of predetermined nodes can be different for every entity on the blockchain.
Benefits	-Secure as the entire network verifies transactions -Transparent as all transactions are made public with individual anonymity	-Efficient as verification is done by just owner of the blockchain -Private as the owner can control who has access to read or write on the blockchain	-Efficient as relatively lesser nodes verify transactions -Private as read and write access can be controlled by the predetermined nodes -No consolidation of controlling power
Challenges	Inefficient as all nodes need to verify the transaction	-Controlling power is consolidated to a single organization -Difficult to align many organizations to use the same blockchain	

Ref: https://devopedia.org/types-of-blockchains

What is the Proof of work?

Proof of work is a protocol that has the main goal of deterring cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests.

What is Mining?

Without going into too many details, we need consensus because anyone can create a block; while we only want an unique chain, so we want a way to decide which block we should trust.

Mining is a process of validating a transaction or block in a network by the process of complex algorithms to prove and validate the correctness of the transaction and thereby add the new block to the chain.

Proof of work and Mining in Blockchain?

Proof of work is a requirement to define an expensive computer calculation, also called mining, that needs to be performed in order to create a new group of trustless transactions (the so-called block) on a distributed ledger called blockchain.

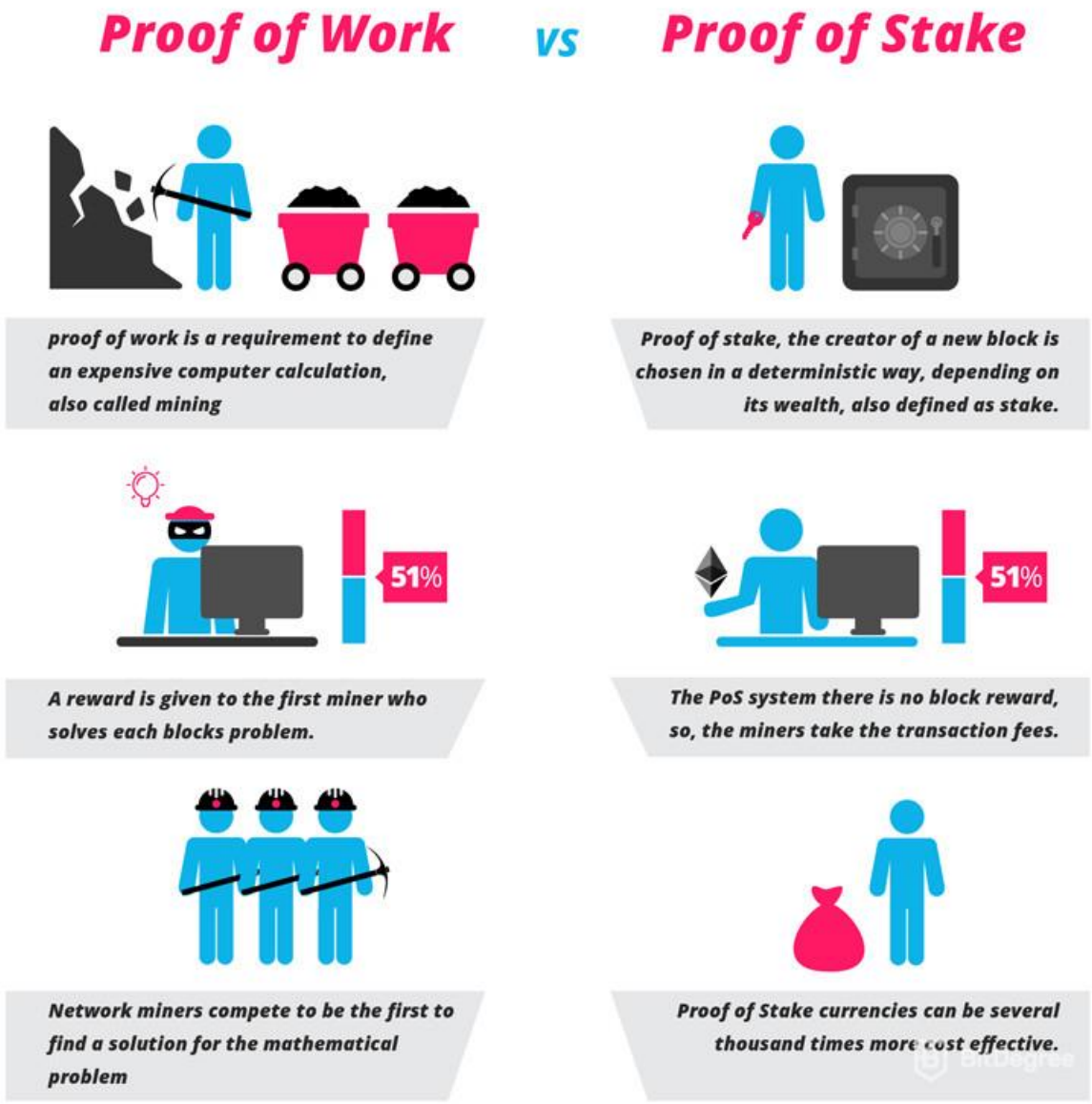
Mining serves as two purposes:

1.To verify the legitimacy of a transaction, or avoiding the so-called double-spending;

2.To create new digital currencies by rewarding miners for performing the previous task.

When you want to set a transaction this is what happens behind the scenes:

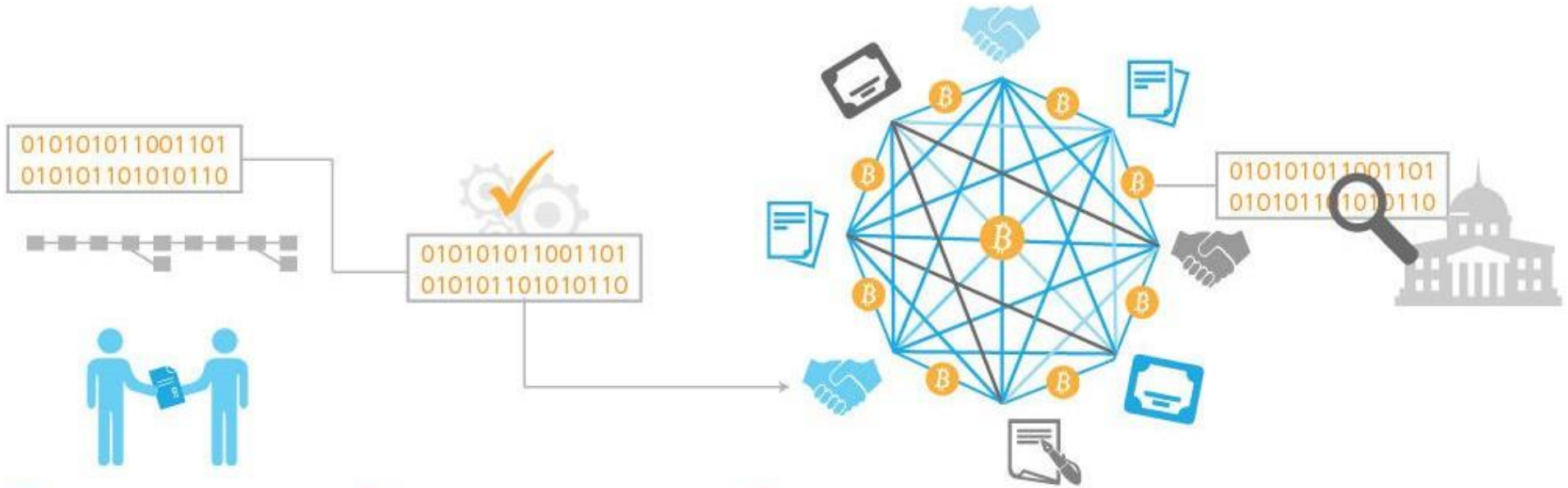
- Transactions are bundled together into what we call a block;
- Miners verify that transactions within each block are legitimate;
- To do so, miners should solve a mathematical puzzle known as proof-of-work problem;
- A reward is given to the first miner who solves each blocks problem;
- Verified transactions are stored in the public blockchain



Ref: https://www.bitdegree.org/tutorials/proof-of-work-vs-proof-of-stake/

- ✓ Business logic that can be assigned to a transaction on the blockchain
- ✓ Acts as a ‘notary’ of blockchain transactions
- ✓ Holds conditions under which specific actions can/must be perfomed
- ✓ Can’t be modified without predefined permissions

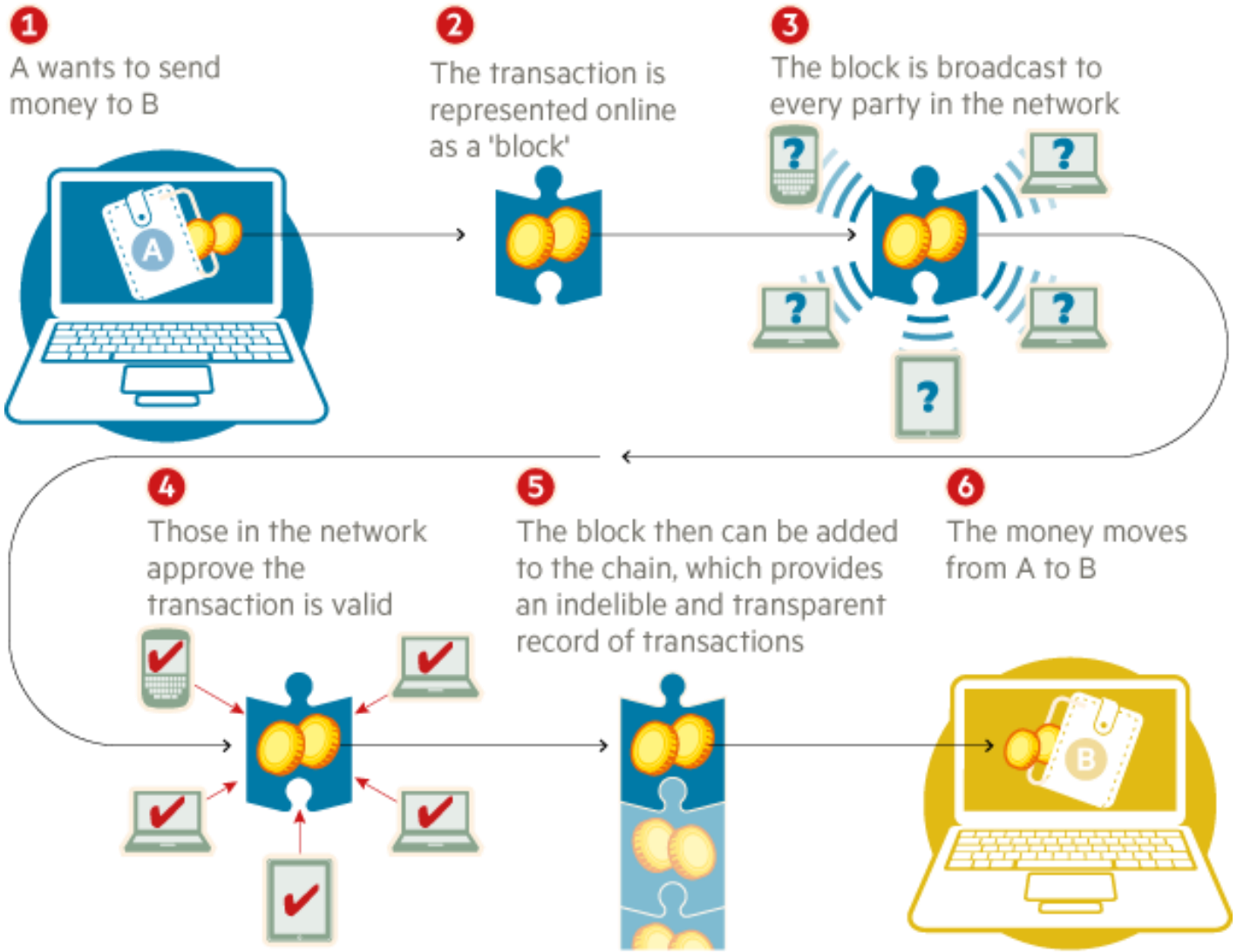
Key Component of Blockchain Technology – Smart Contracts



1. An option contract between parties is written as code into the block chain. The individuals involved are anonymous, but the contract is in the public ledger.
2. A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.
3. Regulators can use the block chain to understand the activity in the market while maintaining the privacy of individual actors' positions.

Ref: https://hackersonlineclub.com/blockchain-technology/blockchain-based-contracts/

How a Blockchain Works?



Ref: http://srini.karlekar.com/?p=370

Reduction of costs and complexity

Secure

Resilience

Reduction of errors

Auditability

Shared trusted transactions

Financial Systems

- ✓ Payments
- ✓ Securities registration & processing
- ✓ Lending

Real Estate and Agriculture

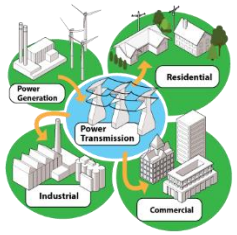
- ✓ Real estate
- ✓ Intellectual property
- ✓ Cars

E-Governance

- ✓ Voting
- ✓ Registrations (passports, driving license)
- ✓ Permits

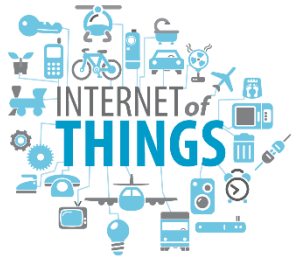
Identification & Security

- ✓ Party/device registration
- ✓ Authentication
- ✓ Access control



Smart Grid and Trading

- ✓ Document exchange
- ✓ Asset exchange
- ✓ Escrow services
- ✓ Trade agreements



Internet of Things (IoT)

- ✓ Autonomous Vehicle
- ✓ Smart Home
- ✓ Smart Healthcare
- ✓ Smart Industry

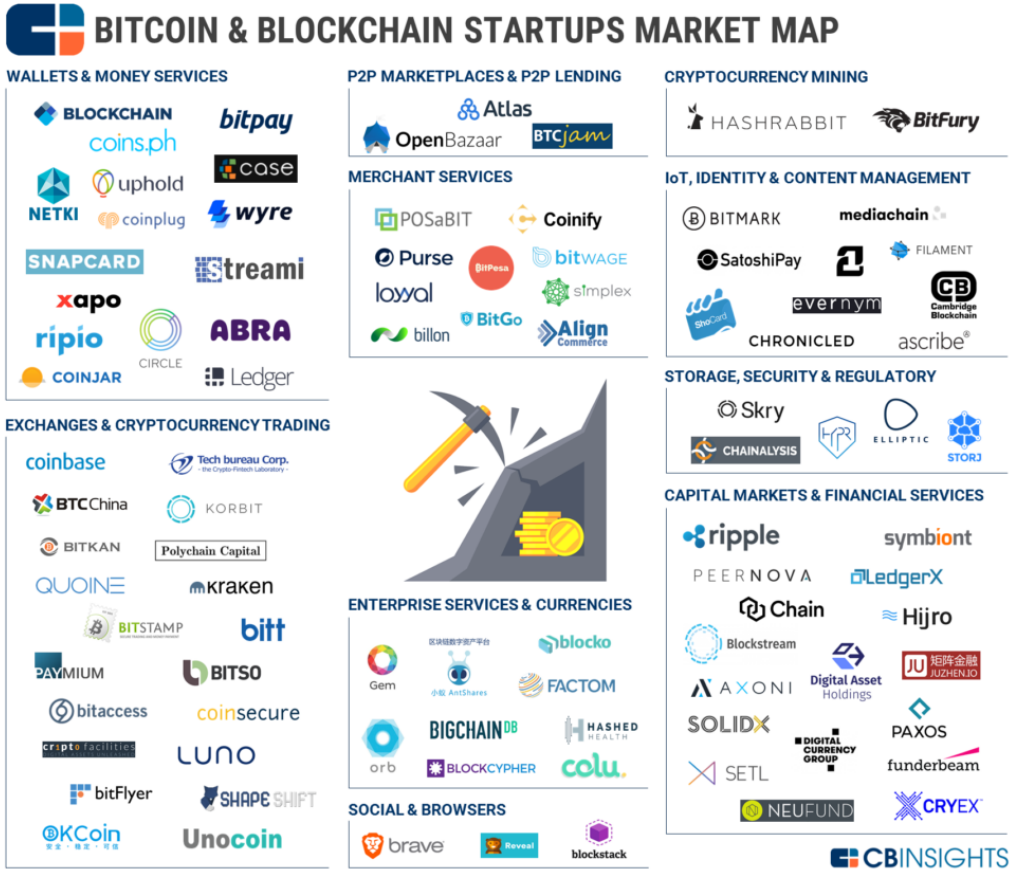
Ref: https://sharetheledger.com/2015/11/25/blockchain-and-the-internet-of-things-3/

Multiple implementations of blockchain related protocols:

- ✓ Bitcoin
- ✓ Ethereum
- ✓ Ripple
- ✓ Stellar
- ✓ Tendermint
- ✓ Factom
- ✓ Hyperledger
- ✓ …and many more

Key differentiating elements between blockchain protocols:

- Permission model (private vs. public)
- Consensus approach
- Smart contracts
- Extensibility & programmability
- APIs
- Scalability & latency
- Resource consumption



Ref: http://www.crushingcorporate.com/curated-list-blockchain-apps-platforms/

Reference

- ✓ Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access*, *6*, 115-124
- ✓ Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Communications Magazine*, *55*(9), 78-85
- ✓ Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650-655
- ✓ Sharma, P. K., Rathore, S., Jeong, Y. S., & Park, J. H. (2018). SoftEdgeNet: SDN Based Energy-Efficient Distributed Network Architecture for Edge Computing. *IEEE Communications magazine*, *56*(12), 104-111
- ✓ Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*
- ✓ Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*
- ✓ Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*

Thank you!

UCSLAB

Ubiquitous Computing & Security Laboratory