Blockchain

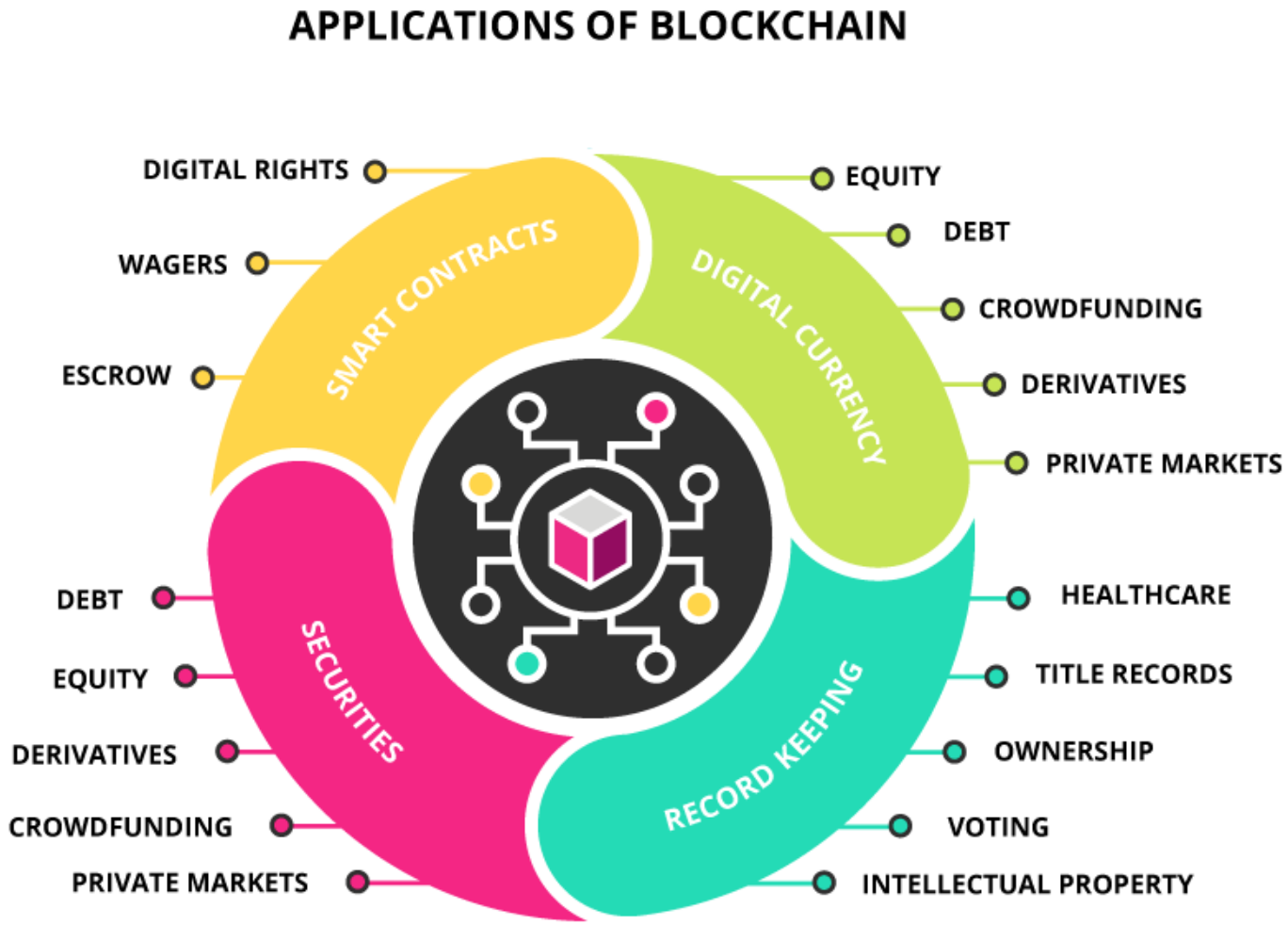
Public-Private Key, Digital Signature, Hashing

Dr. Sarwan Singh

NIELIT Chandigarh

Agenda

- Concept of Public-Private key,
- Digital Signature
- Hashing
- Ledger
- Blocks



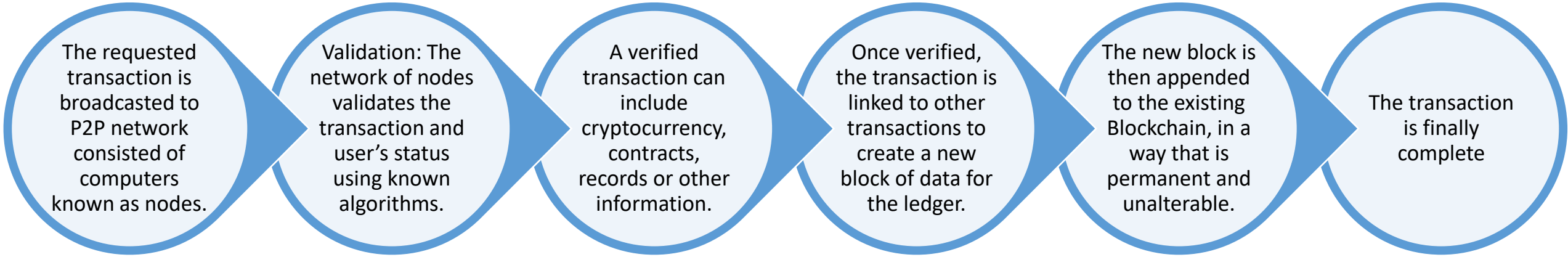
http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

References

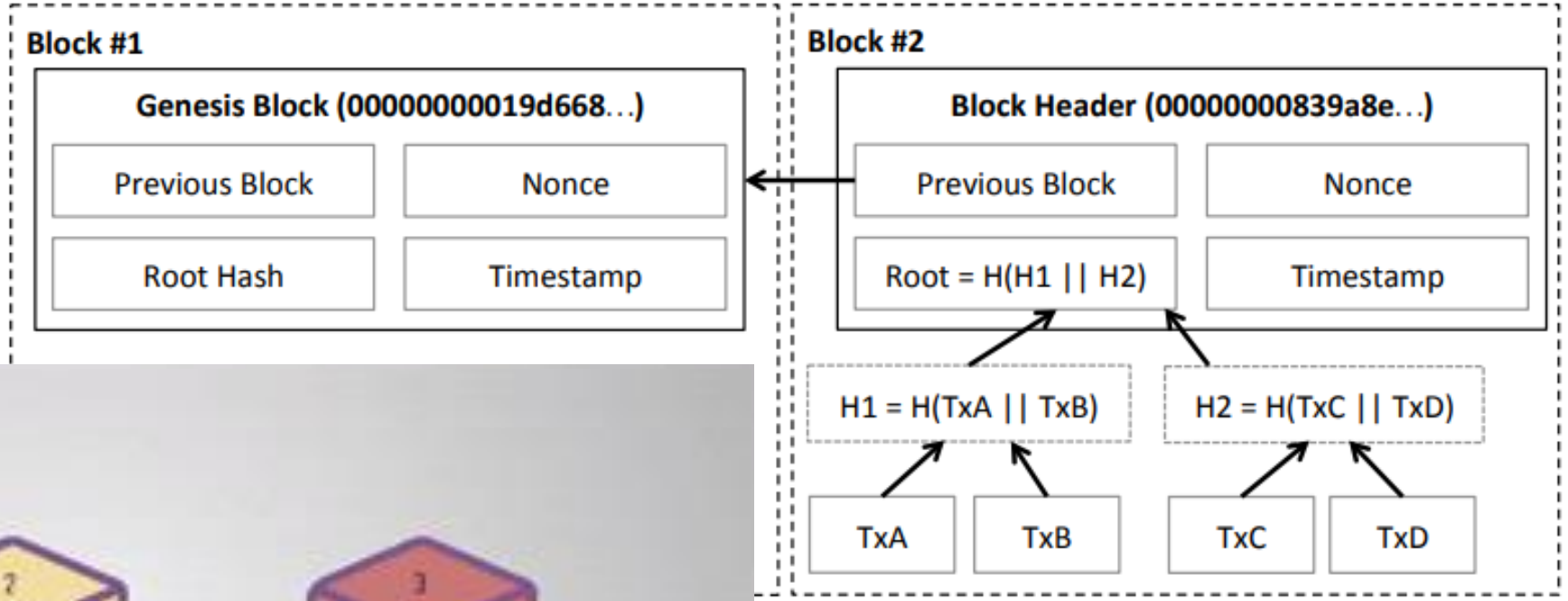
- flatworldbusiness.wordpress.com
- nvlpubs.nist.gov
- ACM Computing Surveys
- Medium.com – Blockchain
- Youngmonks.com
- Capgemini.com – Blockchain, databases vs blockchain
- consensys.net – Blockchain application areas, use-case
- Evolution of the world wide web 1.0 to 4.0 airccse.org - 3112ijwest01.pdf
- 101blockchains.com

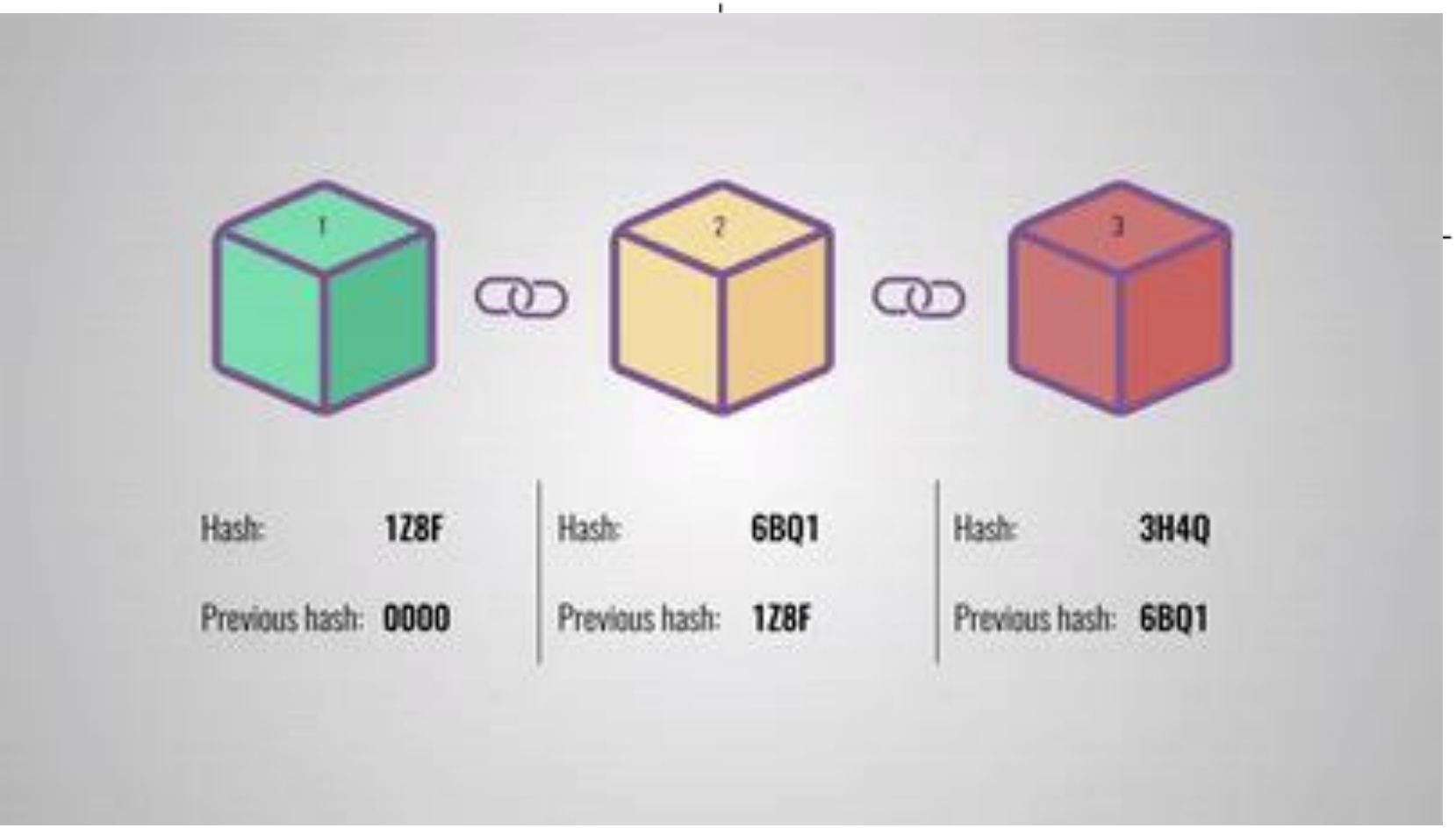
Blockchain …. *Quick review*

- The transactional data is saved in a block, then appended to the ledger



Blocks in a Blockchain





Youtube: Simply Explained

Blockchain Components

- At a high level, blockchain technology utilizes well-known computer science mechanisms and cryptographic primitives
  - Cryptographic hash functions,
  - Digital signatures,
  - Asymmetric-key cryptography
  - mixed with record keeping concepts (such as append only ledgers)
- Three basic and important capabilities that are supported by the blockchain implementation(specially in Bitcoin) are:
  - hash chained storage, merkle tree
  - Digital Signature , and
  - Commitment consensus for adding a new block to the globally chained storage

Cryptographic Hashing Functions

- Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, text, or image)

  https://emn178.github.io/online-tools/sha256.html

- Important security properties of cryptographic hashing functions:
  - They are preimage resistant. This means that they are one-way (e.g., given a digest, find x such that hash(x) = digest)
  - They are second preimage resistant. This means one cannot find an input that hashes to a specific output. (e.g., given x, find y such that hash(x) = hash(y)).
  - They are collision resistant. This means that one cannot find two inputs that hash to the same output

Cryptographic Hashing Functions

- A specific cryptographic hash function used in many blockchain implementations is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256).
- Many computers support this algorithm in hardware, making it fast to compute.
- SHA-256 has an output of 32 bytes (1 byte = 8 bits, 32 bytes = 256 bits), generally displayed as a 64-character hexadecimal string
- This means that there are $2^{256} \approx 10^{77}$, or 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 possible digest values.

Collision resistant

- The entire Bitcoin network in 2015 was 300 quadrillion hashes per second (300,000,000,000,000,000/s) .
- At that rate, it would take the entire Bitcoin network roughly 35,942,991,748,521 (roughly 3.6 x 10^{13}) years to manufacture a collision (note that the universe is estimated to be 1.37 x 10^{10} years old)

Cryptographic hash function uses

- Within a blockchain network, cryptographic hash functions are used
  - Address derivation
  - Creating unique identifiers.
  - Securing the block data
  - Securing the block header

Cryptographic Nonce

- abbreviation for “number only used once”
- A cryptographic nonce is an arbitrary number that is only used once. A cryptographic nonce can be combined with data to produce different hash digests per nonce :

  hash (data + nonce) = digest

- Only changing the nonce value provides a mechanism for obtaining different digest values while keeping the data same.
- This technique is utilized in the proof of work consensus model
- It is the first number a blockchain miner needs to discover before solving for a block in the blockchain.

Cryptographic Nonce

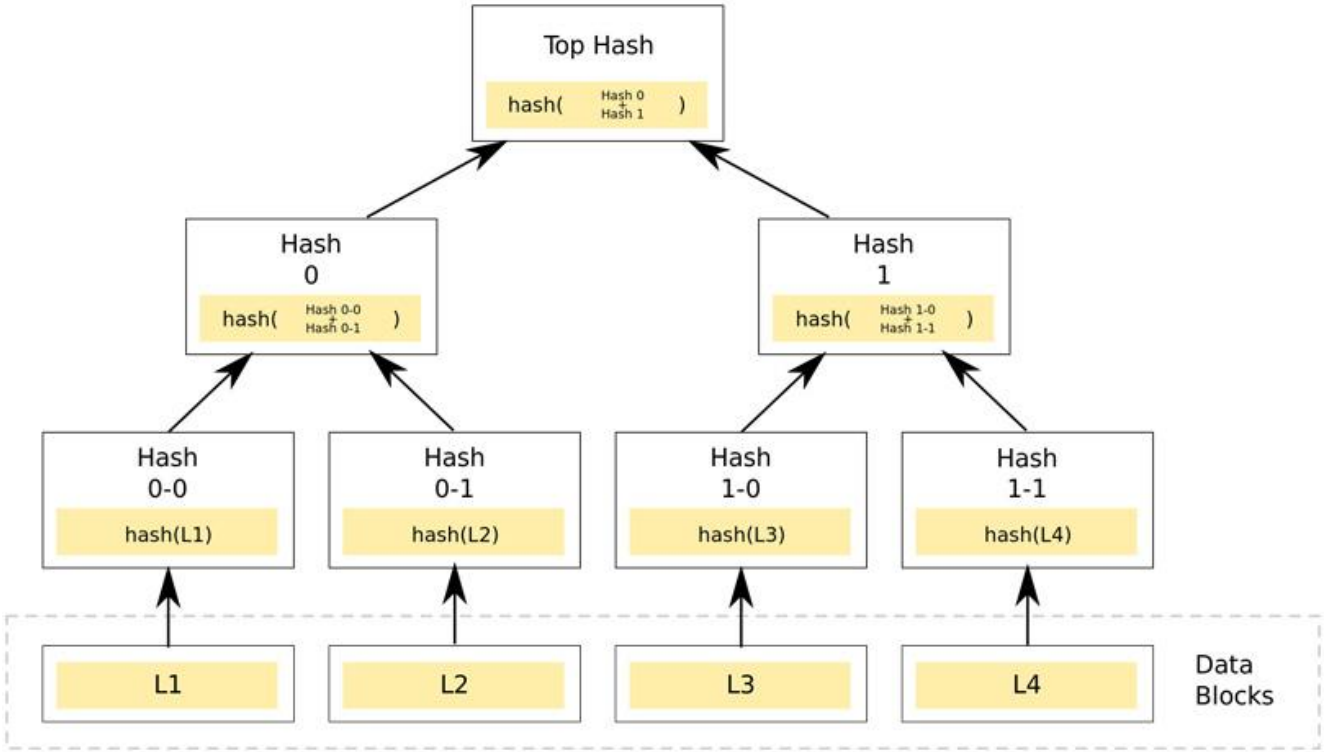
- Nonce is difficult to find and is considered a way to take out the less talented crypto miners. Thus increasing the race to mine the block among miners
- This makes the world of crypto mining an challenging job, and one often needs excellent computational power, along with smart tricks

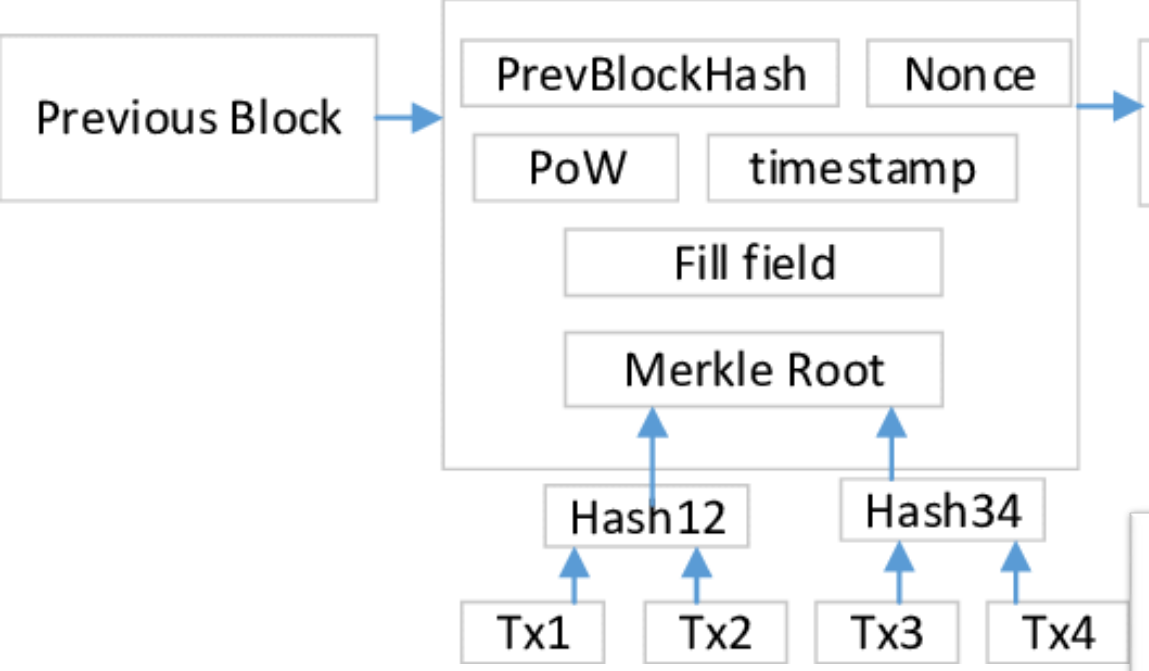
Hash Chained Storage

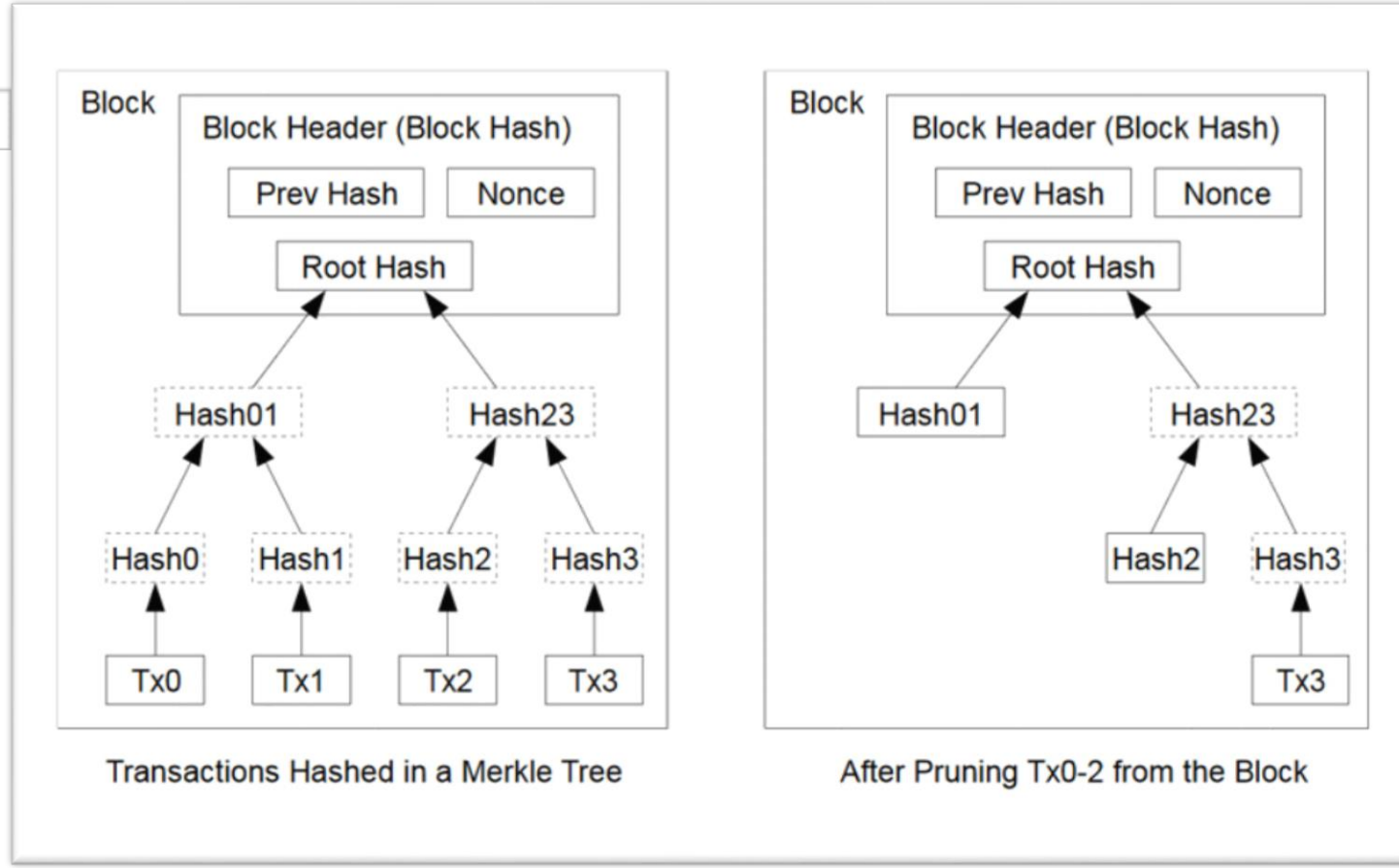
- Hash pointer and Merkle tree are the two fundamental building blocks for implementing the blockchain (e.g. Bitcoin)using the hash chained storage
- Hash pointer is a hash of the data by cryptography, pointing to the location in which the data is stored.
- {Thus, a hash pointer can be used to check whether or not the data has been tampered.}
- A block chain is organized using hash pointers to link data blocks together. With the hash pointer pointing to the predecessor block, each block indicates the address where the data of the predecessor block is stored.

Merkle Trees and Merkle Proofs

- Named after Ralph Merkle, who patented the concept in 1979,
- Merkle trees fundamentally are data structure trees where each non-leaf node is a hash of its respective child nodes.
- The leaf nodes are the lowest tier of nodes in the tree.



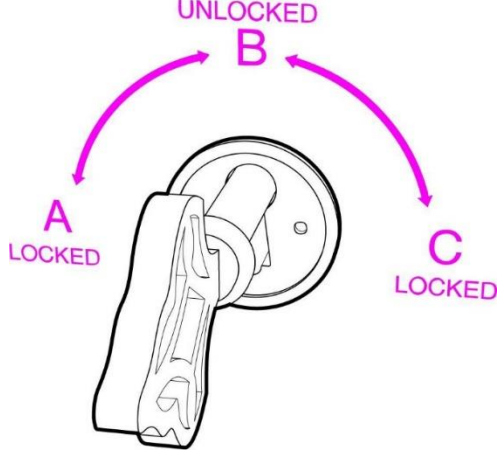

Previous Block
PrevBlockHash
Nonce
PoW
timestamp
Fill field
Merkle Root
Hash12
Hash34
Tx1
Tx2
Tx3
Tx4
Next Block

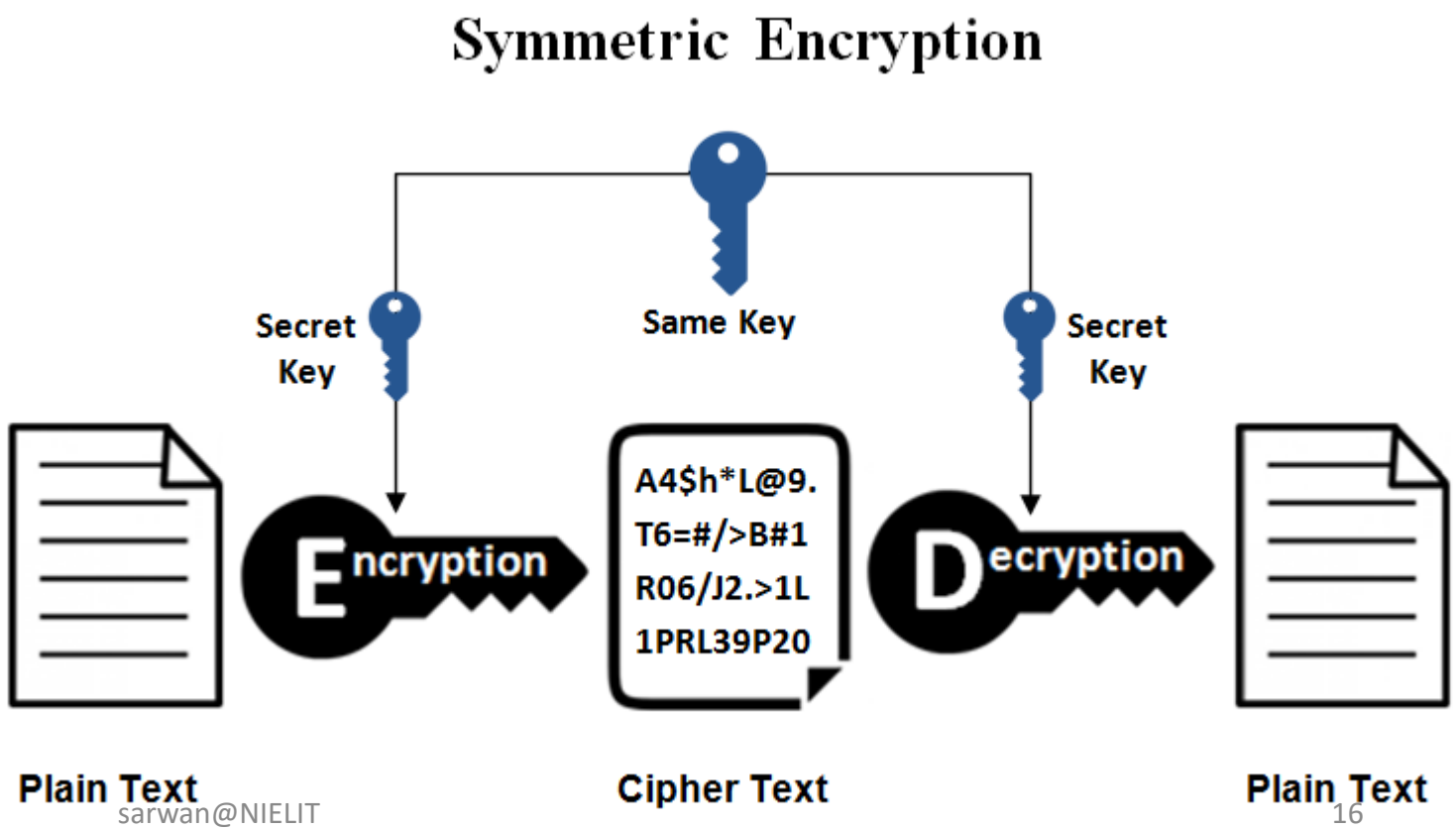

Block
Block Header (Block Hash)
Prev Hash
Nonce
Root Hash
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3
Transactions Hashed in a Merkle Tree
Block
Block Header (Block Hash)
Prev Hash
Nonce
Root Hash
Hash01
Hash23
Hash2
Hash3
Tx3
After Pruning Tx0-2 from the Block

Cryptography

- Public Key or symmetric cryptography
- one key, and you use it to encrypt (“lock”) and decrypt (“unlock”) your data

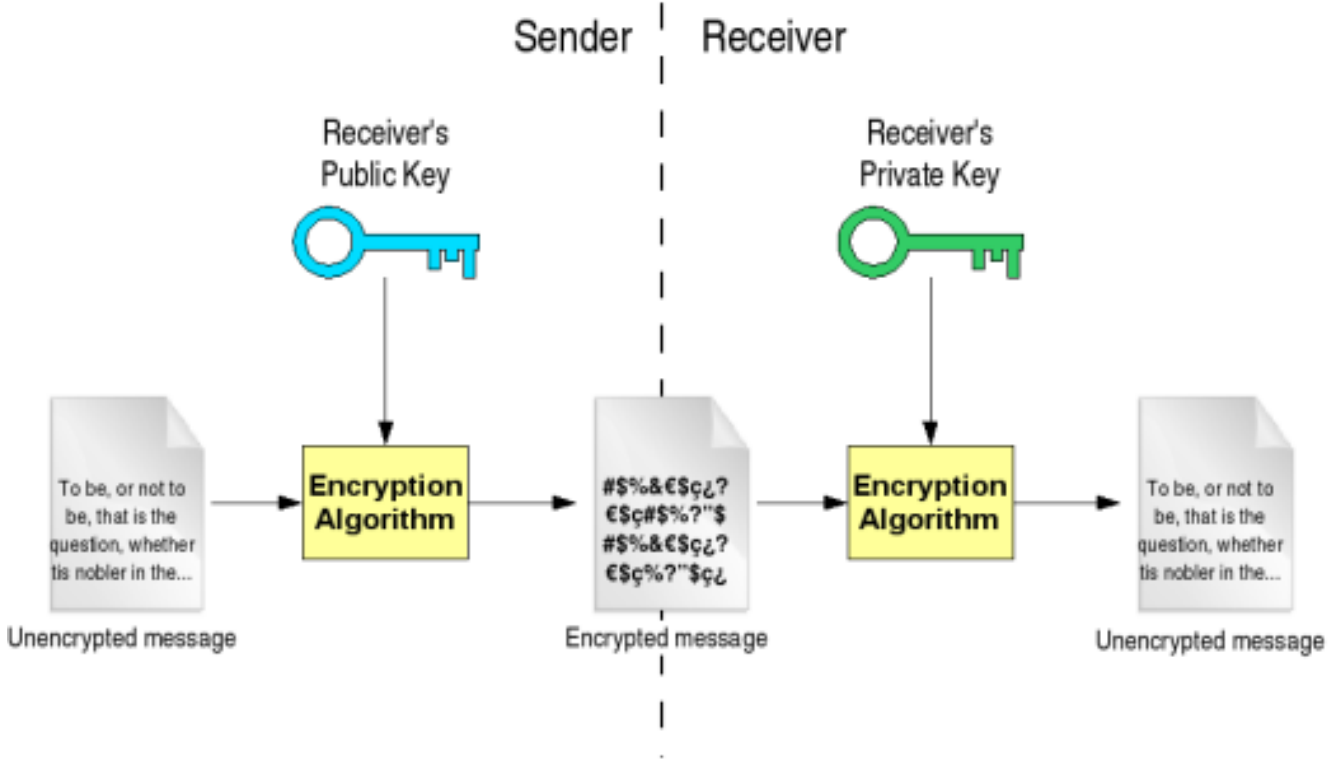
The first one can only turn clockwise (from A to B to C) and **the second one can only turn counterclockwise** (from C to B to A).





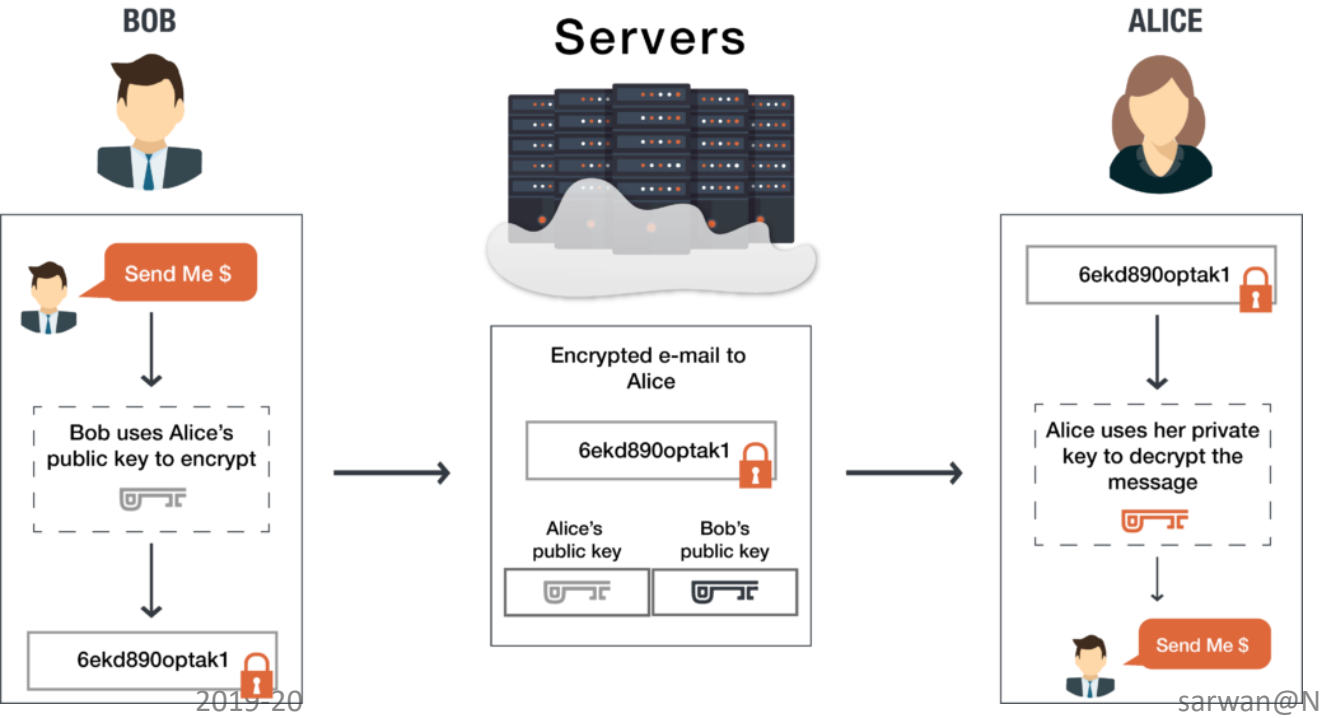
Cryptography

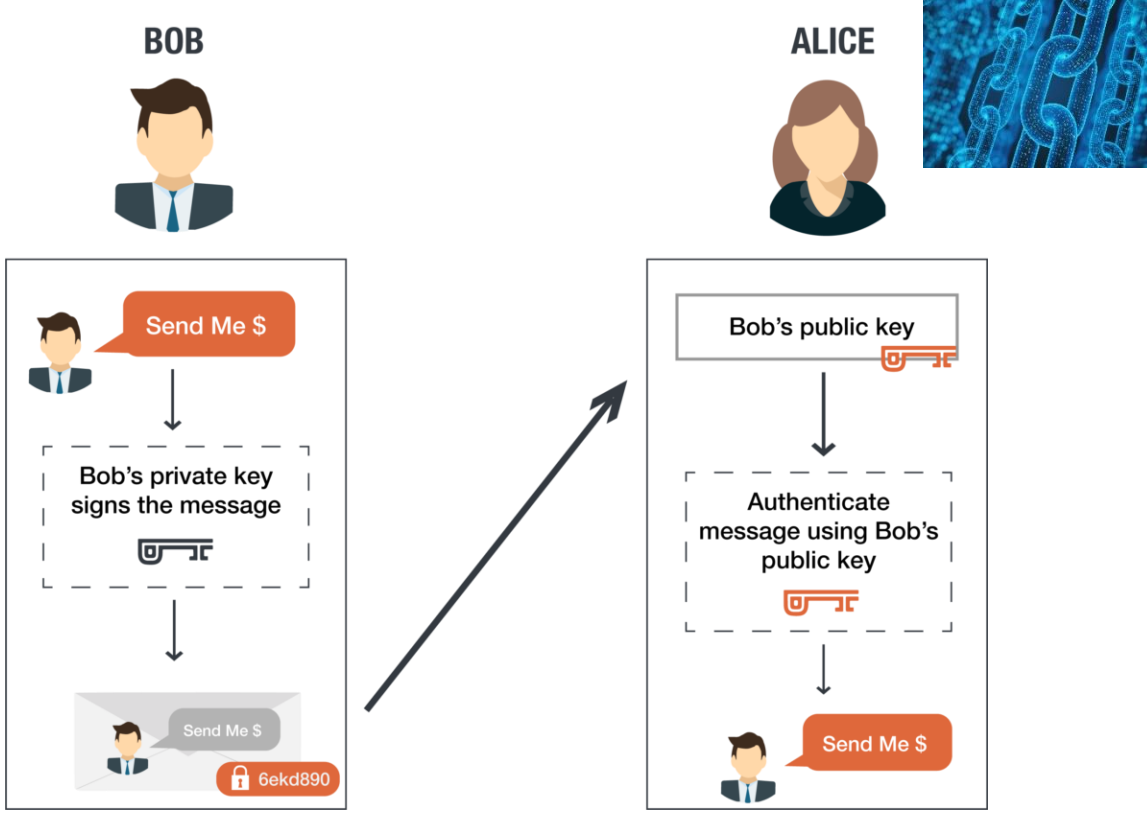
- Public-Private Key or asymmetric cryptography
- Private key is kept private to encrypt the data
- Publically available multiple copies of **'Public key'** used to decrypt the message
- We call this as **Digital Signature**



Cryptography

- Private key cannot efficiently be determined based on knowledge of the public key





Asymmetric Encryption

- different keys are used for encryption and decryption; both public and private keys come into play
- E.g. RSA algorithm, comes up with a set of a public and private key that are mathematically linked to each other

benefits of public private key encryption

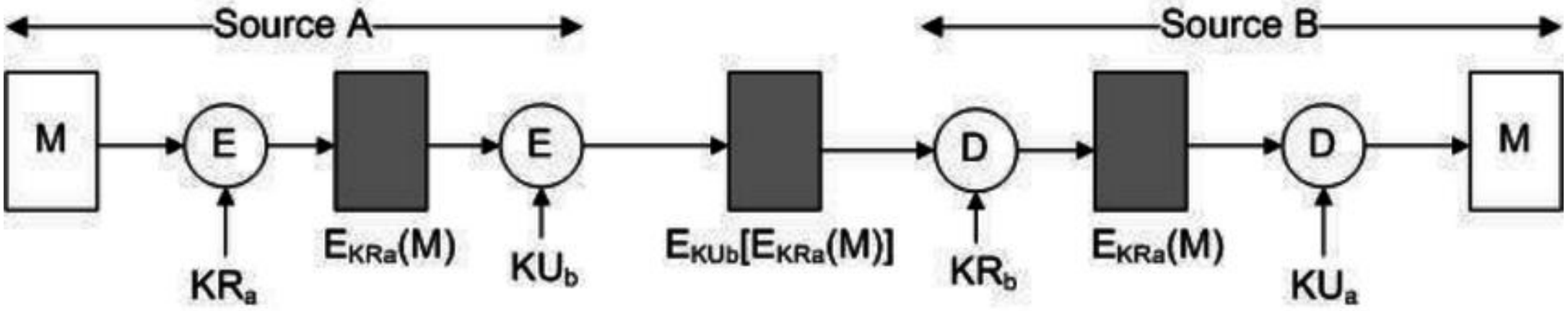
- **Confidentiality** is ensured
  - Public key used for encryption
  - Private key used for decryption
- **Integrity** is ensured
- **Authenticity** is ensured

Private Key	Public Key
Symmetric encryption.	Asymmetric encryption.
Remains in the confidential use of two individuals.	Available to everyone through the publicly accessible directory.
The possibility of key getting lost, which will render the system void.	Key is publicly held so no possibility of loss.

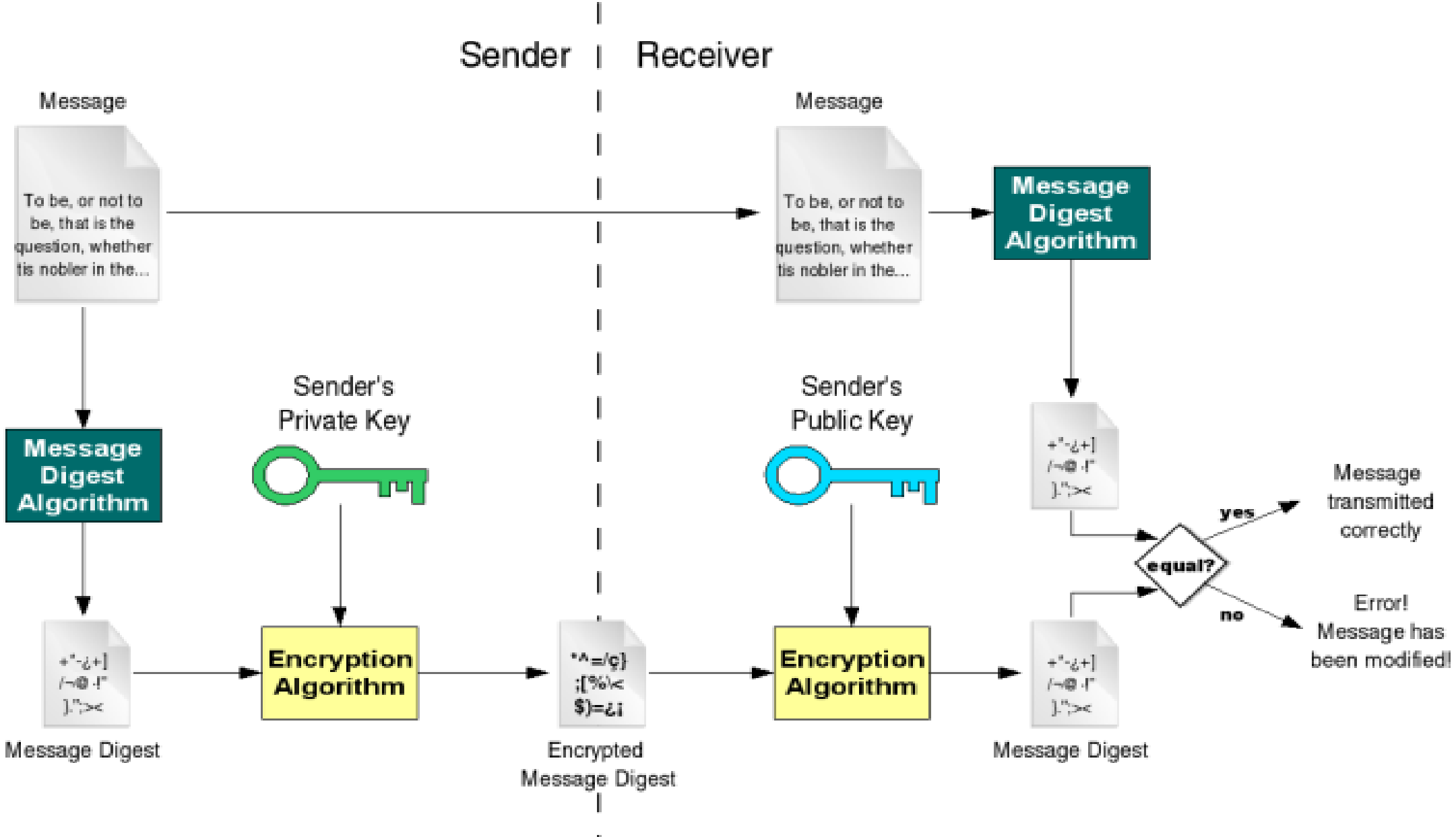
http://travistidwell.com/jsencrypt/demo/index.html

Digital Signature

- Encrypt with private key
- Decrypt with Public key
- Both confidentiality and Authentication



Digital Signature



Digital Signature

- A well defined and secure signature algorithm should have two properties.
- The first property is valid signatures must be verifiable.
- The second property is signatures are existentially unforgeable. It means that an adversary who has your public key cannot forge signatures on some messages with an overwhelming probability
- The blockchain used in Bitcoin adopts Elliptic Curve Digital Signature Algorithm (ECDSA) as its digital signature scheme for singing transactions

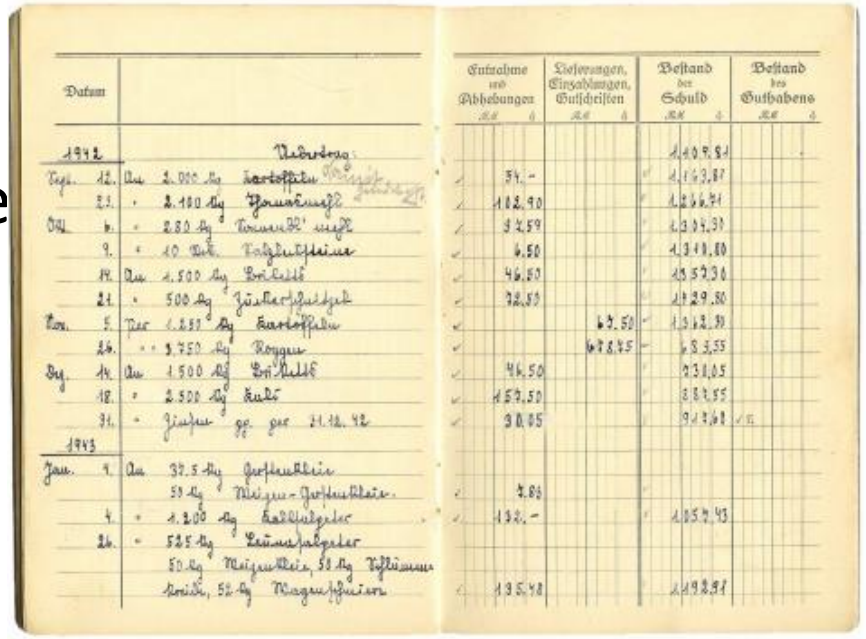
Asymmetric-key cryptography in blockchain

Use of asymmetric-key cryptography in many blockchain networks

- Private keys are used to digitally sign transactions.
- Public keys are used to derive addresses.
- Public keys are used to verify signatures generated with private keys.
- Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

Ledger

- A *ledger* is a collection of transactions.
- Throughout history, pen and paper ledgers have been used to keep track of the exchange of goods and services
- Ledger records all business activity as transactions – Databases
- Every market and network defines a ledger
- Ledger records asset transfers between participants
- Blockchain technology enables such an approach using both distributed ownership as well as a distributed physical architecture



Centrally owned vs distributed ledgers

- Centrally owned ledgers may be lost or destroyed; a user must trust that the owner is properly backing up the system.
- A blockchain network is distributed by design, creating many backup copies all updating and syncing to the same ledger data between peers.

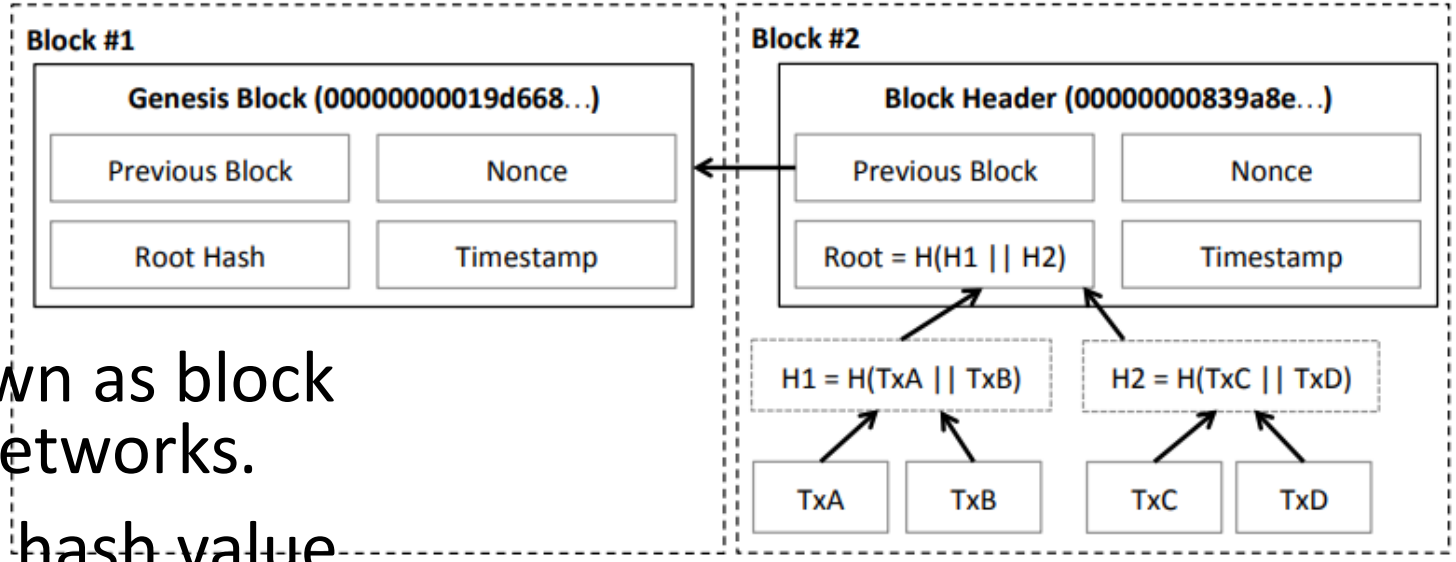
- Centrally owned ledgers may be on a homogeneous network, where all software, hardware and network infrastructure may be the same.
- A blockchain network is a heterogeneous network, where the software, hardware and network infrastructure are all different

Centrally owned vs distributed ledgers

- Centrally owned ledgers may be located entirely in specific geographic locations (e.g., all in one country).
- A blockchain network can be comprised of geographically diverse nodes, around the world

- transactions on a centrally owned ledger are not made transparently and may not be valid or may have been altered
- A blockchain network must check that all transactions are valid.
- A blockchain network utilizes cryptographic mechanisms such as digital signatures and cryptographic hash functions to provide tamper evident and tamper resistant ledgers

Blocks



Block Header

- The block number, also known as block height in some blockchain networks.
- The previous block header's hash value.
- A hash representation of the block data (different methods can be used to accomplish this, such as a generating a Merkle tree and storing the root hash, or by utilizing a hash of all the combined block data).
- A timestamp.
- The size of the block.
- nonce value


HAVE ANY
QUERY