Cryptocurrency and Blockchain Protocols

Mayank[1]

[1]Department of Computer Science and Engineering
Indian Institute of Technology, BHU, Varanasi

Feb, 2018

Outline

Outline

Currencies and conventional banking, in general

- Banks act as middle men to regulate all the fund and money transfer.
- We trust banks to take care of every single transaction.
- All the power is centralized with the banks.
- All the transactions have the names of senders and receivers
- They charge autocratic amounts whenever we make overseas transactions.
- All our transactions are open to all sorts of manipulations by the banks.
- A cryptocurrency promises to solve all of these problems.

Cryptocurrencies

- All transactions are anonymous (at least, somewhat anonymous. Public keys get recorded).
- Cryptocurrencies are decentralized.
- There is no single party with whom all the power rests.
- The power is distributed across a network of computers.
- Each of these computers maintain a database and record each transaction from the beginning of time (when the first ever block, called Genesis block, is ignited in the network marking the beginning of the currency's life)
- It is not necessary that each computer on the network stored all the past transactions. There are some computers, called **Light Nodes**, which are free from that constraint.

Basic Terminology I

Node

Typically, a computer on the network.

Consensus

A method by which all the nodes in the network are able agree on a **single** consistent view of the **past** (transaction of past).

Block

A container for transactions.

Blockchain

A data structure in which the blocks of future are linked to the blocks of past via some special links.

Basic Terminology II

Mining

It is the process, specific to Proof-of-Work consensus (Will come later in the talk), where nodes participate in a contest which results in the election of a block generator node, which is responsible for the packing some recent transactions into a new block.

Miner

The person who runs the mining process on their machines is called a Miner.

Fork

A complicated issue where more than one view of **history** exist on the network. This sometimes does require human intervention.

Basic Terminology III

Box

$box = (amount, pubkey)$, where *amount* refers to a monetary value and *pubkey* refers to the public key of the account who owns the *box*.

Transaction

$tx = [([inputbox_1, inputbox_2....]), ([outputbox_2], [outputbox_2], ...)]$

UTXO - Unspent transaction outputs

$\text{UTXO} = \{x | x \in box \wedge !(\exists y \in tx \ s.t. \ x \neq y(inputbox_i))\}$

Definitions, by graphics I

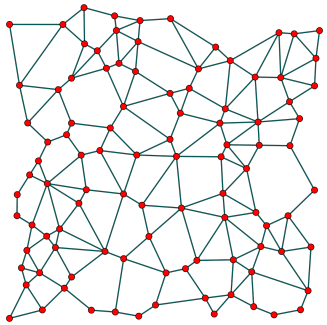

Figure: A network of Nodes

Definitions, by graphics I

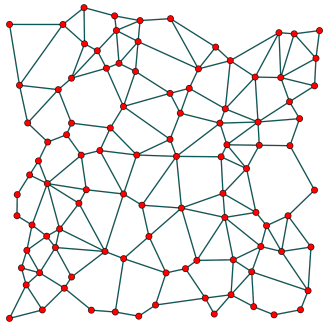

Figure: A network of Nodes

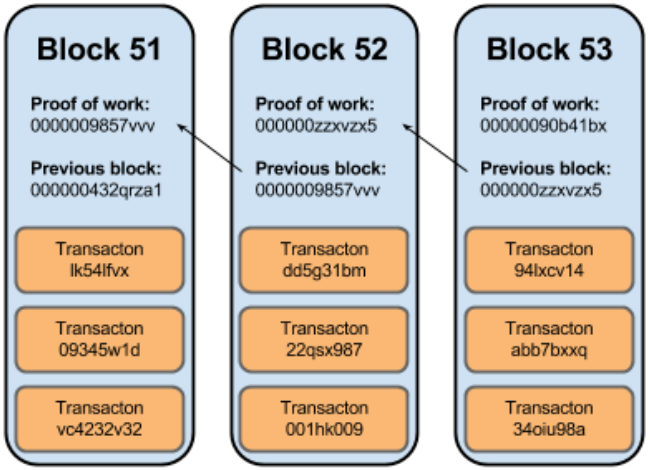

Figure: A blockchain

Definitions, by graphics II

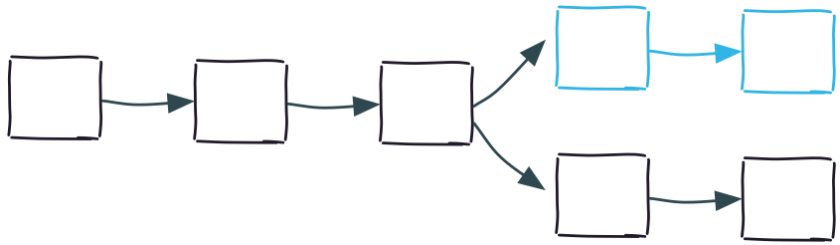

Figure: A typical fork

Definitions, by graphics III

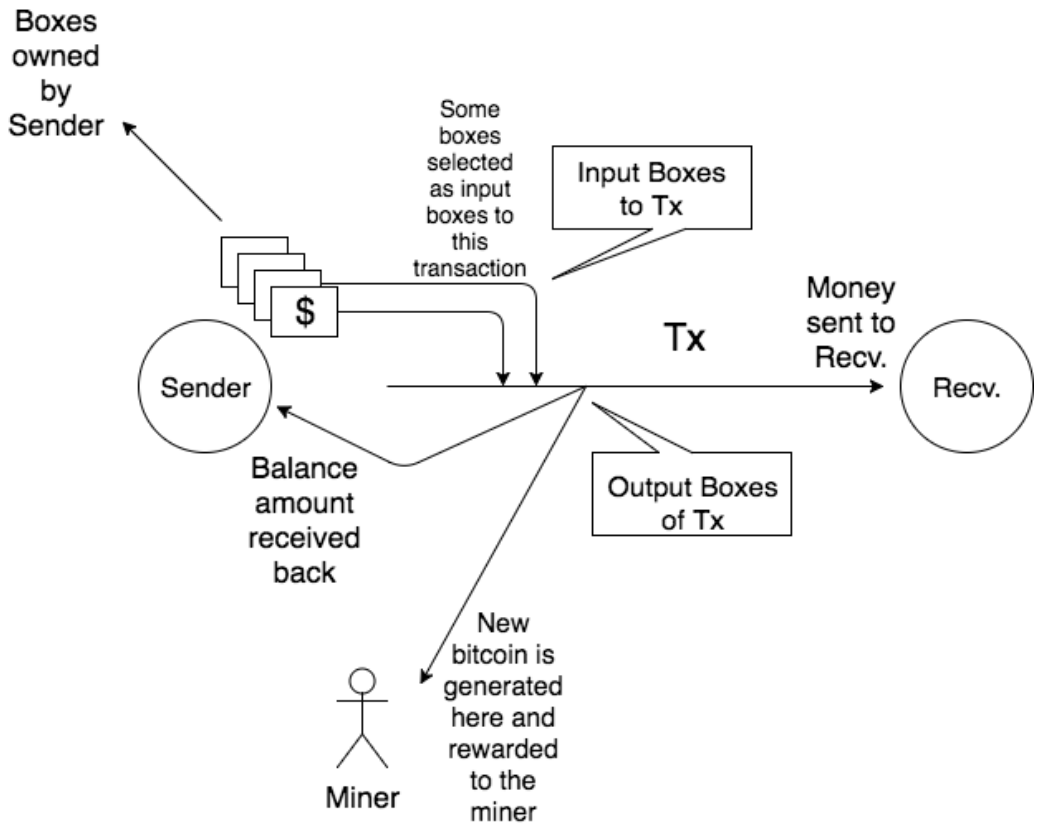

Figure: A transaction process

Cryptocurrencies - An introduction

- Untamperness: A currency which relies on complex cryptography to ensure that all the transactions remain untampered.
- Authenticated: Only a person owning a *box* should be authorized to spend it.
- Anonymous: All transactions are anonymous.
- Decentralized: It consists of a network of many nodes which help maintain the history database and run the network consistently.

Outline

Untamperness I

- This property of ensures that once transactions are added to history, or once appended the blockchain, no one should be able to change them.
- Since the blockchain is a public ledger, it should be tamper-proof so that no once can change the past transactions.

Untamperness I

- This property of ensures that once transactions are added to history, or once appended the blockchain, no one should be able to change them.
- Since the blockchain is a public ledger, it should be tamper-proof so that no once can change the past transactions.
- This property is ensured by a merkle tree.
- All the transactions are taken as leaves and the merkle tree is made from them.
- The root of the merkle tree is included in the header of the block which has all these transactions of whom the merkle tree was constructed.
- If any transaction is changed afterwards, the root hash of the transactions of the block will not match up with the one included in the header.

Untamperness, by graphics

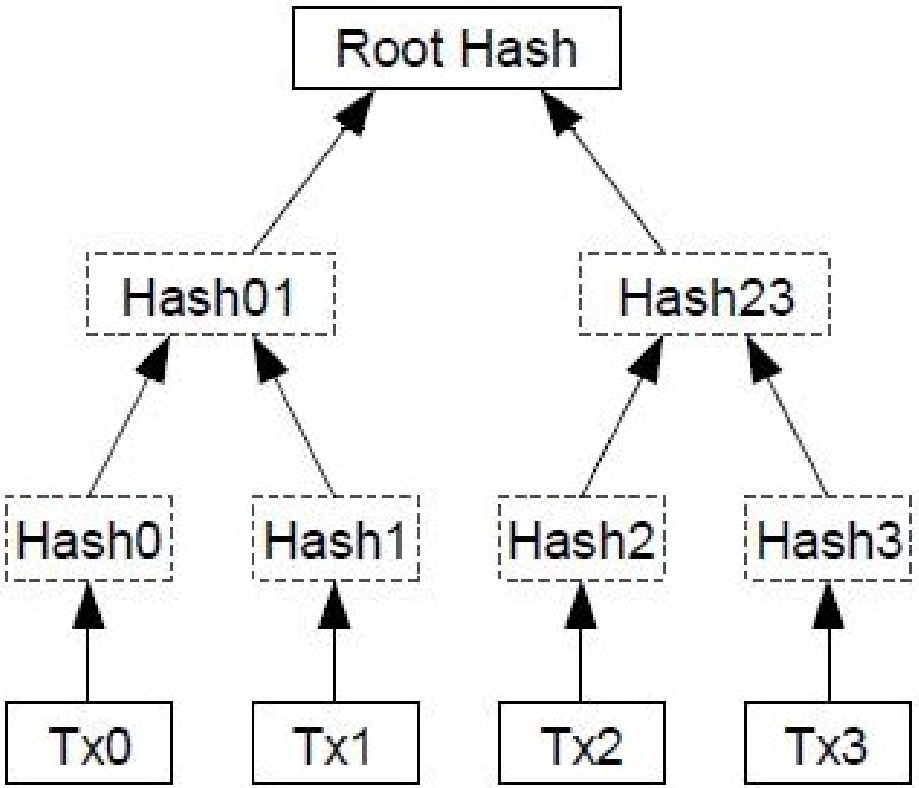

Figure: A merkle tree

Untamperness II

Let us try to see what happens when one transaction of a merkle tree is changed.

Simple Proof

Consider a 2-depth merkle tree.
Let $T_1 = (tx_1, tx_2)$ and $T_2 = (tx_1', tx_2)$
Let us represent the hash function by $\mathbb{H}$ the root of ith merkle tree by R_i.
Therefore, by definition of merkle tree
$R_1 = \mathbb{H}(\mathbb{H}(tx_1)||\mathbb{H}(tx_2))$ and $R_2 = \mathbb{H}(\mathbb{H}(tx_1')||\mathbb{H}(tx_2))$.
It is evident that $R_1 \neq R_2$.

Authenticated I

- This property makes sure that only the person who owns a box b_i can spend that box.

Authentic spending

If $\exists a$ s.t. $\forall x \in UTXO \wedge x = (c, a)$ for some c, then only the account with the public key $= c$ can spend this box.

Authenticated I

- This property makes sure that only the person who owns a box b_i can spend that box.

Authentic spending

If $\exists a$ s.t. $\forall x \in UTXO \wedge x = (c, a)$ for some c, then only the account with the public key $= c$ can spend this box.

- This is ensured by using digital signatures, which are a cryptographic primitive facilitating people to sign documents digitally such that anyone else can **verify** with an **absolute confidence** if the signature is indeed valid or not.

Digital Signatures by pictures

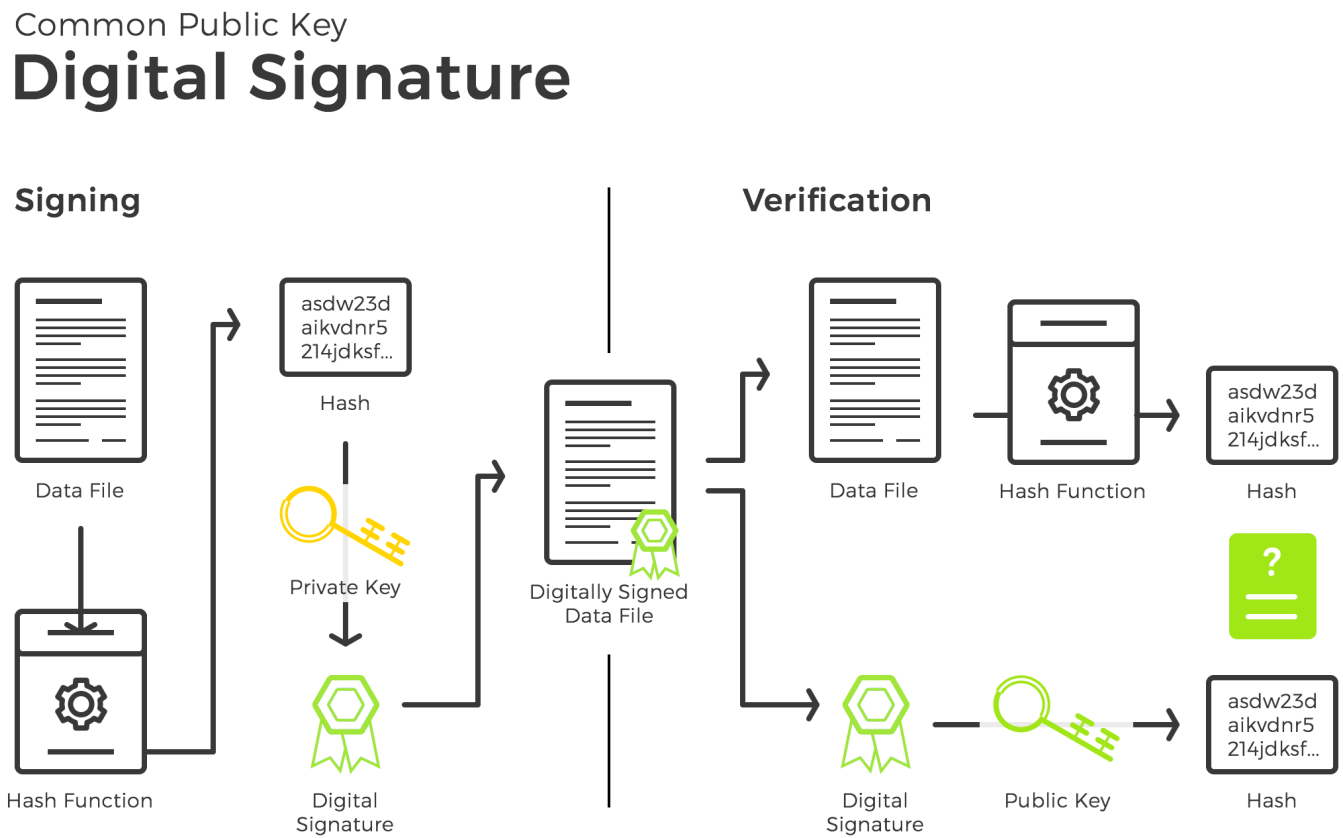

Figure: Digital Signature signing and verification

Authenticated II (Digital Signatures)

- Bitcoin uses Elliptic Curve Digital Signature Algorithm, or **ECDSA**, for this purpose.
- The account holder who wants to send some money to someone via a transaction has to sign the transaction with his **secret key**.
- Once the transaction has been signed, it is broadcast on the network and eventually gets added to a block by some miner. Here, the miner ensures that the signature to all the transactions that she includes in her block are indeed valid by using the **public key** of the signer.

Authenticated III (Elliptic Curves over $\mathbb{R}$)

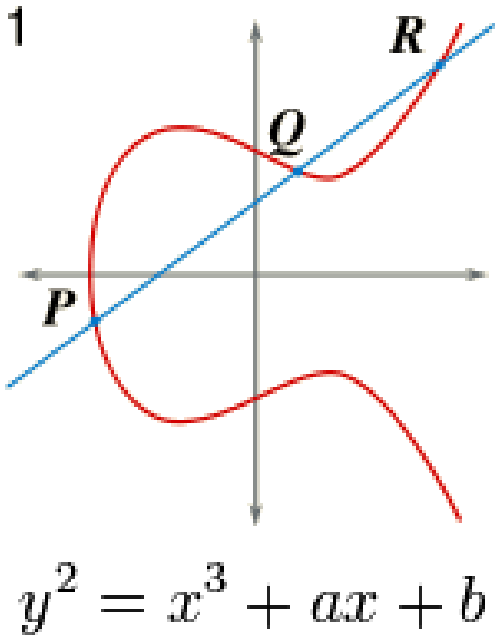

Figure: A standard elliptic curve over $\mathbb{R}$

- If we select any 2 points on the curve, then a line passing from both these points will cut the curve at atmost one more point.

Authenticated IV (Elliptic Curves over $\mathbb{F}_p$)

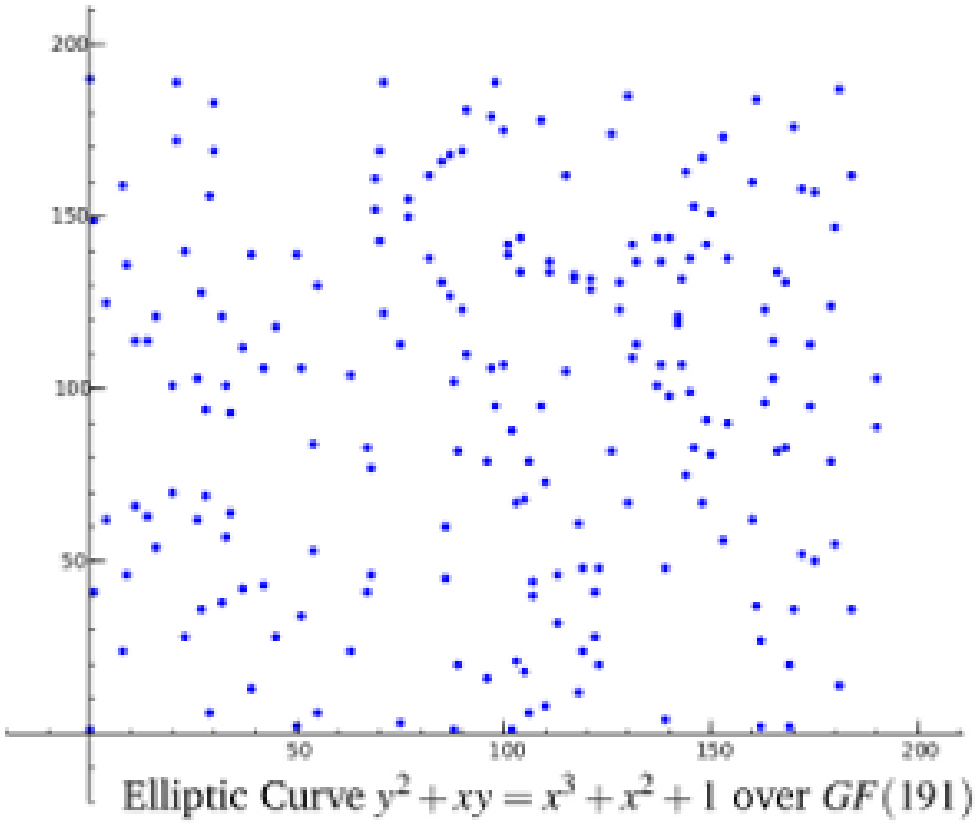

Figure: A standard elliptic curve over $\mathbb{F}_p$

- The elliptic curves of the type $y^2 = x^3 + ax + b \bmod p$ are used in cryptography and ECDSA.

Authenticated V (Arithmetic on Elliptic Curves over $\mathbb{F}_p$)

- For brevity, we will use the illustration over $\mathbb{R}$ rather than over $\mathbb{F}_p$.

Authenticated V (Arithmetic on Elliptic Curves over $\mathbb{F}_p$)

- For brevity, we will use the illustration over $\mathbb{R}$ rather than over $\mathbb{F}_p$.

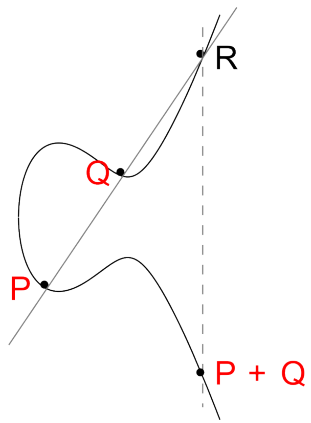

Figure: Point addition example

Authenticated VI (Arithmetic on Elliptic Curves over $\mathbb{F}_p$)

Point addition

We have 2 points P and Q and we want to find R such that $R = P + Q$
$(x_r, y_r) = (x_p, y_p) + (x_q, y_q)$
It is trivial to find that:
$y_r = \lambda(x_p - x_r) - y_p$ and $x_r = \lambda^2 - x_p - x_q$, where $\lambda = (y_q - y_p / x_q - x_p)$

Point doubling

We have 1 point P and we want to find $2P$
Same as above but the slope of the line is now the slope of the tangent at point (x_p, y_p)
$\lambda = (dy/dx)_P = (3x_p^2 + a)/2y_p$

Authenticated VII (Arithmetic on Elliptic Curves over $\mathbb{F}_p$)

Point of infinity

The point O is called the point of infinity and it is also the additive identity inside the additive group of the elliptic curve, meaning that for $P \in elliptic curve$ we have that $P + O = P$

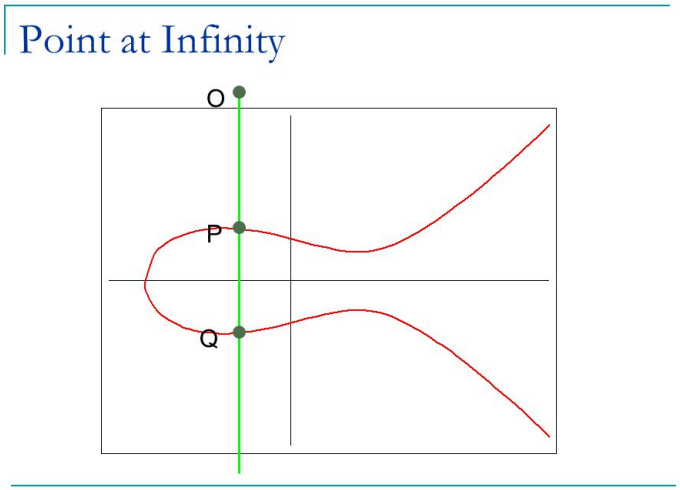

Figure: $P + O = P$

Something noteworthy

Example

Find the point R such that $P + R = O$.

Something noteworthy

Example

Find the point R such that $P + R = O$.

Let us call the point $R = -P$.

It is trivial to see that $-P = (x_p, -y_p)$. It is interesting to see that conventionally in geometry $-P = (-x_p, -y_p)$, but the case is different here.

How do we make a hard problem out of ECs?

Hardness of EC algebra

Given 2 points P and Q such that $Q = nP$ along with the description of the curve, it is **very hard to find** n.

Simply speaking, given initial and final positions on the curve, it is very hard to tell how many hops did we take to reach the final point from the start point.

ECDSA - Elliptic Curve Digital Signature Algorithm

- Key Generation
  - Alice generates a random integer d in $\mathbb{F}_p$, where p is the prime order.
  - She then selects a point Q on the curve such that $Q = d.P$, where P is the generator for the cyclic group generated by the elliptic curve.
  - Now, $pubkey = (Q)$ and $seckey = (d)$.
- Signing
  - Take a cryptographic hash function $\mathbb{H}$ and represent $e = \mathbb{H}(m)$, where m is the message to be signed.
  - Select a random number $k \in [1, n-1]$, where n is the order of elliptic curve group.
  - Calculate a curve point $(x_1, y_1) = k.P$
  - Keep $r = x_1 \bmod n$. This value r will be used to see if the signature is valid in the end.
  - Calculate $s = k^{-}\ 1(e + r.d)$.
  - If any of the values s or r is 0, then repeat the process.
  - The final signature is (r, s).

ECDSA - Elliptic Curve Digital Signature Algorithm

- Signature Verification
  - Use hash function $\mathbb{H}$ and find $e = \mathbb{H}(m)$, where m is the message which has been signed.
  - Find $w = s^{-1} \bmod n$.
  - Calculate $u_1 = e.w$ and $u_2 = r.w$.
  - Then find the curve point $(x_1, y_1) = u_1.P + u_2.Q$.
  - The signature is valid if $r \equiv x_1 \bmod n$.

ECDSA - Proof of Correctness

Proof

Let $C = u_1.P + u_2.Q$ Given that $Q = d.P$, we get that
$C = u_1.P + u_2.d.P = P(u_1 + u_2.d)$
Now subsituting the values of u_1 and u_2
$C = P(e.s^{-1} + r.d.s^{-1}) = s^{-1}(e + r.d)P$
Now putting the value of $s = k^{-}\ 1(e + r.d)$, we get
$C = (e + r.d)(e + r.d)^{-1}(k^{-1})^{-1}P = k.P$
From the signing phase, we know that x-coord of C mod $n = r$ mod n.
Hence proved.

Anonymous

- All transactions remain anonymous because the only identity associated with a transaction is the public key of the sender and receiver.
- Since there is no place where it is recorded that a person x possesses the public key y, so there is no way to link public keys to people.
- In conventional banking, our banks have our personal information associated with our account numbers.
- A person can actually possess more than one public keys by creating more than one accounts for himself and associating each key with an account.
- The only thing that keeps anyone from using anyone else's boxes is that they don't have the secret key. Remember that the secret key only remains with the person who owns the public key.
- Accounts can also be created and deleted at any time meaning that new keys can be created and old ones revoked at any time.

Decentralized

- A cryptocurrency operates in a decentralized manner meaning that the power doesn't rest in the hands of one party.
- To ensure that the power is properly distributed, a **randomized process** is done which will be covered in a while.
- Since the history database is maintained in the blockchain itself and everyone can read it. if any issue comes up, it can be easily resolved.
- Even if a node cheats, the system works fine. We won't go into much detail on this in this talk.

Outline

The Blockchain

- A blockchain is a chain of blocks of data, which happens to be a block of transactions in case of a cryptocurrency, where newer blocks are connected to the block just before it in terms of history via a special link.

The Blockchain

- A blockchain is a chain of blocks of data, which happens to be a block of transactions in case of a cryptocurrency, where newer blocks are connected to the block just before it in terms of history via a special link.
- With a constraint that the structure of blocks and their security is ensured by **cryptography**.

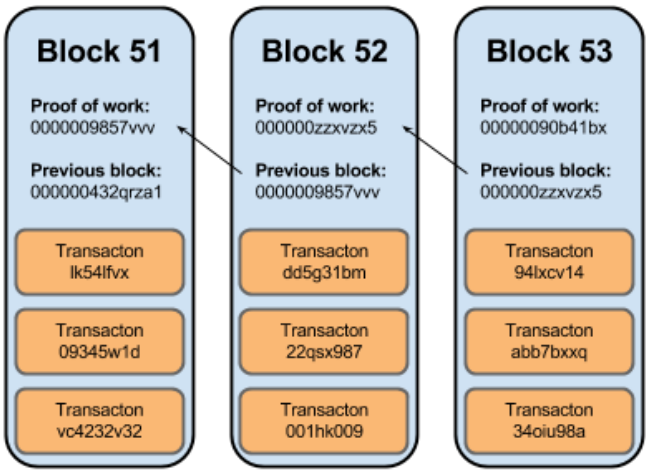

Figure: A blockchain

Outline

What is consensus?

- Since cryptocurrencies are decentralized, we need a way in which all the nodes on the network **unanimously agree** on to the present state of the system, i.e. the present blockchain which records all the past transactions.

What is consensus?

- Since cryptocurrencies are decentralized, we need a way in which all the nodes on the network **unanimously agree** on to the present state of the system, i.e. the present blockchain which records all the past transactions.
- We call these methods by which all the nodes come into agreement as **distributed consensus**.

Slot Leader Election

- All the time that the network runs for, is divided into slots and a slot is defined such that at the end of each slot, we get a **block added to the blockchain**.

Slot Leader Election

- All the time that the network runs for, is divided into slots and a slot is defined such that at the end of each slot, we get a **block added to the blockchain**.
- At the start of each slot, all the miners go through a slot leader election process which results in a miner getting elected. Now, this elected miner is called the slot leader.

Slot Leader Election

- All the time that the network runs for, is divided into slots and a slot is defined such that at the end of each slot, we get a **block added to the blockchain**.
- At the start of each slot, all the miners go through a slot leader election process which results in a miner getting elected. Now, this elected miner is called the slot leader.
- The job of this slot leader is to take some transactions from the network, verify them and create a block from those. This block is then broadcast to all the nodes on the network for them to append it to their local running copies of the blockchain.

Slot Leader Election

- All the time that the network runs for, is divided into slots and a slot is defined such that at the end of each slot, we get a **block added to the blockchain**.
- At the start of each slot, all the miners go through a slot leader election process which results in a miner getting elected. Now, this elected miner is called the slot leader.
- The job of this slot leader is to take some transactions from the network, verify them and create a block from those. This block is then broadcast to all the nodes on the network for them to append it to their local running copies of the blockchain.
- The way this slot leader is elected is governed by the **consensus protocol**.

Consensus Protocols

- These protocols define how the slot leader is selected.

Consensus Protocols

- These protocols define how the slot leader is selected.
- An important point to note here is that if a node becomes a slot leader, it **earns some money** as well. So, it is in the best interest of all the nodes to participate in the process.

Consensus Protocols

- These protocols define how the slot leader is selected.
- An important point to note here is that if a node becomes a slot leader, it **earns some money** as well. So, it is in the best interest of all the nodes to participate in the process.
- We will discuss about only 2 major types of consensus protocols today:
  - Proof-of-Work (PoW), used by Bitcoin.
  - Proof-of-Stake (PoS), used by DASH and Neo.

PoW

- In order for nodes to be selected as the slot leader, they have to solve a hash puzzle. The node which **first solves** the puzzle becomes the slot leader.
- A big problem with PoW is that just to select the slot leader, a lot of nodes are continuously **wasting energy** in trying to solve the hash puzzle and all this energy is wasted because only on of these nodes will get to become the slot leader.

PoW

- In order for nodes to be selected as the slot leader, they have to solve a hash puzzle. The node which **first solves** the puzzle becomes the slot leader.
- A big problem with PoW is that just to select the slot leader, a lot of nodes are continuously **wasting energy** in trying to solve the hash puzzle and all this energy is wasted because only on of these nodes will get to become the slot leader.

The puzzle

Suppose that the most recent node is the blockchain has a digest of X and that some header information is H. Let a hash function be denoted by $\mathbb{H}$. Then typically speaking, the puzzle is:
$\mathbb{H}(X||H||n) < T$
where n is a random nonce value and T is a target value.
T is predecided by the network and the puzzle is to find a value of n which satisfies the above inequality.

PoS

- In order for nodes to be selected as the slot leader, they participate in a secure coin tossing algorithm. Here we discuss one such algorithm called **Follow the Satoshi**.

PoS

- In order for nodes to be selected as the slot leader, they participate in a secure coin tossing algorithm. Here we discuss one such algorithm called **Follow the Satoshi**.
- All the nodes participating in the election take part in a fair coin tossing algorithm and use the blockchain itself as the broadcasting channel.
- The probability of becoming the slot leader here is directly proportional to the **amount of money** that you have in the system.
- Since we cannot ensure guaranteed output delivery in a fair coin tossing game, we can use $k-$out-of$-n$ secret sharing to ensure that honest majority gets the result of the coin tossing.

Summary

- The Cryptocurreny section of this talk gave us an insight into how they actually work. We also dived into the details and sow how ECDSA works.
- The Blockchain section of this talk covered the basics of 2 most popular consensus protocols, namely PoW and PoS.

References I


Satoshi Nakamoto
Bitcoin: A Peer-to-Peer Electronic Cash System.


J. R. Willett
The Second Bitcoin Whitepaper.


Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov
Ouroboros: A provably secure proof-of-stake blockchain protocol.


Kroll, A. Joshua, Ian C. Davey, and Edward W. Felten
The economics of Bitcoin mining, or Bitcoin in the presence of adversaries.


J. Lopez and R. Dahab
An Overview of Elliptic Curve Cryptography