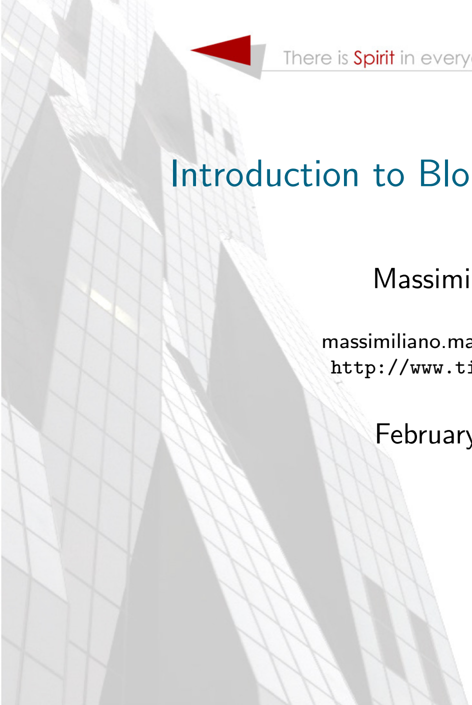


Introduction to Blockchain Technologies

Massimiliano Masi

massimiliano.masi@tiani-spirit.com
http://www.tiani-spirit.com

February 21, 2018

Outline

1. A bit of cryptography
2. History of Blockchain
3. The blockchain of Bitcoin
4. Ethereum blockchain
5. ERC-20

Confidentiality (or Secrecy)

Confidentiality (or Secrecy)

Guarantees that the useful information contained in messages is accessible only to authorized parties. In other words, confidentiality guarantees that (parts of) information is not disclosed to unauthorized peers. It can be achieved by cryptography and access control

Integrity

Integrity

Guarantees that a message is transmitted and it arrives to the latest recipient without any modifications made by unauthorized third parties, or, at least, such modifications, if made, are known to the recipient. It can be achieved by digital signatures and hash functions

Authentication

Authentication

Ensures that the origin of a message is correctly identified, and that has not been altered

- *Data Origin Authentication*: guarantees that the message is sent by the declared sender (e.g., S/MIME, PGP)
- *Peer Entity Authentication*: in a multiparty connection, guarantees that the identity of a party is the one declared (e.g., the claiming identity has not been impersonated)

It can be achieved by channel authentication, IA&A, digital signature, tokens, etc...

Non-Repudiation

Non-Repudiation

Guarantees that the sender of the message will not have the possibility to deny to have sent the message itself. In other words, the operation “send message” can be proven in front of other parties. It can be achieved by means of digital signatures, timestamps

Encryption

Two types of encryption:

- Symmetric: Alice and Bob shares a secret, K

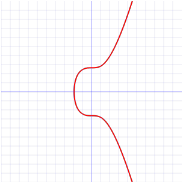
$$D_K[E_K[M]] = M$$

$$\forall M, M', \text{ if } M \neq M', \; E_K[M] \neq E_K[M']$$

- Asymmetric: Alice and Bob have their own respective secrets K_A^-, and a public part K_A^+

$$D_{K_A^-}[E_{K_A^+}[M]] = M$$

Elliptic Curve Factorization



- It is a type of public key cryptography
- `secp256k1` is used by bitcoin
- $y^2 = (x^3 + 7) \text{ over } (\mathbb{F}_P)$ where $\mathbb{F}_P$ is a finite field of prime order p
- Example: $K = k * G$, where k is a random number and G is a point in the curve. k is the private, and K is the public. $K = (x, y)$, thus a bitcoin address is: $0x00 + Base58(RIPEMD160(SHA256(K)))$

Hash Function

One Way Hash Function

A function H that maps an arbitrary length message M to a fixed length message digest MD is a one-way hash function if

1. It is a one-way function
2. Given M and $H(M)$, it is hard to find a message $M' \neq M$ such that $H(M') = H(M)$

Example of such functions are MD5, or the SHA family (including Keccak).

Digital Signature

The digital signature permits to the receiver

- To verify the authentication of the message
- To verify the integrity of the message
- To verify non-repudiation

$$A \rightarrow B: \; M \| E_{K_A^-}[SHA(M)]$$

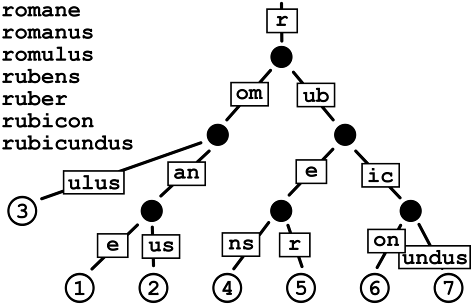
B verifies the signature as:

- $hash \; = \; SHA(M)$
- $hash' \; = D_{K_A^+}[E_{K_A^-}[SHA(M)]]$
- $if \; (hash == hash') \; then \; OK \; else$ CALL MALLORY!

Trie

A re*trie*val is a data structure (a tree) used in indexing strings[1].

```
1 romane
2 romanus
3 romulus
4 rubens
5 ruber
6 rubicon
7 rubicundus
```



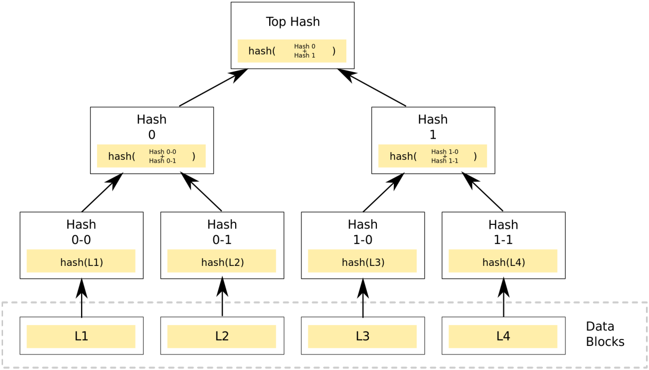
Key Concept

A trie is a tree structure where every path from the root to a leaf defines a string. Two or more strings that have the same prefix share the path from the root up to the end of the common prefix.

[1] A. Bhattacharya, *Fundamentals of Database Indexing and Searching*, CRC Press. 2015

Merkle tree

A Merkle tree is a data structure (a tree) in which each leaf node is a hash of a block of data, end each non-leaf node is a hash of its children[2].



[2] `https://medium.com/@evankozliner/merkle-tree-introduction-4c44250e2da7` and `https://www.codeproject.com/Articles/1176140/Understanding-Merkle-Trees-Why-use-them-who-uses-t`

Where Satoshi finds his roots

- The first concept of blockchain was introduced by Haber et al.[3], the digital safety deposit box
- Schneier et al[4] introduced the concept of Secure Logs (avoiding attackers to gain knowledge by accessing logs)
- Vishnamurty et al[5] where a token was used to keep p2p file trading in check, ensuring consumers be able to make micro payments to suppliers for their services.
- Szabo [6], is also a reference on the topic

⇒ Bitcoin's technology completed the puzzle!

[3] S. Haber, and W.S. Stornetta, *How to timestamp a digital document*

[4] B. Schneier, J. Kelsey, *Cryptographic support for Secure Logs on Untrusted Machines*, in Proceedings of the 7th USENIX

[5] V. Vishnamurty et al., *Karma: A secure economic framework for peer-to-peer resource sharing*, 2003

[6] N. Szabo, *Formalizing and securing relationships on public networks*, 1997

The Satoshi paper

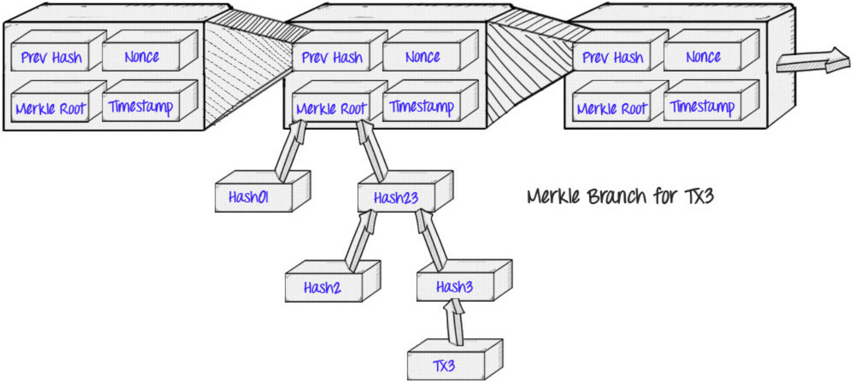
In 2008, Satoshi Nakamoto[7] made public the Bitcoin Paper.

- It aimed at defining a decentralized model avoiding a *central timestamping authority*, and a distributed *ledger* where transactions from/to addresses are stored
- He proposed a solution to achieve consensus in hostile environments by adopting the Proof-of-Work, initially from Dwork et al.[8] and from `hashcash.org`

[7] Conspiration theory: SAmsung, TOSHIba, NAKAmichi, MOTOrola ☺

[8] C. Dwork, and M. Naor, *Pricing via Processing or Combatting Junk Mail*, Crypto 92

The blockchain data structure is an ordered, back-linked list of blocks of transactions[9]



[9] A. Antonoupoulus, *Mastering Bitcoin*, O'Reilly

The problem of consensus

In the blockchain, since we transfer value, everyone is encouraged to cheat! ☺

Several consensus model

- Consensus in trusted environments
- Consensus in hostile environments (byzantine)

Clearly, if the consensus style changes, also the deployment of the blockchain changes.

- Permissioned (Hyperledger, Sawtooth, Coco framework)
- Public (Bitcoin, Ethereum, EOS, Rai)

The problem of consensus

Achieving consensus is complex.

The CAP theorem

It is impossible for a distributed system to simultaneously provide Consistency, Availability, and Partition Tolerance. A distributed system can satisfy any two of these, but not all three

The Proof-of-Work achieves consensus in hostile environments by solving the following equation

$$\mathcal{F}_d(c, x) \rightarrow SHA256(SHA256(c|x)) < \frac{2^{224}}{d}$$

where d is increasing constantly. Miners pool use specialized hardware (ASICs) to perform the PoW

The block

Block definition

A block is a data structure used to communicate incremental changes to the local state of a node. A block consists of a list of transactions, a reference to a previous block and a nonce. A block lists some transactions the block creator (the "miner") has accepted to its memory-pool since the previous block. A node finds and broadcasts a block when it finds a valid nonce for its PoW function. When a miner "closes" the block it has a reward (12,5 bitcoins now)

Blockchain

The longest path from the genesis block, i.e., the root of the tree, to a leaf is called the blockchain. The blockchain acts as a consistent transaction history on which all nodes eventually agree[a]

[a] R. Wattenhofer, *The Science of the Blockchain*

Wallets

Transactions are made on addresses. Each address is owned by a software, named *wallet*. A wallet

- Maintains a state of the addresses' balances (or pointers to balances)
- Manages and protect keys
- Generate addresses on demand (to avoid kidnapping)
- Hardware, Paper, Software, Online, Multisig
- Listens for events on the blockchain, avoiding to download the WHOLE blockchain (around 350 GB)

Wallets

- If a wallet is lost, or stolen, funds are lost *forever*.
- Should not use a online wallet (like Coinbase). They own your keys
- See the Mt. Gox, and Bitgrail (Francesco)

Wallets

What you can do with Bitcoin?

- a limited amount of coins available (21 millions)
- very inefficient (the blockchain of bitcoin processes 7 transactions per second)

Exchange

Exchange to FIAT or other currencies in Crypto Exchanges (Coinbase, Bitfinex)

Pay

You can pay services using the Simple Payment Verification, or the Lightning / Raiden network. Note that a transaction is verified if there are at least 6-14 confirmations.

After bitcoin: Ethereum

In 2013, Vitalik Buterin proposed Ethereum, a blockchain who is to solve some bitcoin's curses

- The ASICs: since mining new blocks comes with a reward, the PoW secures confidence that the blockchain will remain canonical, and ensures the wealth of the mechanism. However it should be open to as many people as possible, and it should not be possible to make a linear profit out of it, especially not with a high initial barrier
- The scripting. The "smart contract" (a contract in a electronic form) has been introduced in the 50s. Since the blockchain can be a distributed notary service, adding such functionality would be a benefit

Ethereum

Ethereum has a different execution model.

- It provides a quasi-Turing language in the EVM, Ethereum Virtual Machine
- Languages can be built on top of the EVM, such as Solidity, Serpent, and LLL
- In order to avoid to consume miner's resources, and to avoid DDoS, each execution of a EVM instruction costs *gas* `https://ethgasstation.info`.

Attacks to Ethereum

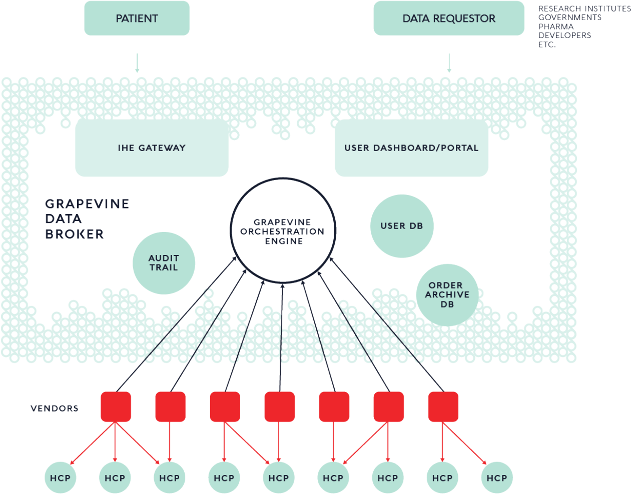
- The kitten
- The DAO
- Parity's suicide

But is blockchain a good programming paradigm?

We're at the beginning

- Solidity is a strongly typed programming language: avoids a zoology of mistakes
- Using Token Standards (ERC-20) helps a lot
- But still, a bug is forever!

For this reason (and for the cost of gas) many operations are made off-chain.



A erc-20 token

ERC-20 is a standard which defines how tokens can be created in Ethereum that comply with all the ERC-20 wallets.
Major functions:

- `transfer(to, value);`
- `uint initialSupply;`
- `contract Owner` paradigm.

Security vs Utility

If a token is known to have in advance an increase of price is a security (thus illegal in most of the countries), however if it is used to exchange value, it is a utility

How many tokens we create?

A token is either generated at every block (bitcoin, ethereum), or all in advance (Token Generating Event, TGE). TGEs are usually created in ICO, Initial Coin Offering.

- How to check if an ICO is a scam? Good question. Check the team, due diligence the cost plan
- How to set a price of a token?

$$S_t^{\$/B} = \frac{T_t^{B*}}{(M_t^B - Z_t^B)V_t^{B*}}$$

The exhange rate:

- Increases concurrently with the volume of transactions paid with tokens T_t^{B*}
- Decreases concurrently with the velocity of the tokens V_t^{B*} and the total quantity M_t^B
- Increases inversely with the quantity of tokens held in the speculative position Z_t^B, as this effectively reduces the quantity of virtual currency available

Input from Attendees / Discussion

Thank You