Blockchain and Beyond

Erwin Rooijakkers, Jeroen Bruijn, Ruud Hendrikx & Elisa Aachterberg

21-01-2017

Agenda

- Consensus
  - Distributed consensus
- Blockchain
  - What is the blockchain?
  - Hashing, public key cryptography, P2P-networking, consensus algorithms, Merkle trees
- Bitcoin
- Meditation session
- Ethereum
  - White paper
  - Smart contracts
- Blockchain applications
- Beyond

Consensus

Consensus

- How to confidently and securely transfer values (e.g. money or digital asset)?
- Use third-party ledger (e.g. your bank)???
- No, we want distributed consensus
- And a non-refutable, uncompromisable and unbreakable record of data

The blockchain

What is the blockchain?

”A shared, programmable, cryptographically secure and therefore trusted ledger which no single user controls and which can be inspected by everyone.” – Klaus Schwab (Chairman World Economic Forum)

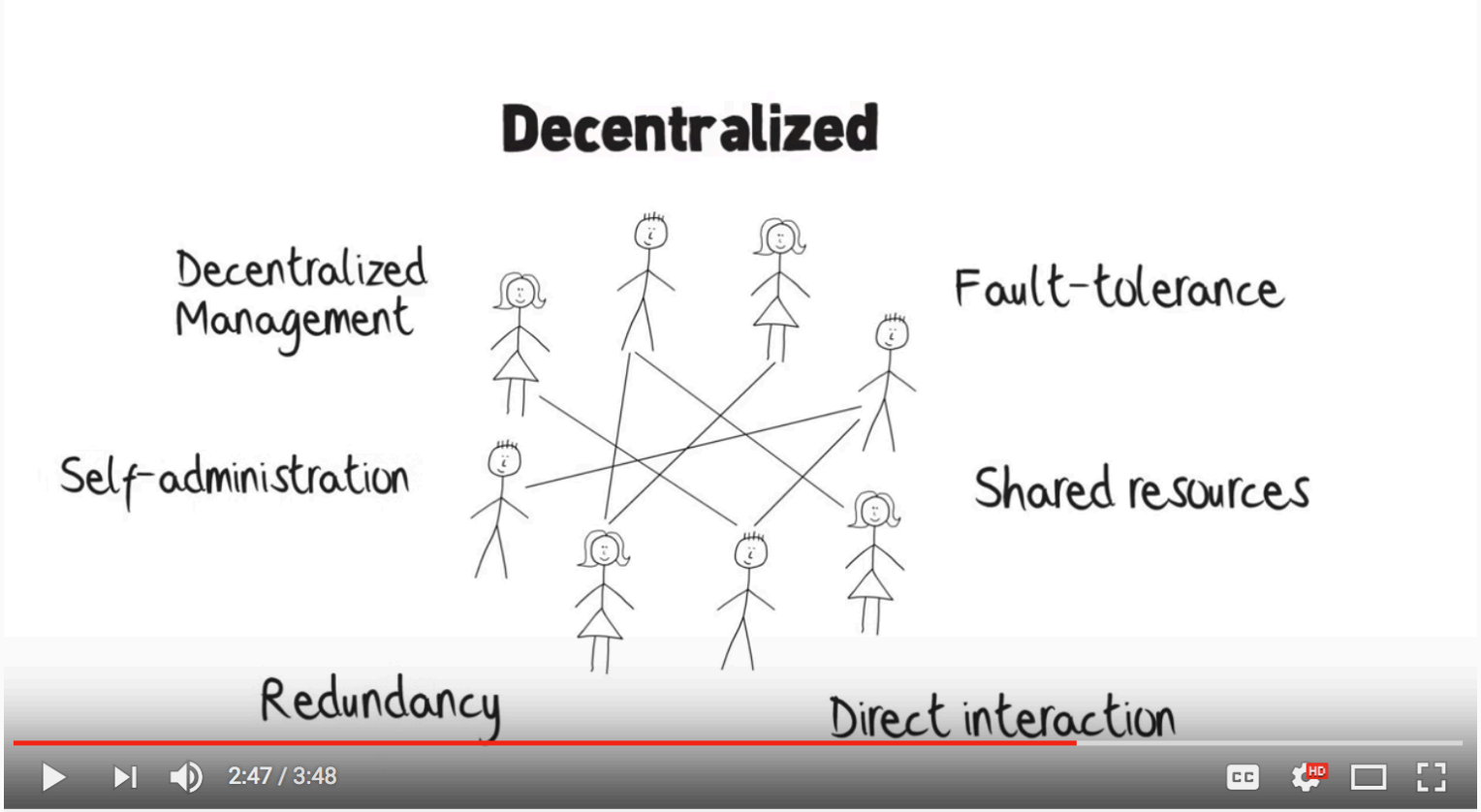
What is the second-generation blockchain?

”A programming language that allows users to write more sophisticated smart contracts [more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules, Ethereum White Paper], thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level.” (The Economist)

What is the blockchain?

- Two kinds of records:
  - Transactions
  - Blocks: batches of valid transactions that are hashed and encoded into a Merkle tree
- Each block includes the hash of the prior block in the blockchain, linking the two.
- Decentralized (eliminate risk of data held centrally)
- Every node or miner has whole copy
  - No centralized ”official” copy
- Data is incorruptible
- Quality by massive data replication and computational trust

P2P networking



What is P2P?

Public key cryptography

- A public key
  - (a long, randomly-generated string of numbers) is an address on the blockchain. Bitcoins sent across the network are recorded as belonging to that address.
- A private key is like a password that gives its owner access to their digital assets or otherwise interact with the various capabilities that blockchains now support.

Public Key Cryptography - Computerphile

`https://youtu.be/GSIDS_lvRv4`

- A public key
  - (a long, randomly-generated string of numbers) is an address on the blockchain. Bitcoins sent across the network are recorded as belonging to that address.
- A private key is like a password that gives its owner access

Hashing

- A hash function is any function that can be used to map data of arbitrary size to data of fixed size

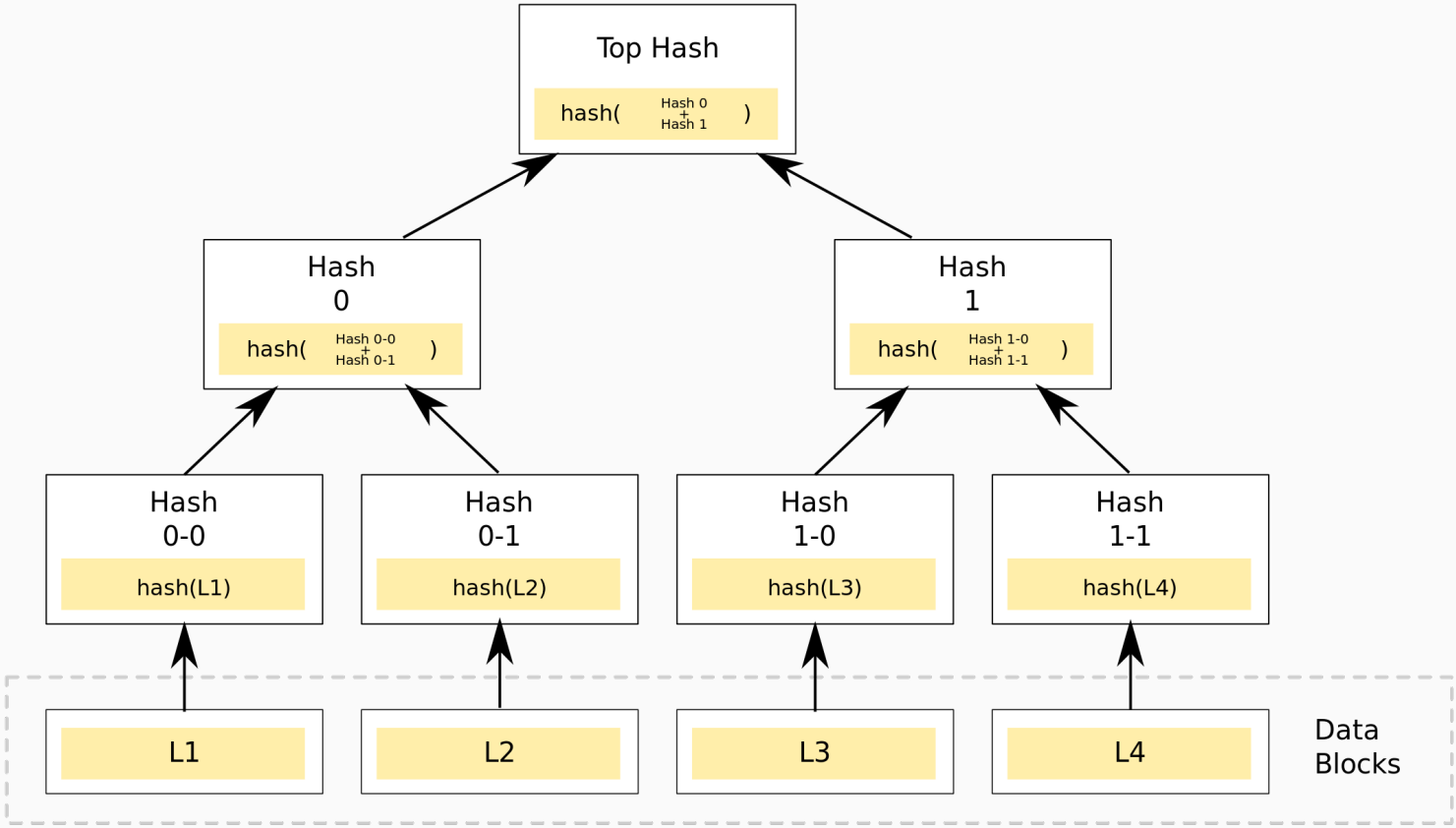
Consensus

- Proof of work: the current difficulty in bitcoin network requires miners to try quadrillions of times before finding a nonce that fits.
  - hashing can provide vastly different outputs on minor changes
- Proof of stake: mining is done by stakeholders in the ecosystem who have the strongest incentives to be good stewards of the system. (E.g., by having large amount of currency.)

Merkle tree

”Merkle trees are a fundamental part of what makes blockchains tick. Although it is definitely theoretically possible to make a blockchain without Merkle trees, simply by creating giant block headers that directly contain every transaction, doing so poses large scalability challenges that arguably puts the ability to trustlessly use blockchains out of the reach of all but the most powerful computers in the long term. Thanks to Merkle trees, it is possible to build Ethereum nodes that run on all computers and laptops large and small, smart phones, and even internet of things devices.” (Merkling in Ethereum)

Merkle tree (Wikipedia)



Quiz

- Demonstrating that a leaf node is a part of the given hash tree requires processing an amount of data proportional to the logarithm of the number of nodes of the tree.

Quiz

Why logarithmic?

Merkle proof

- Someone reading the proof can verify that the hashing, at least for that branch, is consistent going all the way up the tree, and therefore that the given chunk actually is at that position in the tree.
- If a malicious user attempts to swap in a fake transaction into the bottom of a Merkle tree, this change will cause a change in the node above, and then a change in the node above that, finally changing the root of the tree and therefore the hash of the block, causing the protocol to register it as a completely different block (almost certainly with an invalid proof of work).

Video - ChainThat

Merkle trees and hashing

https://youtu.be/lik9aaFIsl4

What is a Merkle proof? (Quora)

1 Answer

Weston Mizumoto, Stanford CS Theory

Written 27 Nov 2015

A Merkle tree is just an efficient way to prove that something is in a set, without having to store the set. Each non leaf node of a Merkle tree is just the hash of the concatenation of it's children. Each of the leaves are the set we want to prove membership for. In a sense, the root of the Merkle tree is a digest of all of the elements in the data set. Say person A contains the root node of the Merkle tree for set S, and person B wants to convince person A that element E is in S. To do this, person B only has to provide person A with the siblings of all of the elements in the tree in the path from E to the root node. This is only log(n) nodes. So B only has to provide only log(n) pieces of data, and person A only has to store the root node. With this provided information, person A can recompute the root node of the tree, and check to make sure that it matches the one that he knows is correct. If the hash function is collision resistant, then he can be sure that E is in S.

975 Views · View Upvotes

Quiz

What is a hash collision?

Bitcoin

What is Bitcoin?

- Managing ownership
  - through public key cryptography
  - with consensus algorithm for keeping track of who owns coins (known as "proof of work")

The first blockchain

- 2008
- The first blockchain
- Solved the double spending problem
- High fault-tolerance for Byzantine Generals' Problem
- Public ledger
- Uses Merkle proofs in order to store the transactions in every block
- Decentralized mechanism for emergent consensus
    - artifact of the asynchronous interaction of thousands of independent nodes, all following simple rules.

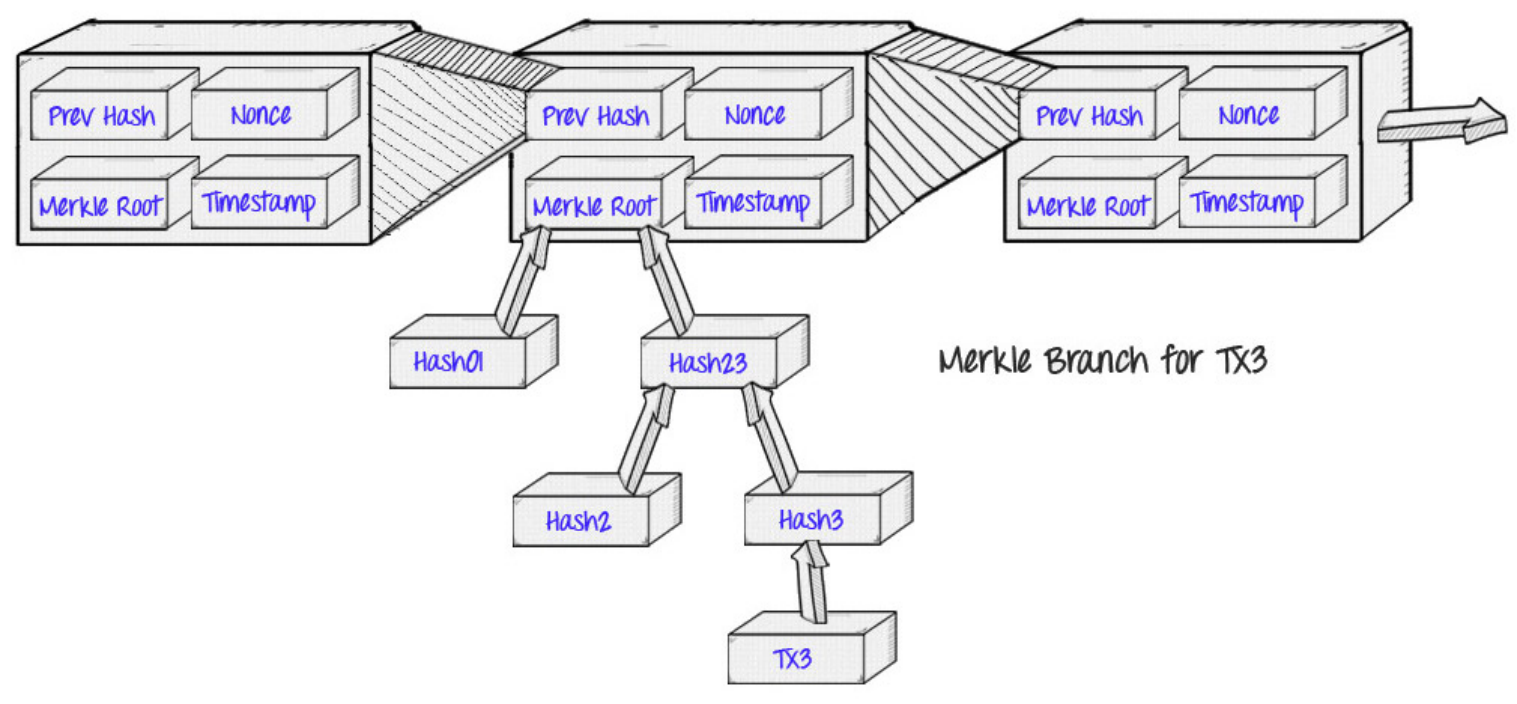
Video - Computerphile

Bitcoin - Computerphile

Bitcoin: `https://youtu.be/JyxRH18YlpA`

Problems: `https://youtu.be/s2XHyzPA9Zc`

The Bitcoin blockchain



(https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/)

The Bitcoin blockchain

- Full node
  - one that stores and processes the entirety of every block (more than one GB a month added)
- Light node
  - Simplified payment verification (SPV)
- Instead of downloading every transaction, light clients only download the the chain of block headers
  - 80 bytes
- Verification by Merkle proof

Problems with the Bitcoin blockchain

- Follow the money
- Consensus Attacks
- Blockchain forks
  - Two candidate blocks compete to form longest blockchain
  - As both miners discover a solution for their respective candidate blocks, they immediately broadcast their own ”winning” block to their immediate neighbors who begin propagating the block across the network.
- Light clients cannot prove anything about the currents state, like:
  - Digital asset holdings; Name registrations; The status of financial contracts; How many bitcoins do you have right now?
- You might need to authenticate the entire chain!
- Ethereum takes the concept one step further

Meditation session

Ethereum

Ethereum (1)

”The Ethereum protocol was originally conceived as an upgraded version of a cryptocurrency, providing advanced features such as on-blockchain escrow, withdrawal limits, financial contracts, gambling markets and the like via a highly generalized programming language. The Ethereum protocol would not ”support” any of the applications directly, but the existence of a Turing-complete programming language means that arbitrary contracts can theoretically be created for any transaction type or application.”

Ethereum (2)

”What is more interesting about Ethereum, however, is that the Ethereum protocol moves far beyond just currency. Protocols around decentralized file storage, decentralized computation and decentralized prediction markets, among dozens of other such concepts, have the potential to substantially increase the efficiency of the computational industry, and provide a massive boost to other peer-to-peer protocols by adding for the first time an economic layer. Finally, there is also a substantial array of applications that have nothing to do with money at all.” (Ethereum White Paper)

Videos - Ethereum

Ethereum the World Computer

`https://youtu.be/j23HnORQXvs`

Three Merkle threes per block header

- Transactions tree
- Receipts tree
- State tree
- Unlike transaction history, state can be updated
- Not a Merkle (binary) tree, but a Patricia tree
  - New root value needs to be calculated after insertion, update, or delete.
  - Bounded depth (against DDOS [denial of service] attacks)
  - 16 children per node
  - Root value only depends on data, not on order
  - path trough the tree towards particularly value is encoded

Facilitates things like

- Has this transaction been included in a particular block? (transaction tree)
- Tell me all instances of an event of type X (eg. a crowdfunding contract reaching its goal) emitted by this address in the past 30 days (receipt three)
- What is the current balance of my account? (state tree)
- Does this account exist? (state tree)
- Pretend to run this transaction on this contract. What would the output be? (state tree, special!)
    - Merkle state transition proof

Merkle state transition proof

- If you run transaction T on the state with root S, the result will be a state with root S, with log L and output *O*”
- “output” exists as a concept in Ethereum because every transaction is a function call.
- Enables the coding of smart contracts that will execute when specified conditions are met.
- Extensible programming instructions which both define and execute an agreement.
- Ethereum is an open source blockchain project that is built specifically to realize this possibility by implementing a Turing-complete programming language capability to implement such contracts

Serpent

- Token System

```
def send(to, value):
    if self.storage[msg.sender] >= value:
        self.storage[msg.sender] =
^^I         self.storage[msg.sender] - value
        self.storage[to] =
^^I         self.storage[to] + value
```

Serpent

- A basic smart contract for a name registration system (e.g., like DNS, used in mapping domain names to IP-addresses)

```
def register(name, value):
    if !self.storage[name]:
      self.storage[name] = value
```

- All it is is a database inside the Ethereum network that can be added to, but not modified or removed from
  - Immutability

Applications

The immense potential

"With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction. This is the immense potential of blockchain."
(Harvard Business Review, 2017)

Applications currently

- Cryptocurrencies
- Georgia: blockchain based *property-*registry
- Factom as a distributed registry
- Gems for decentralized messaging
- MaidSafe for decentralized applications
- Storj for a distributed cloud
- Tezos for decentralized voting
- Online voting
- Medical records
- Smart contracts (reduce moral hazards)
- Identity management
- `http://www.electricchain.org/`
- ...

Future

Vitalik Buterin explains Ethereum

`https://youtu.be/TDGq4aeevgY`

Sustainability

- Smart energy
- Virtual power plants (VPPs)
  - represent energy generating resources that are connected across a smart grid but that aren't necessarily concentrated in one central location, such as traditional power plants

Sustainability

”Distributed energy is really about generating your own energy, being self-reliant, selling excess energy to others.”

”Distributed energy is really about generating your own energy, being self-reliant, selling excess energy to others.” ”Blockchain is not only useful in moving money, it’s useful in moving any asset in a very transparent and reliable way,”

Problems with Ethereum

- Scalability
- Centralization risk (because of growth of blockchain only few organisations with full node)

Demo

Sources

- https://en.wikipedia.org/wiki/Blockchain_(database)
- https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/
- https://monax.io/explainers/permissioned_blockchains/
- https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-char
- https://github.com/ethereum/wiki/wiki/White-Paper

To watch

- http://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business
- https://www.youtube.com/channel/UC6rYoXJ_3BbPyWx_GQDDRRQ