Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 4

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is dead! Bitcoin Obituaries, *url*

Blockchain is immutable!

Bitcoin is the blockchain!

Blockchain is not Bitcoin!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is the blockchain!

Blockchain is immutable!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Confusing, isn't it? To get better understanding and to be able to decide which statement is true, follow this presentation series!

Outline of the whole series

Blockchain matters

- Little steps to the beginning
- The born of the technology
- Bitcoin, why is it so important?
- OK, so what is blockchain? And what is DLT?
- Consensus mechanisms
- Oracles
- Ethereum, the world computer
- Smart contracts
- Tokens and the digitization of physical objects, NFTs, SFTs
- The tsunami of cryptocurrencies
- ICO, IEO, STO, CeFi/DeFi, DID and other buzzwords
- The enterprise answer: consortium/private blockchain solutions
- When can/should I use blockchain? - The blockchain solution feasibility chart
- Possible use cases

Notation of references

References related to a slide are listed at the bottom of the slide, or right next to the text.

Visual Capitalist, G. Bhutada, “Purchasing Power of the U.S. Dollar Over Time”, 2021, url.

EOS, url

Solana, url

CertiK, “The Blockchain Trilemma: Decentralized, Scalable, and Secure?”, 2019, url

Blockchain matters

Part 4 – Ethereum

Ethereum

Blockchain matters

- Bitcoin's scripting language is hard to use and it has limited possibilities.
- Proposals of Vitalik Buterin were rejected.
- Buterin started Ethereum in 2015.
- Ethereum is a general purpose blockchain platform.
- If Bitcoin is the P2P money than Ethereum is the P2P everything.
- Native cryptocurrency is Ether (ETH), which equals to 10^{18} wei which equals to 10^{9} gwei.

C. Russo, "The Infinite Machine: How an Army of Crypto-hackers Is Building the Next Internet with Ethereum", 2020, url

Ethereum's properties

Blockchain matters

- Distributed, public, permissionless blockchain
- Transactions are public
- PoW consensus (Ethereum 2 is coming with PoS), block reward is currently 2 ETH.
- 2nd biggest chain in hash power (security, immutability) and in market capitalization (425 billion USD in Sept. 2021)
- Total supply is not finite!
- Transaction throughput: ~30 tx/s
- Number of necessary confirmations: ~50
- Average block time: ~50 s
- Average transaction fee: 5 USD (at 17th Sept. 2021)
- World state model instead of UTXO
- World computer, EVM – Ethereum Virtual Machine

Ethereum Doc, url

Average ETH tx fee, url

Ethereum accounts

Blockchain matters

- Addresses (which are derived from private and public keys) are called accounts
- Two types of accounts
  - Externally Owned Accounts (EOA): normal user wallet accounts used for sending and receiving ETH
  - Contract Accounts: storing smart contracts
- The state variables of an account are stored by the nodes (in decentralized way) in the world state trie.
  - Balance in case of EOA
  - Contract variables in case of Contract Account

Ethereum transactions

Blockchain matters

- Transactions are changing the state variable(s) of the accounts.
- Three types of transactions
  - Value transmission
  - Deploy smart contract (creates new contract account for the contract)
  - Interaction with smart contract

The Ethereum Virtual Machine (EVM)

Blockchain matters

- Decentralized virtual computer runs on full nodes.
- The nodes runs operations on EVM which are necessary to do the state changes initiated by transactions.
- Practically any program can be run on EVM.
- Also called as world computer.
- Programs run on EVM are called smart contracts.

Smart contracts

Blockchain matters

- The term was first used by Nick Szabo in 1994.
  - “A smart contract is a computerized transaction protocol that executes the terms of a contract”

N. Szabo, “Smart Contracts”, url

- Ethereum is the first blockchain platform which fully supports general purpose smart contracts.
- Smart contracts are simply computer programs whose binaries are stored on the blockchain and run by the miners (and other validating nodes). Their output are read from and their output is written in the decentralized database (hashes are stored on the blockchain).
- Usually smart contract is the business logic.

Properties of smart contracts

Blockchain matters

- Smart contracts are neither smart nor contracts :)
- The binary code and the program input/output is immutable.
- When certain conditions are met a smart contract runs automatically and inevitably.
- Advantages
  - The binary code is transparent
  - Adjustable transparency of state-space
  - Can be simulated and tested
  - Clear and consistent
  - Can be automated
  - Event driven
  - Immutable and final
  - Independent
- Disadvantages
  - Not for everything (e.g. date can't be a condition)
  - Not suitable for everything (a lawyer is essential in case of a high value real estate sale)
  - Only exact conditions (heartless)

T. Czeglédi, Blockchaineum, "Blockchain Gazdaság", 2019

Running smart contracts

Blockchain matters

- A smart contract can be executed by calling one of its functions.
- A function can be called by sending special transaction to the contract address with the function name and attributes.
- The function will be run by the miners and other validating nodes.
- The changed state-space (contract variables) will be updated and written to the blockchain (more precisely in the decentralized database) by the miners.

The cost of running smart contracts

Blockchain matters

- The smart contract are run by the Ethereum miners.
- In order to avoid infinite loops, the contract executor (transaction sender) must pay for executing the contract.
- Analogous to car petrol, the transaction sender must pay “gas” for contract execution.
- In Ethereum every operation type in the program has a predefined gas unit. (MLOAD = 3 gas, SSTORE = 5000 gas)
- The total gas cost of calling the contract is the sum of gas cost of each statement.

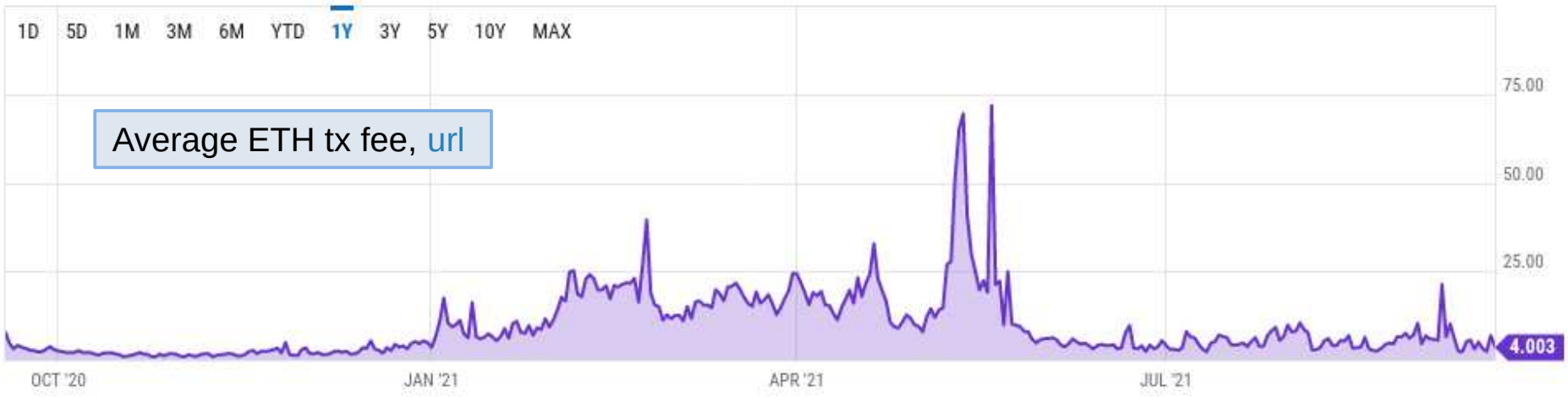
Ethereum transaction fee

Blockchain matters

- In order to detach tx fee from the current price of ETH, the transaction fee is paid in gas.
- Generally transactions are calling smart contracts.
- Tx fee depends on how complex program (how much operations) the EVM must run.
- Tx fee in gas equals to the sum of gas cost of all of the operations.
- When initiating a transaction the sender must tell
  - Gas limit: the total amount of gas he is willing to pay for the transaction
  - Gas price: the ETH price of a gas unit he is willing to pay.
- The tx fee in ETH ≤ gas limit * gas price.
- The maximum tx fee of the transaction is gas limit * gas price. If the gas limit is not enough for the given transaction than the tx will be reverted, i.e. finally there won't be any state changes. (The tx fee is paid to the miners even in this case.)
- The higher the gas price is the higher the probability is to be included in the next few blocks.

Ethereum transaction fee

- Simple ETH sending transaction costs 21000 gas. Currently (Sept. 2021) 254 gwei gas price is high enough for a fast transaction. This follows that in this case the transaction fee is 0.005334 ETH ~ 16 USD!
- Contract executions usually cost much more. Doing a token swap on the Uniswap platform can cost more than 100 USD!



Ethereum transaction fee

EIP-1559

- EIP: Ethereum Improvement Proposal
- EIP-1559 : at block 12.965.000, 5th of Aug. 2021.
- Transaction fee is divided
  - Base fee for txs. Base fee is burnt.
  - A tip can be added to prioritize the tx. The tip goes to the miners.
- Consequences
  - Cheaper transactions? (In Dec. 2021 this possible effect is not verified… :)
  - Decreasing minting -> deflation policy

EIP-1559: Fee market change for ETH 1.0 chain, url

Decentralized applications (dApps)

Blockchain matters

- Applications which are communicating with smart contracts (running on a decentralized network).
- The frontend of the dApp can be desktop or mobile application.
- WEB 3.0 enables running dApps.
- Examples
  - Augur (bet on outcomes of sports and other world events)
  - Compound (lending)
  - Uniswap (decentralized exchange)

Compound, url | Augur, url

The Ethereum block explorer - Etherscan

Blockchain matters

Etherscan, url

Transaction Hash:	0xf9e4d640a79857fcbb04f29061c7cf1e3d5aaafa985acb5157aab7447b05f7e8
Status:	Success
Block:	13271074 4 Block Confirmations
Timestamp:	1 min ago (Sep-21-2021 07:41:39 PM +UTC) | Confirmed within 30 secs
From:	0xbdca9094effd5c6dbe609ce65dc9f6b9a2ae516d
Interacted With (To):	Contract 0xe592427a0aece92de3edee1f18e0157c05861564 (Uniswap V3: Router) TRANSFER 0.532073586843700177 Ether From Wrapped Ether To Uniswap V3: Ro... TRANSFER 0.532073586843700177 Ether From Uniswap V3: Ro... To 0xbdca9094effd5c6dbe609ce65...
Transaction Action:	Swap 137,643.30585944356284 NII For 0.532073586843700177 Ether On Uniswap V3
Tokens Transferred: 2	From Uniswap V3: NII 2 To Uniswap V3: Ro... For 0.532073586843700177 ($1,540.45) Wrapped Ethe... (WETH) From 0xbdca9094effd5c... To Uniswap V3: NII 2 For 137,643.30585944356284 ($1,538.89) Nahmii (NII)
Value:	0 Ether ($0.00)
Transaction Fee:	0.028942464 Ether ($83.79)
Gas Price:	0.000000138 Ether (138 Gwei)

Ethereum wallets

Blockchain matters

- Web wallets
  - Myetherwallet (www.myetherwallet.com)
- Full node wallet
  - Go Ethereum
  - Parity
- SPV (Simplified Payment Verification) wallet
  - Electrum
  - Exodus
- Browser extension
  - Metamask
- Hardware wallets
  - Ledger
  - Trezor

Web3 and web3 service providers

Blockchain matters

- Web3 is the collection of functions (API) with which we can communicate with an Ethereum node.
  - Numerous implementations
    - Javascript - web3.js
    - Java - web3j
    - Python - web3.py
- Web3 service providers
  - Local service provider
    - Geth
    - Parity
  - Remote service providers
    - Infura
    - Alchemy

Tries

Blockchain matters

Tries are core data structures stored by every (full) nodes

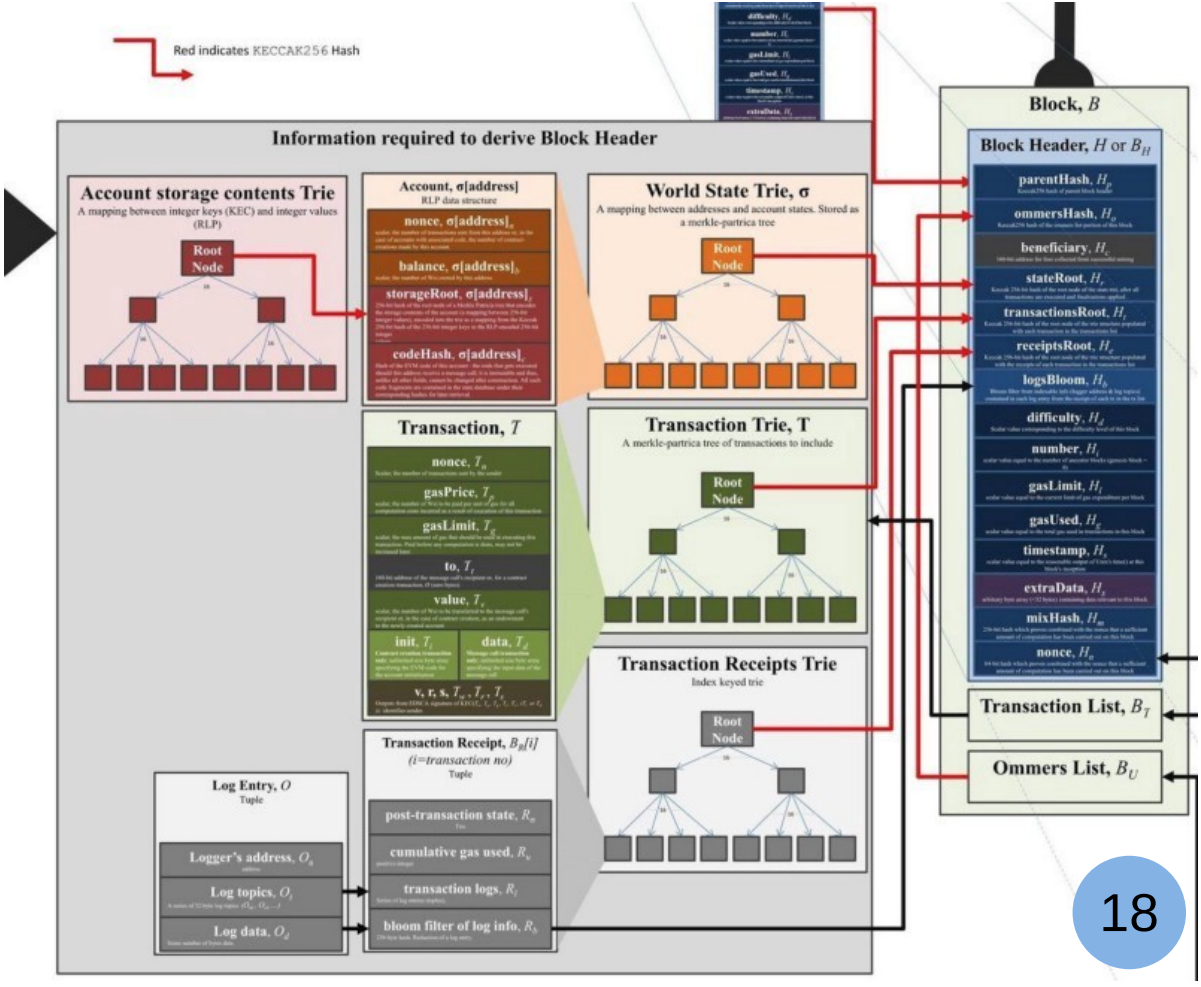
- World State Trie
- Transaction Trie
- Receipt Trie
- Account Storage Trie

Ethereum State Trie Architecture Explain, url

What is stored on the blockchain?

Blockchain matters

- Lots of us think
  - Transactions
  - Smart contracts
  - World state
- In reality
  - Transaction list
  - Hashes



Ethereum State Trie Architecture Explain, url

Tokens

Blockchain matters

- Tokens are traceable virtual units (digital assets) which have value, can have an ID, and their value is independent of the value of ETH (or other cryptocurrencies).
- Ethereum is the first blockchain platform which support tokens.
- Tokens can be defined, minted and transferred with smart contracts.
- Token standards
  - ERC-20 (Ethereum Request for Comments 20): general fungible tokens. Plenty of cryptocurrencies without native blockchains are defined as ERC-20 tokens (e.g. ChainLink)
  - ERC-721: non-fungible tokens. Collectibles (e.g. CryptoKitties)

F. Vogelsteller, V. Buterin, “EIP-20, Token Standard”, url

CryptoKitties, url

W. Entriken, D. Shirley, J. Evans, N. Sachs, „EIP 721: ERC-721 Token Standard”, url

S. Ellis, A. Juels, S. Nazarov, „ChainLink, A Decentralized Oracle Network”, url

Current usability of Ethereum network

Blockchain matters

- As more and more applications are built on Ethereum and more and more people are using them the network struggles with scalability issues.
- Really high fees.
- Practically unusable for everyday transactions.
- The original goal to be a World Computer hasn’t not been exceeded.
- Competitors are on the screen (BSC, Cardano, NEO, Tezos, etc.)
- EIP-1559 hasn’t substantially reduced the tx fees.
- ETH 2.0 will be good, but when? (PoS, scalability with sharding, etc.)
- On the other hand: 1st mover’s advantage. Nevertheless, Ethereum is THE smart contract platform: if Bitcoin is P2P money than Ethereum is P2P everything.

C. Russo, “The Infinite Machine: How an Army of Crypto-hackers Is Building the Next Internet with Ethereum”, 2020, url

Blockchain matters

Coming up next: Digital assets

Blockchain matters

Thank you!

If you liked this material you can tip me

Blockchain matters

- Bitcoin: *3FvgmYScorEje3WTrdDn5synEU6j917SZz*
- Litecoin: *ltc1qs457h3899qj4yry8k6u5xva79wa8f6xspant4e*
- Ethereum: *0xdF7eAab54BC9070a140D0251247406cEe40029B7*
- QTUM: *MGo31aQ74yHJ9Lan4tgYeFy5XhtHZuoimQ*
- Tezos: *tz1VpDWz45fvqv69Laa6YVa3h6MtkCoq1BDc*

Blockchain matters

Thank you again!