Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 7

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

Blockchain matters

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 7 – ICO, IEO, STO, CeFI, DeFI

ICO – Initial Token Offering

Blockchain matters

- Modern start-up financing method similar to IPO (Initial Public Offering) but with the benefit of tokenization.
- Instead of or besides venture capital.
- Before publishing the final product, the (blockchain) start-up mints and sells (security) tokens. Initial investors get discount and promise for some future rights and benefits.
- Some blockchain platforms support ICO out-of-the-box.
- Some successful ICOs:
  - Tezos, 2017: 232 million USD only during 9 minutes!! Tezos, „What is Tezos?”, url
  - TRON, 2017: 70 million USD Tron, „About Tron”, url
  - EOS, 2018: 4 billion USD Block.one, „eosio”, url

ICO – Initial Coin Offering

Blockchain matters

The dark side

- The “easy” money attracted scammers around 2017: buzzwords in the white paper, get the money and run (rug pull)! No regulation, no prosecution.
- Yetanotherico :) yetanotherico, „ICO generator for fun”, url
- ICO tsunami on Ethereum platform contributes to “bull run” in 2017 Q4.
- At that time it was enough to put the word “blockchain” in company’s name and the company’s stock price went sky-high. Long Island Iced Tea Corp. -> Long Blockchain Corp.

Reuters, “Factbox: Companies change names, businesses to ride the crypto wave”, 2017, url

IEO – Initial Exchange Offering

Blockchain matters

- The ICO scams resulted the born of IEO.
- The token sale is managed by an Exchange, which people already trust.
- The exchange filters the projects, only trustworthy and serious projects have chance to be listed on an reputable crypto exchange.
- The exchange means some guarantee.
- The most famous IEO was managed by Binance in 2019: the BTT tokens of BitTorrent project were sold out only in 15 minutes and raised 7 million USD.

BitTorrent IEO, 2019, url

STO – Security Token Offering

Blockchain matters

- Practically STO is an ICO offering security tokens.
- From another point of view STO is a tokenized IPO.
- From regulatory point of view security tokens are financial instruments.
- Regulatory requirements e.g. KYC or AML must be applied.
- ESMA (European Securities and Markets Authority) in EU: MiFID II (Markets in Financial Instruments Directive), AIMFD (Alternative Investment Fund Manager Directive), AMLD5
- SEC in USA: security tokens are under the same laws as traditional securities.
- The largest, and the first SEC registered STO was INX in April 2021, they raised 330 million USD.

Security token offering, Wikipedia, url

S. Voshmgir, “Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy”, 2019, url

INX Token Offering, url

ITO, IDO

Blockchain matters

- ITO (Initial Token Offering): very similar to ICO, often used as synonym, but “the focus of ITOs usually centers on offering tokens that have proven (or unproven) intrinsic utility”. The token holders will get exclusive services within an ecosystem (e.g. lower trading fees in case of an exchange).
- IDO (Initial DEX Offering): IEO on DEX.

Initial Token Offering (ITO), url

CeFI

Blockchain matters

- Centralized Finance, e.g. traditional banking services
- In blockchain context CeFI means centralized platform which is the part of the whole decentralized blockchain ecosystem.
- In case of a CeFI platform the clients must deposit their coins to the platform in which they must trust. “Not your keys not your coins”
- Benefits:
  - Users don’t need to guard private keys.
  - Usually cheaper than DeFI apps.
- Usual CeFI platforms
  - Custodial platforms, lending platforms (Inlock, BlockFi)
  - Centralized exchanges (Binance, Kraken)

Inlock: Unlock Your Crypto’s Potential, url

BlockFi, url

DeFI – Decentralized Finance

Blockchain matters

- Decentralized manifestation of traditional banking solutions.
- Automated financial infrastructure based on blockchain and controlled by algorithms, smart contracts and dApps.
- Clients can connect to a DeFI platform with their own cryptocurrency wallet, i.e. they have full control (and don’t lose control) over their coins.
- Due to transaction fees DeFI applications can be more expensive than CeFI apps, especially those which are built on Ethereum platform.
- DeFi applications are available on several platforms (Ethereum, BSC, Ontology, Tezos, etc.)
- Most popular DeFI applications are lending platforms (like Compound) and decentralized exchanges (DEX) like Uniswap.
- Complex financial services can be build by chaining smart contracts/dApps like LEGO parts.
- First DeFi applications published on Ethereum platform in 2019.
- The hype around DeFI started in the summer of 2020.

DeFI lending platforms

Blockchain matters

- Compound
- Aave
- Curve
- Yearn.finance
- Yearn.finance 2
- MakerDAO

Compound

Blockchain matters

- P2P lending platform on Ethereum network.
- Interest bearing tokens: cTokens (ERC-20 tokens)
  - Clients depositing crypto to Compound get appropriate cToken. (Depositing USDC client gets cUSDC tokens, etc.)
  - cTokens can be freely sent or traded.
  - Owner of cToken gets interest after each block.
  - cTokens can be used on other DeFI platforms (e.g. TokenSets automated trading platform).
- Borrowing crypto against deposited crypto as collateral (over-collaterized loan)
- Liquidity pools: the total amount of deposited crypto
- Flexible interest rate (deposit and loan) based on the balance of the liquidity pool.
- Governance tokens (COMP) provide voting rights on the Compound protocol (e.g. cUSDC interest calculating method)
  - COMP tokens are distributed to all lenders and borrowers (who already own cTokens). Distributions happen every time an Ethereum block is mined.
- Criticism: the platform is not decentralized, the funds of the clients can be withdrawn by the platform owners.

Compound, url

Yield farming

Blockchain matters

- Users supply liquidity to DeFi pools and getting interest bearing tokens (e.g. cUSDC)
- After their interest bearing tokens the users
  - are earning interest
  - and also earning governance tokens (COMP, YFI, YFII, etc.)
- Why is it good?
  - Ok, voting rights are good, but not enough.
  - But, the price of governance tokens can explode, especially after an exchange listing.
  - Moreover earned interest can be also remarkable.
  - “LEGO”: user can lend cUSDC to e.g. Curve platform. In this case Curve will get COMP tokens after cUSDC, but the user will get Curve’s CRV governance token which may have higher value.

Alexandria, “What Is Yield Farming?”, url

Variance,”Amikor a DeFi gazda betakarítja a Yieldet a Farmon!”, url

Yearn.Finance

Blockchain matters

- Automated asset balancing between different lending platforms in order to maximize interest. (Allows to leverage automated yield farming strategies across numerous lending pools.)
- Clients get interest-bearing tokens (yTokens) after depositing crypto to the platform. (After USDC, they get yUSDC)
- Governance token: YFI (ERC-20), users can earn it by contributing liquidity. Total supply is only 30.000 YFI.
- Sounds good? But what is the problem with this?
  - The re-balancing method is too simple...
  - Let us assume that yearn.Finance allocates 360k USDC to Aave.
  - Compound current interest rate is higer than that of Aave, so yearn.Finance moves all of the 360k USDC to Compound.
  - This causes that finally Aave interest rate will be higher than that of Compound :)



yearn

```
function rebalance() public {
    Lender newProvider = recommend();
    if (newProvider != provider) {
      _withdrawAll();
    }
    if (balance() > 0) {
      if (newProvider == Lender.DYDX) {
        _supplyDydx(balance());
      } else if (newProvider == Lender.FULCRUM) {
        _supplyFulcrum(balance());
      } else if (newProvider == Lender.COMPOUND) {
        _supplyCompound(balance());
      } else if (newProvider == Lender.AAVE) {
        _supplyAave(balance());
      }
    }
    provider = newProvider;
  }
```

yearn, url

Variance,”A DeFi kevésbé napos oldala”, url

Yearn.Finance

The devil is in the detail

- Is yearn.Finance decentralized?
- We have seen that the whole balance can be moved to e.g. Compound.
- But let see e.g. the yUSDC contract. The owner can change the Compound address to anything...

```
function set_new_COMPOUND(address _new_COMPOUND) public onlyOwner
{
    compound = _new_COMPOUND;
}
```

yearn, url

Variance,"A DeFi kevésbé napos oldala", url

yUSDC contract, url

Yearn.Finance 2

Blockchain matters



- Fork of yearn.Finance, also named as DFI.Money.
- Governance token: YFII (ERC-20)
- Mining new tokens: additional 30.000 YFII tokens will be mined with a similar method to Bitcoin's halving. Total supply is 60.000 YFII.
- Some other minor differences compared to yearn.Finance.
- Potential backdoors found in the protocol's code:
  - Owner could mint infinite number of tokens.
  - Metamask issued warning to its users.
  - Later owner keys were burnt, backdoors were closed.

DFI.Money, url

AAX Academy, "DeFi Decrypted: What Is DFI Money and YFII?", url

MakerDAO

Blockchain matters



- Similar to other lending platforms.
- For deposits the platform mints stable coin DAI.
- Auction
  - If the collateral value is lower than the loan (the value of the minted DAI), the collateral must be sold by the platform. This is the auction process.
  - Keepers can make bids. They buy collateral coins for DAI.

MakerDAO, url

Decentralized exchanges (DEX)

Blockchain matters

- What is DEX?
  - Contrary to centralized exchanges (e.g. Binance) DEX allows P2P transactions between users.
  - No KYC.
  - Each trade is written to the blockchain.
  - Due to transaction fees trading can be expensive especially in case of Ethereum network.
- Popular DEXes
  - Uniswap (Ethereum network)
  - Sushiswap (Ethereum network)
  - Pankakeswap (BSC network)
  - FEGEX (BSC, Ethereum network)

Uniswap Protocol, url

Blockchain matters

Coming up next: Enterprise blockchain

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!