Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 9

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

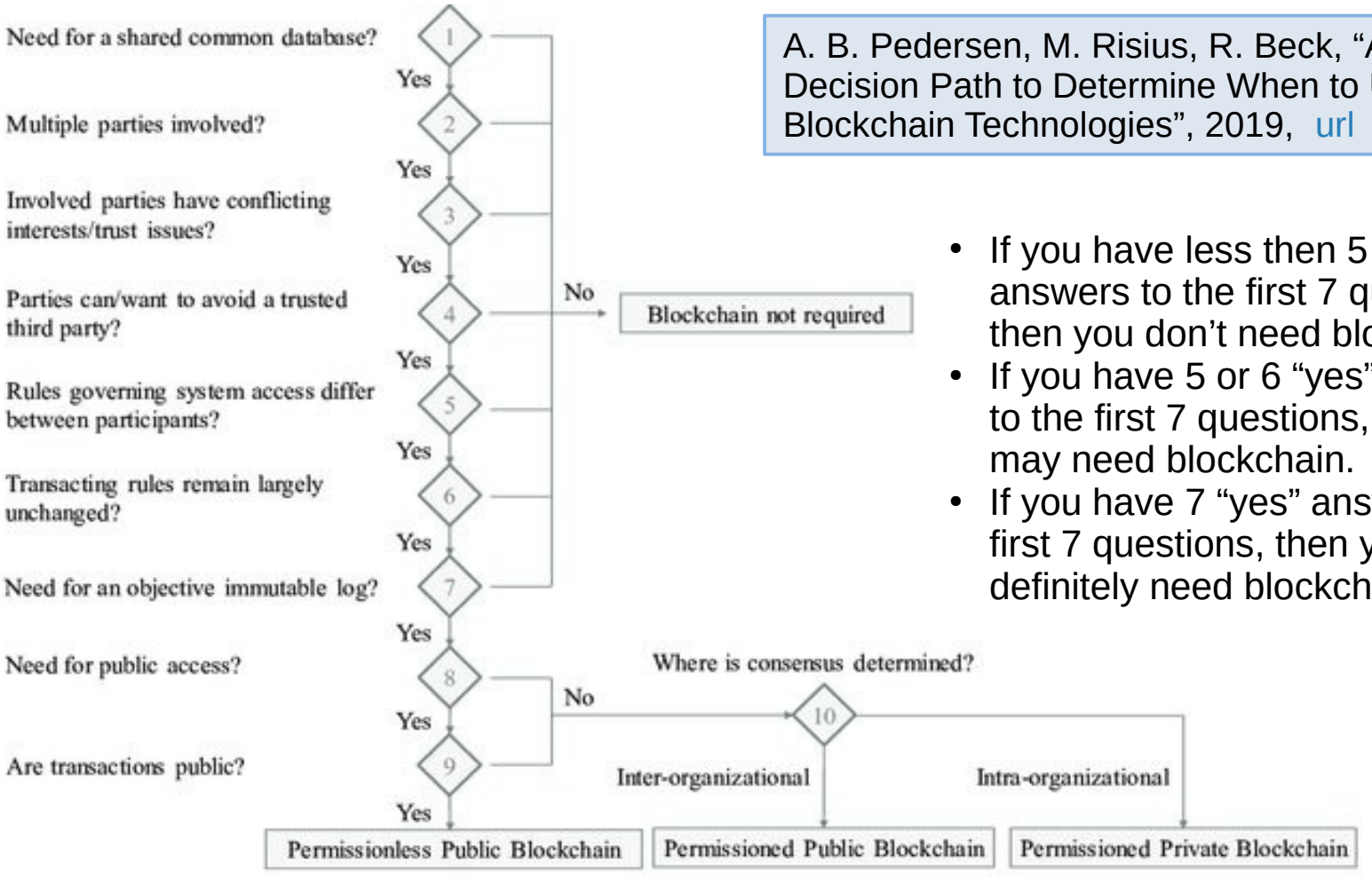
Part 9 – Use cases

So what is blockchain for?

Blockchain matters

- Blockchain is not the Holy Grail. Not every problem can be solved with using blockchain.
- Blockchain is neither secure nor immutable by default.
- If blockchain is not only considered as the date structure, but also the distributed ledger with clever distributed consensus, than blockchain is indeed one of the most disruptive technologies in the last 15 years.
- So, is blockchain a revolution? Will it be able to revolutionize our World? There is no evidence, but yes, it is a highly possible scenario.
- Blockchain can be world changing invention in the next few years.

The blockchain decision path



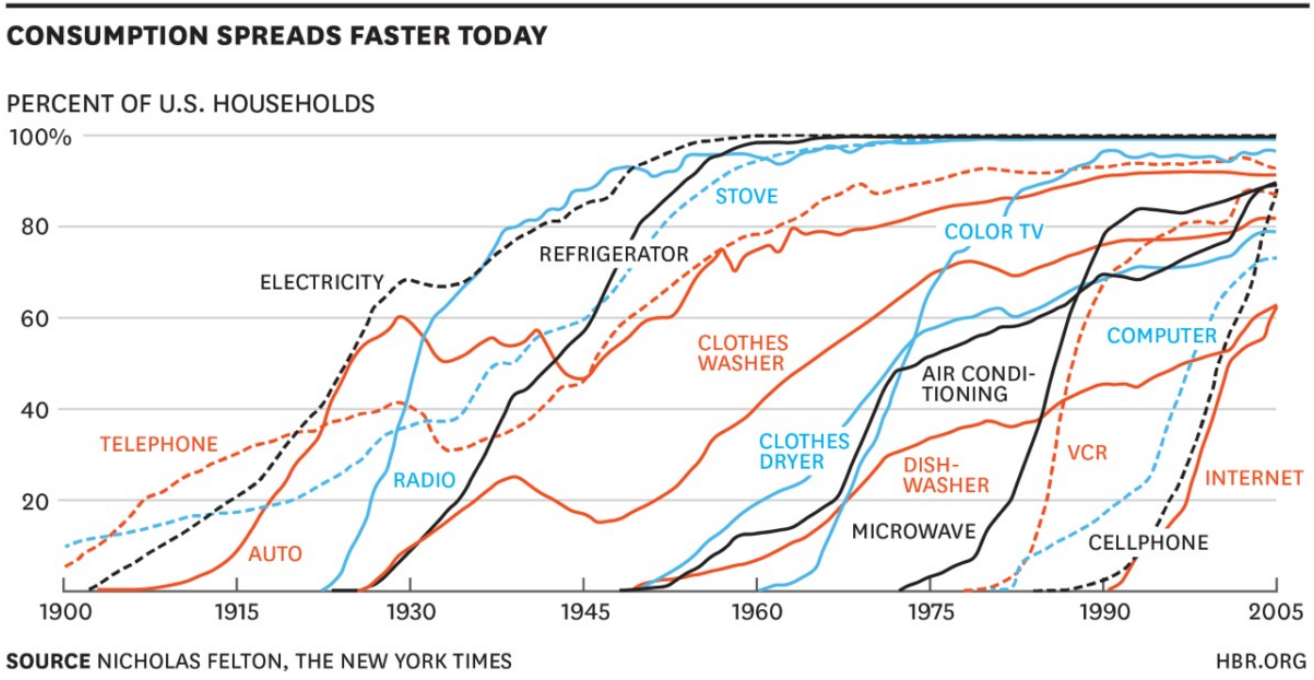
A. B. Pedersen, M. Risius, R. Beck, “A Ten-Step Decision Path to Determine When to Use Blockchain Technologies”, 2019, url

- If you have less then 5 “yes” answers to the first 7 questions, then you don’t need blockchain.
- If you have 5 or 6 “yes” answers to the first 7 questions, then you may need blockchain.
- If you have 7 “yes” answers to the first 7 questions, then you definitely need blockchain.

Widespread adoption?

Blockchain matters

- The pace of technology adoption is speeding up.
- Telephone needed >50 years.
- Color TV needed >25 years
- Internet needed >15 years
- How much time will blockchain need?



R. G. McGrath, “The Pace of Technology Adoption is Speeding Up“, 2019, url

Industrial revolutions

Blockchain matters

- According to Jeremy Rifkin, industrial revolutions comes, when there is sudden and simultaneous change in
  - Communication
  - Energy (raw material)
  - Mobility
- 1st industrial revolution: 18th century, steam based printing, telegraph, coal, steam engine
- 2nd industrial revolution: 19th century, telephone, oil, automobile
- 3rd industrial revolution: 20th century – nowadays, Internet, recycled “digitalized” green energy Internet, automated transportation, self-driving cars (Industry 4.0) (Hey, these are potential blockchain use cases!)
- Zero marginal cost society: people can self-produce green energy and exchange it P2P between each other without centralized energy companies and with practically zero marginal cost.

J. Rifkin, “The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism”, 2014, url.

The birth of centralized Internet

Blockchain matters

- The Internet was born to be decentralized
  - The early Internet connected campuses
  - In the beginning nobody wanted a centralized Internet
  - The vision was a decentralized Internet which can survive a world war of authoritarian shutdown.
  - Web 1.0 (1990-1995): “read” era: users could operate their own web pages with simple and static content, but basically average users only read the content which were created and uploaded by web page operators.
  - Lot of trials for decentralized data sharing
    - Napster, Kazaa
    - Torrent
- Tech giants (FAAMG – Facebook, Apple, Amazon, Microsoft, Google) brought us the centralized Internet
  - Tech giants are operating centralized services. These platforms are “free to use”, but users still pay for them with their data. There is no free lunch!
  - Web 2.0 (2005-2020): “read-write” era: social media, instant content sharing, average users could easily create, upload and share content on centralized platforms owned by tech giants.

K. Bickers, “Bitcoin Clarity: The Complete Beginners Guide to Understanding”, url

E. McFarland, “Blockchain Wars”, url

The (idealized) decentralized Internet

Blockchain matters

- Web 3.0: “read-write-possess” era.
- Decentralized platforms, transparent algorithms.
- The term “web3” was first used by the Ethereum developer Gavin Wood for the decentralized blockchain based online ecosystem in 2014.
- In web3 users can participate in the development and operation of online services.
- In web3 users own their own data.
- User accounts with DID, maximum control over own data
- Tokenization in business logic
  - Security tokens
  - No ads, utility token instead
- DAO (Decentralized Autonomous Organization)
- Examples
  - Map application cannot collect location data, because users controls what happens to their own data.
  - Application stores prioritizes dApps by rules made by users.
  - Cloud storage applications are accessible only by the user (with blockchain identity).

G. Edelman, “The Father of Web3 Wants You to Trust Less”, 2021, url

E. McFarland, “Blockchain Wars”, url

Involved industries and potential use cases

Blockchain matters

- Supply chain
- Insurance (Insuretech)
- Fintech
- Interbanking
- The Internet itself
- IoT
- Energy – Zero marginal cost society
- Prediction market platform / betting platform
- Identity management (DID)
- Real estate
- Government (Govtech - Healthcare, CBDC)

Supply chain - consortium

Blockchain matters

"...most of the data relating to ships' maintenance, logs, crews, machinery and monitoring is gathered and stored locally onboard the ships for insurance purposes. To make matters worse, most of this data is stored in paper documents."

A. B. Pedersen, M. Risius, R. Beck, "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies", 2019, url

- Benefits of using blockchain
  - Reduce paper intensive processes, simplify administration and paperwork
  - Reduce transaction costs
  - Improve transparency
  - Improve efficiency
- Companies/Projects: IBM/Maersk Trandelens, Hyundai Merchant Marine Co., IBM Food Trust, Marco Polo, Voltron Trade Finance Platform (Contour)
- Platform: Hyperledger Fabric, R3 Corda

Maersk, "The Tradelens Platform", url

Contour, "The Trusted Network for Global Trade", url

Insurance - public

- Benefit of using blockchain: the sum insured automatically paid to the insured person at the time when the risk materialized. (An oracle service must be used.)
- Companies/Projects: AXA Fizzy (flight delay insurance, abandoned), Aegon (ski resort insurance)
- What is the biggest problem with blockchain solutions? The sum insured must be available all the time at the insurance company.
- Platform: Ethereum

coindesk, „Axa is using ethereum’s blockchain for a new flight insurance product”, 2017, url

FintechZone, „Megérkezett az aegon biztosító blockchain alapú sípálya-biztosítása”, 2020, url

Fintech - public

- DeFI applications/platforms
  - Benefit: in ideal case the user of the DeFi platform don’t have to trust anybody, he don’t loose the control over his assets.
  - Companies/Projects:
    - Lending platforms: Compound, MakerDAO, Yearn.Finance
    - DEX: Uniswap, Pancakeswap
  - Platforms: Ethereum, BSC, Ontology, Tezos
- CeFI applications
  - Benefit: user don’t have to guard private keys, usually cheaper
  - Inlock, BlockFi

Compound, url | yearn, url | Uniswap Protocol, url

Inlock: Unlock Your Crypto’s Potential, url | BlockFi, url

Interbanking - consortium

Blockchain matters

- Benefits of using blockchain:
  - Speed up interbanking speed
  - Connecting financial, insurance and risk rating companies
  - Facilitate cross institutional business processes
- Platforms: Ripple, R3 Corda

D. Szegő, Nordic Blockchain Association, Solidity Services, “Consortium Blockchains á la Hyperledger”

IoT – public / consortium

Blockchain matters

- Massive IoT communication is the part of the Industry 4.0 vision.
- Benefits of using blockchain (Blockchain of Things)
  - Authorization of devices
  - Secure communication and data integrity, transparency
  - Autonomous IoT devices with smart contracts
  - Decentralized P2P architecture instead of Client-Server architecture
  - Monetizing data
- Projects: IOTA (zero fee txs), IoT Chain, Helium
- Platforms: IOTA, Ethereum, Helium, Hyperledger Fabric, Quorum

IoT Chain, url | Helium, url

Iota, url | “Blockchain of Things — cool things happen when IoT & Distributed Ledger Tech collide”, url

Energy - public

Blockchain matters

- Blockchain can be used in the current centralized energy distribution system: blockchain based smart energy meters, e.g. micro transactions after each kW/h energy.
  - Projects: LO3 Energy
  - Platforms: Exergy (Ethereum based permissioned platform)
- P2P energy trading: energy produced by households can be monetized, secondary market of renewable energy. (Zero marginal cost society – Rifkin)
  - Project: PowerLedger (energy exchange platform)
  - Platform: Ethereum

LO3 Energy, url

PowerLedger, url

J. Rifkin, “The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism”, 2014, url.

Prediction market platform - public

Blockchain matters

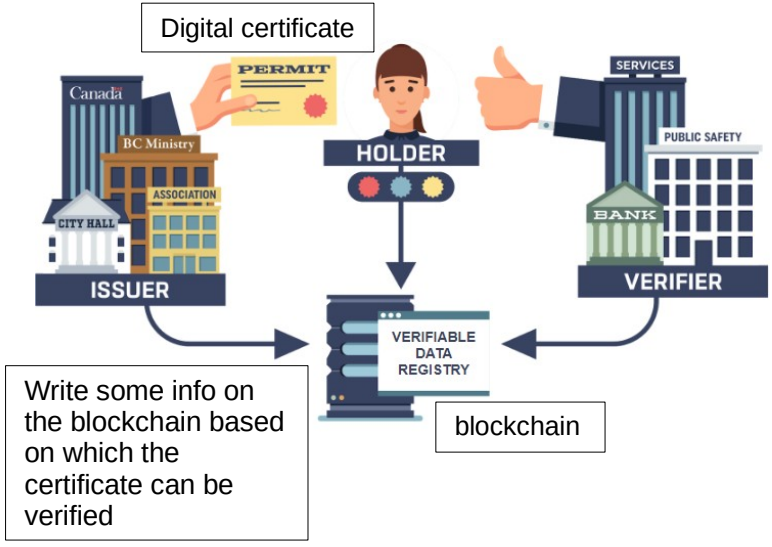
- Augur prediction market / betting platform
  - On Ethereum platform
  - With smart contracts
  - Own token: REP (ERC-20)
- Execution process
  - Market creation based on real world events. Anyone can create a market. Creator sets the initial reporter, the market end date and the creator fee. Creating a market costs REP.
  - Market trading. User buy shares in an outcome in DAI (buy – “bet for”, sell – “bet against”)
  - Market resolution
    - Initial reporter submits a tentative outcome
    - Dispute: those reporters whose report wasn’t part of the consensus lose their staked REP, which is then distributed to those who reported with the consensus.
  - Settlement: winning traders collect payouts
- Legal and ethical concerns.
- Under regulation in many countries.
- How dangerous can it be to bet that e.g. a real man will be alive on a specific date?

Augur, url | What is Augur? (REP), url | The Beginner’s Guide to Augur, url

Identity management

Blockchain matters

- Old school methods
  - user name + password
  - federated identity (via e.g. Google account)
  - paper based (scanned) credentials
- Blockchain based method: public + private key
- Self Sovereign Identity (SSI): anyone can generate pubkey/privkey pair for his own.
- Blockchain based Digital Identity Stack (Verifiable Credentials Model)
  - Different Credentials (e.g. diploma, driving license etc.) can be assigned to someone's SSI.
  - Actors
    - Issuer (issues (or withdraws) a Certificate which contains the issuer's and holder's public key, issuer signs the certificate with its private key)
    - Holder (can reveal info by signing with its private key)
    - Verifier (can verify info with issuer's and holder's pubic key)
- No private data is written to the blockchain.
- Selective Disclosure: only the relevant information must be revealed.
- Several solutions on several platforms
  - Public solution: Ontology
  - Consortium solution: Hyperledger Ursa/Indy/Iris



The Verifiable Credentials Model
By Peter Stokyo, peter.stokyo@elanica.com

Example

1. University "A" issues a diploma to Alice, so Alice holds a diploma issued by University "A".
2. Alice applies for a job at Employer "A".
3. The Employer "A" can verify that Alice holds a diploma issued by University "A" and can verify only this fact.

Why Distributed Ledger Technology (DLT) for Identity?, url

Identity Management

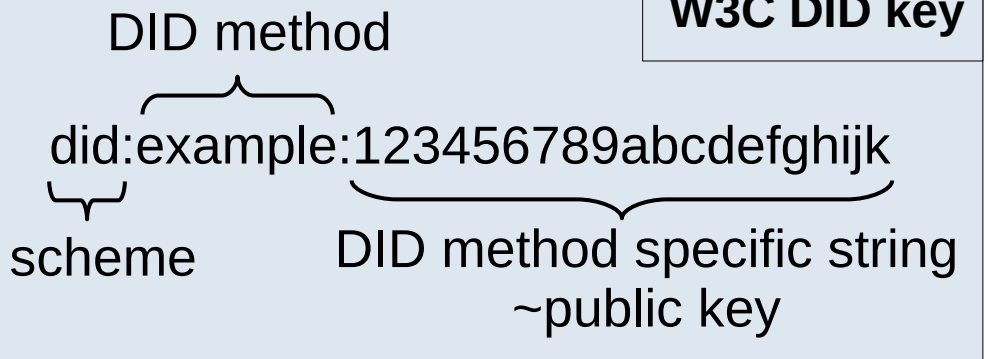
Blockchain matters

DID

- DID = Decentralized Identifier
- DID key is specified by W3C
- Digitalized documents can be attached to a DID key.
- One can have independent DIDs for each service (banking, government, work, social media, etc.)
- Changing DIDs: private communication between participants is possible (DIDcomm).
- Zero Knowledge Proof (ZKP) and Selective Disclosure
- Web of Trust (Trust over IP Stack)
  - Layer 1: DID networks (public ledgers)
  - Layer 2: DIDcomm
  - Layer 3: Credential Exchange (Verifiable Credentials Model)
  - Layer 4: Governance Frameworks

did:ont:TVuF6FH1PskzWJAFhWAFg17NSitMDEBNoa

W3C DID key



Decentralized Identifiers (DIDs) v1.0, url

Highlights of Internet Identity Workshop (IIW) #29, url

Real estate - public

Blockchain matters

- Tokenization of real estates
- Fractional ownership
- Deposit management related to real estate sale contract
- Projects: Digishares, SMARTdeposit
- Platform: Ethereum

Digishares, url

SMARTdeposit.io, url

Govtech - consortium

- Healthcare
- CBDC
- Land registration
- E-election
- Electoral campaign funding

Healthcare - consortium

- Currently independent proprietary systems, difficult to share data e.g. among hospital and insurer. The patient don’t have any control over his own data (medical record).
- Benefit of blockchain:
  - Shared database among different actors
  - Patient has full control over his medical records
    - Patient can control who can access which pieces of medical data (using DID). (The dentist doesn’t need to know e.g. the diopters of your glasses.)
    - Patient can monetize his own data, e.g. participate in a study done by a pharmaceutical firm.
- Project: MIT’s MedRec
- Platform: Hyperledger Fabric, Hyperledger Besu, Quorum

T. Serres, et al, “Basics of Blockchain”, url

What is MedRec?, url

CBDC - private / consortium

- CBDC = Central Bank Digital Currency
- Practically CBDC is a national currency on e.g. blockchain (electronic FIAT money), the issuer is the central bank of the country.
- Use cases of CBDC
  - Retail
  - Wholesale and international
- Benefits (from the government and society point of view):
  - Taxation
  - Traceability of every transactions
  - Marked coins, targeted aid
  - True alternative for cash
- Benefits (from the individual point of view):
  - Fast international money transfer
- Will it really solve everything (e.g. inflation)? No, but markets believes in CBDC so every news on introduction can have positive effect on the exchange rate of the country's currency CBDC is a very trendy word today :)
- However, CBDC can be another step towards government's full control over citizens.
- Experimental projects in many countries: China (e-CNY), Russia, Hungary, Ukraine (e-Hryvnia)
- Platform: Private / consortium blockchain

Hedera, "What is a central bank digital currency (CBDC)?", url

D. Szegő, "A globális Digitális Jegybankpénz kihívás", url

Blockchain matters

Coming up next: Conclusion

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!