Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 5

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 5 – Digital assets

Types of digital assets

Blockchain matters

- Cryptocurrencies
  - Coins and tokens
  - Basically coins are special tokens which are native cryptocurrencies of a blockchain
    - BTC, ETH, ADA, etc.
  - Tokens are not native cryptocurrencies, they are created with smart contracts.
    - ILK, ChainLink
    - Stable coins (USDC, USDT, PAXG, etc.)
    - NFTs
  - However, coins can be also considered as tokens.
- Central Bank Digital Currencies (CBDC)
  - China, Russia, Venezuela, Ukraine

Tokens

Blockchain matters

- Tokens are objects with value
- Everyday tokens
  - Casino token
  - Telephone token
  - Willy Wonka's Golden Ticket
- Blockchain aspect
  - Token is a traceable virtual unit which is storing data, can have an ID and can have value.
  - Bitcoin is the digitized money, tokens, in generally are digitized access right, investment share or arbitrary physical object (partial ownership).
  - Tokens are defined, minted and transferred with smart contracts.

T. Czeglédi, Blockchaineum, „BLOCKCHAIN Gazdaság II.", 2019

Token types

Blockchain matters

- From legal aspects (FCA) — FCA, „Guidance on Cryptoassets”, 2019, url
  - Utility tokens: access right to a platform or service (e.g. ONG, BAT)
  - Security tokens: provide investment share, interest, dividend or voting right (governance token) (e.g. Sia Funds)
  - Exchange tokens: means of exchange like money (e.g. BTC)

- BTC is exchange token from legal point of view, but functionally it is the incentive token of Bitcoin network.
- Gas is the utility token of Ethereum network.

- From fungibility point of view — skalex.io, „Making Sense of Crypto Token Types”, 2020, url
  - Fungible tokens (e.g. BTC, BAT)
  - Non-fungible tokens (NFT): with unique ID, collectibles
  - Semi-fungible tokens (SFT)

Token platforms

Blockchain matters

- First blockchain platform with support of general tokens was Ethereum.
- Currently various platforms support tokens.
- Token standards
  - Ethereum: ERC-20, ERC-721, ERC-1155, etc.
  - BSC: BEP-20, BEP-721, etc.
  - Ontology: OEP-4, OEP-5, etc.
  - Tezos: FA1.2, FA2
  - QTUM: QRC-20, QRC-721, QRC-1155, etc.

ERC-20

Blockchain matters

- ERC-20 (Ethereum Request for Comments 20): general fungible tokens on Ethereum platform.
- Required methods and events are specified by the standard: query token name, query symbol, query decimals, query balance of address, transfer token, etc.
- Variables
  - Name
  - Symbol
  - Decimals
  - Total supply
  - Balance per account
  - Etc.
- Popular ERC-20 tokens: Chainlink (LINK), Tether (USDT), Shiba Inu (SHIB), Augur (REP)

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

ERC-721

Blockchain matters

- ERC-721 (Ethereum Request for Comments 721): non-fungible tokens (NFT) on Ethereum platform.
- ERC-721 lets you create a contract with which you can mint a series of NFTs (similar NFTs with different IDs). (The series can consists of only one NFT).
- ERC-20 like methods: query token name, query symbol, query balance of address (number of NTFs owned by an address), etc.
- Ownership functions
  - ownerOf(tokenID) : returns the address of the owner of a token with a given ID
  - transferFrom(from, to, tokenID)
  - etc.
- Metadata:
  - name : only one name is possible for all of the tokens with different IDs
  - symbol : only one symbol is possible for all of the tokens with different IDs
  - baseURI : base URI (Uniform Resource Identifier)
  - tokenURI(tokenID) : returns the URI of a token with a given ID. The URI may point to a JSON file (which conforms to the ERC-721 Metadata JSON Schema) which contains information about the token

tokenURI = baseURI + tokenID

- Other variables
  - balances: balance per account
  - owners: owners of tokens with given IDs
  - etc.
- ERC721Enumerable extension: totalSupply, tokenByIndex, tokenOfOwnerByIndex methods

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

ERC-721

Blockchain matters

ERC721 Metadata JSON Schema

```
{
    "title": "Asset Metadata",
    "type": "object",
    "properties": {
        "name": {
            "type": "string",
            "description": "Identifies the asset to which this NFT represents"
        },
        "description": {
            "type": "string",
            "description": "Describes the asset to which this NFT represents"
        },
        "image": {
            "type": "string",
            "description": "A URI pointing to a resource with mime type image/* representing the asset to which this
NFT represents. Consider making any images at a width between 320 and 1080 pixels and aspect ratio
between 1.91:1 and 4:5 inclusive."
        }
    }
}
```

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

ERC-1155

Blockchain matters

- Improvement of ERC-721, developed by blockchain game developers Enjin, Horizon Games and The Sandbox in 2017.
- Multi Token Standard (fungible, non-fungible, semi-fungible) on Ethereum platform.
- Advantages over ERC-721
  - A single smart contract can handle both fungible and non-fungible tokens simultaneously and to tokens can be converted from one to the other (atomic swap). Moreover ERC-1155 supports infinite number of tokens in the contract.
  - Batched token transfer (send many items to multiple recipients). This reduces network congestion and tx fees.
  - More efficient metadata:
    - No symbol, or name stored in the smart contract: symbol is removed, name is moved to per token metadata JSON.
    - Multiple URIs (one per token), but only one URI must be stored in the contract.
  - Built-in transaction validation: built-in function that tests the validity of transactions before executing them, therefore no coin or asset will be lost if an incorrect address is inputted or there is a mistake elsewhere in the contract.

EIP-1155: Multi Token Standard, 2018, url

ERC1155 – Exploring the ERC-1155 Token Standard, 2021, url

D. Cheng, “Your Guide to ERC-1155: Comparing ERC-721 to ERC-1155”, 2021, url

ERC-1155

Blockchain matters

Example

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC1155/ERC1155.sol";

contract MultiToken  is ERC1155 {
    uint256 public constant MultiCoin = 0;
    uint256 public constant NFT_1 = 1;
    uint256 public constant NFT_2 = 2;

    constructor() ERC1155("https://multi-token-example/{id}.json") {
        _mint(msg.sender, MultiCoin, 100, "");
        _mint(msg.sender, NFT_1, 1, "");
        _mint(msg.sender, NFT_2, 1, "");
    }
    …
}
```

Token ID

Only one “skeleton” URI is stored

The URIs of the tokens are derived:
Token ID: 0, URI:
https://multi-token-example/0.json
...

Fungible tokens

Non-fungible tokens

ERC1155.sol, url

Tokenization

Blockchain matters

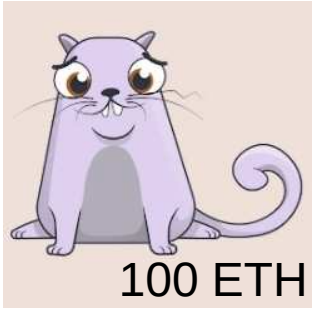
- Tokenize everything! S. Voshmgir, Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy", 2019, url
- Token(s) are assigned to any type of physical, digital objects or even e.g. intellectual property, work etc.
- Physical objects: real estates, fine art objects (e.g paintings), artworks, sport cards, photos, etc.
- Digital objects: digital artistic objects, digital photos, in game objects, etc.
- Future work of university student. V. Chaturvedi, „The Man Who Tokenized Himself Gives Holders Power Over His Life", 2020, url
- Tokenization creates a new token on the blockchain, so similarly to the physical object, one can send it to an other user without the token being multiplied.
- Evidence of ownership: the owner of the account in which the token is stored is the rightful owner of the physical or digital object.
- Fractional ownership: more token is assigned to a physical or digital object
  - Real estates (you can own one millionth part of a hotel and have a share from the revenue automatically)
  - Fine arts (what if you could buy one millionth part of Mona Lisa?)

NFTs (Non-fungible tokens)

Blockchain matters

- Practically tokenized digital or physical objects are NFTs (non-fungible tokens).
- Unique tokens (in contrast to e.g. Bitcoin, where one bitcoin is exchangeable for another bitcoin)
- First concept was elaborated around 2012 on Bitcoin network (Colored Coins)
- First real NFT platform was Ethereum (initially ERC-721 token standard, currently also ERC-1155)
- Currently several platforms support NFTs: Ethereum, BSC, Ontology, etc.
- Practically NFTs are tokenized digital or physical objects, which are sendable, tradable and stored in the owner's wallet.
- NFT examples
  - Digitally generated artistic object (CriptoKitties, CrytoPunks)
  - In game objects (computer games)
  - Sport cards
  - Photos
  - Paintings

Colored Coins, url



CryptoKitties, url



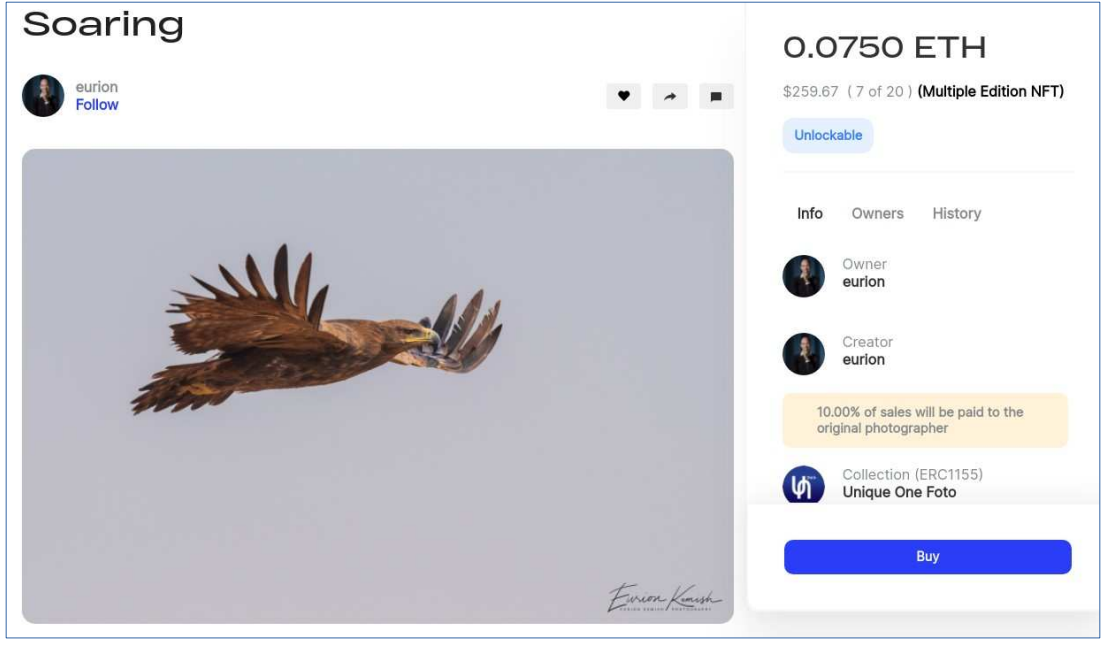
499.99 ETH

CryptoPunks, url

NFT marketplaces

Blockchain matters

- Opensea (digital paintings, digital art, collectibles, music)
- Rarible (digital paintings, digital art, collectibles)
- SuperRare (digital art, collectibles) – approved artists only
- Photocentra (photos)
- Unique One Photo (photos) – decentralized, ETH or BSC chain
- Crypto exchanges
  - Binance
  - Kraken



Unique One Photo, “Soaring”, url

Semi-fungible tokens (SFT)

Blockchain matters

- Merge properties of fungible and non-fungible tokens.
- A semi-fungible token is fungible until it is redeemed, it becomes a non-fungible token (lose face value) afterward.
- Analogy: entrance ticket to a concert
  - Let us consider that there is no difference between the tickets each of them entitles the owner to enter and listen to the concert. Before the concert these tickets are fungible, however, each ticket has different serial number.
  - After the concert the tickets become collectibles, which are differing from each other due to the serial number, so they become non-fungible. Tickets with lower serial number can have higher value for example.
- Semi-fungible tokens can be created with e.g. ERC-1155 token standard on Ethereum platform, or QRC-1155 on QTUM platform etc.
- Example: In game tokens. Since fungible and non-fungible tokens are defined in the same smart contract changing one to other doesn't need to call additional contracts. The players can trade fungible game-coins to an non-fungible axe (NFT), in other words his fungible tokens can be converted to an NFT and vice verse.

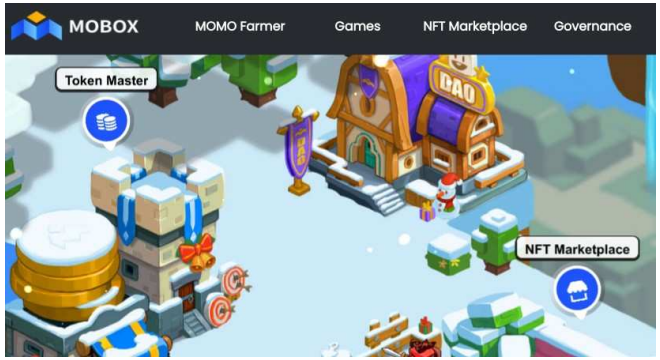
ERC1155 – Exploring the ERC-1155 Token Standard, 2021, url

Play to earn (P2E) games

Blockchain matters

- Blockchain games (GameFi = Game + Finance)
- Players can collect tokens during playing
  - Utility tokens are paid after given time of playing the game (some kind of incentive to play). Example: SLP (Smooth Love Potion) token in Axie Infinity.
  - NFTs
    - Collectible in-game items (objects (e.g. weapons), characters)
    - Generating new NFT characters (Axie Infinity)
- Generate some income for the player. (For some in developing countries P2E games may be their primary source of income)
  - The tokens earned by playing can be traded out of the game.
  - Staking. Examples:
    - 200-1000 USD can be earned per month with Axie Infinity by farming SLP tokens
    - Staking MBOX tokens in MOMOverse generates MOMO NFT Mystery Box.





Axie Infinity, url | MOMOverse, url

Regulations

Blockchain matters

United Kingdom

- Financial Conduct Authority (FCA) is the financial regulatory board in the United Kingdom.
- FCA permission is necessary for all the companies in the financial sector whose activity is regulated by RAO (Regulated Activities Order).
- FCA resolution about cryptocurrencies in January 2019.
- Regulation depends on the token type
  - Utility tokens: access right to a platform, service or product, i.e. practically money-like tokens. They have no security properties so FCA doesn't plan to regulate them. One exception: those utility tokens which can considered as electronic money, e.g. stable coins.
  - **Security tokens: provide investment share, interest, dividend or voting right (governance token). These tokens are classified as specified investments by RAO and transferable securities specified by MiFID II (Markets in Financial Instruments Directive), so regulations of standard securities apply to them.**
  - Exchange tokens: means of exchange like money, but no central/issuing authority. For example Bitcoin. Cannot be considered as money (because their value is volatile, not widely accepted and cannot be used as units of account) therefore no regulations.

FCA, „Guidance on Cryptoassets", 2019, url

Regulations

United States

- Securities and Exchange Commission (SEC)
- After DAO hack SEC issued a resolution in 2017: DAO tokens are declared to be investment contracts, and therefore securities.
- Public sales of securities are regulated by the SEC, therefore DAO would have had several obligations and SEC regulation would have applied to it.

D. Gardos, “SEC Issues Report – Declares DAO Tokens to be Securities”, url

Regulations

Hungary

- In Hungary only security tokens are under regulation, but only if the security tokens can be deemed as securities.
- Definition of securities under the Civil Code (Ptk.): securities are unilateral legal statements (i) issued in the form of paper-based documents or any other legal means (in practice: dematerialized securities); (ii) containing all mandatory material information listed in the Hungarian Capital Market Act; and (iii) the rights represented by the security can be exercised or disposed exclusively with the securities.
- Based on this definition, security tokens may be classified as securities if:
  - Their form is either physical or dematerialized; and
  - one may dispose of the right represented by them exclusively with the token.
- In this case the provisions of the act on the capital market regarding to public (or private) issuance with supervisory license will apply to the issuing of security tokens.

STO regulation and law in Hungary, 2019, url

Regulations

Blockchain matters

Lichtenstein

- Token and Trusted Technology Service Provider Act (TVTG) came into force in January 2020.
- One model to regulate all tokens, comprehensive regulation of the token economy.
- No token classification.
- Transaction systems based on trustworthy technologies (TT systems).
- Token is a piece of information in a TT system which
  - can represent claims or rights of memberships against person, rights to property, or other absolute or relative rights and
  - is assigned to one or more TT identifiers.
- Token functions: legitimization, liberation and transportation (transfer the underlying right).
- Token Container Model - the container can be filled with any claims and/or rights.
  - The regulation applying on a given token depends on the claims or rights that are attached to the token.
  - Two independent but collaborating elements
    - The container as described in the basic, technology-neutral, token definition
    - The specific content of the container, which changes depending on the features and qualities of the particular token.
  - If a security is represented in a token, security laws apply. If a financial instrument is represented in a token, financial market laws may apply, etc.
- Physical validators:
  - The responsibility of the physical validator is to ensure that the rights represented by the token are always valid.
  - To become a physical validator, private companies need to apply for a license at the FMA (Financial Market Authority). No licenses have been issued so far, but several applications are in preparation at the moment.
- Legal Certainty (TT, legal framework (enforceability), real-world asset)

One model to regulate all tokens, 2020, url

T. Nägele, “TVTG aka Blockchain Act / Token Act”, 2020, url

Regulations

MiCA

- 2020: Proposal of Markets in Crypto Assets directive was submitted: directive for crypto asset categories and corresponding risk classification. Practically MiFID II but for crypto. The goal is the same: to protect investors and ensure the transparent operation of the investment services (projects).
- 2021: European council adopted MiCA.
- Crypto asset types defined:
  - Asset-referenced tokens: type of stablecoin, asset-referenced tokens are backed by a basket of different fiat currencies, commodities or crypto assets (unlike USD-pegged stablecoins, such as USDC). Example: Libra.
  - E-money tokens: a stablecoin pegged to the value of a fiat currency like the USD. Example: USDC.
  - Utility tokens: issued with non-financial purposes to digitally provide access to an application, services or resources available on DLT networks. Example: BAT.
- MiCA clarifies what actions can investors take against a project that fails to deliver on its promises.
- Several exceptions based on the size of the project. E.g. whitepaper is required, but only if total consideration is more than 1M EUR.
- MiCA would not apply to CBDC nor security tokens.
- MiCA will probably not come into effect before the end of 2023.

MiCA: A Guide to the EU's Proposed Markets in Crypto-Assets Regulation, 2020, url

S. Handagama, "Europe's MiCA Crypto Rules Are Coming Soon. Here's Why They Matter", 2021, url

Blockchain matters

Coming up next: Other cryptocurrencies

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!