# Classification.

**Cryptocurrency** – name most widely used in mass media. That is currency supported by cryptographic methods.

**E-cash** – this name was often used in whitepapers published 10-30 years ago [[E-Cash Payment Protocols]](https://www.researchgate.net/publication/266279383_E-Cash_Payment_Protocols):

*“****E-cash is a payment system designed and implemented for making purchases over open networks such as the Internet.****”*

What is the proper name for such systems as Bitcoin? How to classify such systems using traditional financial terminology?

These are the characteristics of **currency**:

* 1. Medium of exchange;
  2. A Unit of account;
  3. Divisible;
  4. Durable;
  5. Fungible;
  6. Portable.

**Money** includes all mentioned characteristics plus “Storage of value”. Nowadays cryptocurrencies are considered more as speculative asset then storage of value. High correlation with Nasdaq shows that it’s difficult to consider cryptocurrencies as safe heaven/money/storage of value. At least today.

Some economists claim that cryptocurrencies can’t be used as currencies because of their rate volatility – it’s difficult to use currency that doesn’t support stable prices.

Proper classification using traditional financial terminology allows to predict further trends in cryptocurrency’s evolution based on the trajectory passed by traditional financial systems/notions.

* 1. **Medium of exchange**: some cryptocurrencies with low transaction fee are used as medium of exchange (for example: EOS, Tron, Matic…). But cryptocurrency hasn’t taken off the same way in every country, with its adoption and use being sporadic across the world[. These are the 10 countries](https://www.euronews.com/next/2022/08/16/ukraine-now-ranks-second-in-the-world-for-crypto-use-which-other-countries-have-embraced-i) with the highest number of businesses accepting payments in [crypto](https://www.euronews.com/next/2022/08/16/ukraine-now-ranks-second-in-the-world-for-crypto-use-which-other-countries-have-embraced-i): Colombia , Venezuela, South Korea, France, Greece, Thailand , Germany, Spain, Austria, The Netherlands.
  2. **A Unit of account**: cryptocurrency is measured in numbers, so it’s obvious a unit of account.
  3. **Divisible**: yes.
  4. **Durable**:

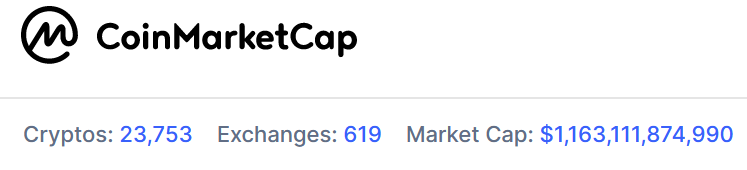
- The intensive circulation of the token can reduce its value in some blockchains significantly because of high transaction fee. So to be durable transaction fee should be low.

- Most of the tokens have a lifetime equal to lifetime of their network. The history of Bitcoin-like blockchains is short. One of the goals of this paper is to make lifetime of the token independent of lifetime of its origin network.

1.5 **Fungible**: the token in my pocket(wallet) is the same as token in other pocket. *Almost* the same: tokens in cold wallet are more secure then tokens in the exchange hot wallet. But traditional currencies have the same security issues: cash is more secure then amount on bank account from credit risk perspective and less secure in other aspects.

1.6 **Portable**. This is the main characteristics discussed in this paper. It depends. It’s easy to transfer an amount of some cryptocurrency between persons that are located in different places all over the world. But within the same blockchain. If two counterparties use different cryptocurrencies/blockchains then sender should convert token issued in his blockchain into token circulated in receiver’s blockchain. Often using exchanges. And this often requires some efforts: sender may have to transfer amount from cold storage into hot wallet of exchange (paying transaction fee). Then sender pays commission for conversion one token to another. And he pays commission for withdrawal when sending from exchange wallet to wallet of receiver. The steps may be different but often transferring is not a trivial task and often it has significant overheads. Evolution of traditional currencies shows the tendency of simplification of transfers between different geographical regions. But legislations of different countries introduce berries. So difficulties in transferring are comparable between traditional and cryptocurrencies. Nowadays it’s harder for legislation of different countries to control free movement of cryptocurrency. This property is often related with so called censorship-resistance.

In the second decade of 21-st century we have following picture: hundreds of tokens are listed in exchanges (more than 23 thousands as per CoinMarketCap).



Most often there is one to one relationship between token and blockchain/network. Usually P2P network supports one blockchain – distributed ledger/database. Most blockchains has their “native” currency/tokens: say, Ethereum network has its native token *Ether* for paying transaction fee - gas. Some blockchains support their native token plus wrapped tokens issued by other blockchains. For example [article from [CoinMarketCap](file:///D:\Books\Blockchain\Blockchains_Integration\WrappedTokens\What%20Is%20Wrapped%20Ethereum%20(WETH)_%20_%20CoinMarketCap%20(4_22_2023%208_17_14%20PM).html)]:

“[WETH](https://coinmarketcap.com/currencies/weth/) is the wrapped version of [Ether](https://coinmarketcap.com/currencies/ethereum/). Wrapped tokens, like WETH or [Wrapped Bitcoin](https://coinmarketcap.com/currencies/wrapped-bitcoin/), are tokenized versions of cryptocurrencies that are [pegged](https://coinmarketcap.com/alexandria/glossary/peg) to the value of the original coin and can be unwrapped at any point. Almost every major blockchain has a wrapped version of its native cryptocurrency like [Wrapped BNB](https://coinmarketcap.com/currencies/wbnb/), [Wrapped AVAX](https://coinmarketcap.com/currencies/wavax/), or [Wrapped Fantom](https://coinmarketcap.com/currencies/wrapped-fantom/). The mechanism of such coins is similar to that of [stablecoins](https://coinmarketcap.com/alexandria/glossary/stablecoin). **Stablecoins are essentially “wrapped USD” in the sense that dollar-pegged stablecoins can be redeemed for**[**FIAT**](https://coinmarketcap.com/alexandria/glossary/fiat)**dollars at any point.** In a similar fashion, WBTC, WETH, and all other wrapped coins can be redeemed for the original asset at any time.

Wrapped coins solve a particular problem: because of the low interoperability of blockchains, native coins of one chain cannot be used on another chain. For instance, you cannot use Bitcoin on the Ethereum blockchain and you cannot use Ether on Bitcoin or [Avalanche](https://coinmarketcap.com/alexandria/article/a-dive-into-avalanche). Wrapping coins solves this problem by tokenizing them and applying the blockchain’s token standard to the tokenized version of the original cryptocurrency.

On Ethereum, **almost all fungible tokens follow the**[**ERC-20**](https://coinmarketcap.com/alexandria/glossary/erc-20)**standard developed in 2015**. This token standard was developed to have a standardized set of rules for tokens on Ethereum, which simplified new token launches and made all tokens on the blockchain comparable to each other. Mandatory rules all ERC-20 tokens have to follow are totalSupply, balanceOf, transfer, transferFrom, approve, and allowance. Unfortunately, **Ether itself does not comply with the ERC-20 standard. Wrapped Ethereum was developed to increase**[**interoperability**](https://coinmarketcap.com/alexandria/glossary/interoperability)**between blockchains and make Ether usable in decentralized applications ([dApps](https://coinmarketcap.com/alexandria/glossary/decentralized-applications-dapps" \t "_blank)).”**

Thus, “low interoperability of blockchains” reduces portability of tokens.

Attempts to create digital cash were made 3 decades before appearance of Bitcoin[BackSidechains]:

“David Chaum introduced digital cash as a research topic in 1983, in a setting with a central server

that is trusted to prevent double-spending[Cha83]. To mitigate the privacy risk to individuals from

this central trusted party, and to enforce fungibility, Chaum introduced the blind signature, which he

used to provide a cryptographic means to prevent linking of the central server’s signatures (which

represent coins), while still allowing the central server to perform double-spend prevention. The

requirement for a central server became the Achilles’ heel of digital cash[Gri99]. While it is

possible to distribute this single point of failure by replacing the central server’s signature with

a threshold signature of several signers, it is important for auditability that the signers be distinct

and identifiable. This still leaves the system vulnerable to failure, since each signer can fail, or be

made to fail, one by one.

In January of 2009, Satoshi Nakamoto released the first widely used implementation of peer-to-

peer trustless electronic cash[Nak09], replacing the central server’s signature with a consensus

mechanism based on proof of work[Bac02], with economic incentives to act cooperatively.”

So, Bitcoin eliminated single point of failure replacing it with a decentralized consensus. Decentralization made Bitcoin a robust system with absence of trust to centralized 3-rd party. And mechanism used for existence of such wrapped tokens as WETH is based on trust to 3-rd party [CMCWETH]:

“Wrapped tokens require [custodians](https://coinmarketcap.com/alexandria/glossary/custodian) to hold the collateral.For instance, if you want to wrap Ethereum, a custodian will hold your Ether and give you Wrapped Ethereum in return. Custodians can be **merchants,**[**multi-signature**](https://coinmarketcap.com/alexandria/glossary/multisignature)**wallets, or simply a**[**smart contract**](https://coinmarketcap.com/alexandria/glossary/smart-contract)**.”**

Approach with Custodians works but introduces single point of failure – further decentralization is desirable for interoperability of blockchains. The goal of this paper is to find out the way to increase interoperability of blockchains/portability of cryptocurrency using decentralized mechanisms.

Thus, we can see that cryptocurrencies mostly support characteristics of traditional fiat currencies. And trends of fiat currencies may influence trends of cryptocurrencies – cryptocurrencies may face the same requirements. Fiat currencies are issued by national Central Banks and interoperability between them (and also between commercial banks) is essential for international trade and financial system. Interoperability of blockchains is actual direction of cryptocurrency evolution. We can see that some steps were made to introduce interoperability (using custodians) but further elimination of central trust is required to comply with decentralized nature of cryptocurrency. According to weakest link principle of IT Security: Security is Only as Strong as the Weakest Link.

# Similarity with other systems

Many blockchains appeared as fork of Bitcoin codebase. Some blockchains added new outstanding properties to Bitcoin. For example, Monero added anonymity. Ethereum may be considered very differently that just platform for particular token – Ethereum pretend to be distributed world computer. Some projects appeared because it’s difficult to introduce changes in Bitcoin. And they try to improve Bitcoin. But most of projects didn’t introduce something new. Creating a new cryptocurrency sometimes is similar to currency emission. Currency is not created only by emission of Central Bank – 10% reservation gives opportunity for bank to issue new amount of currency giving a credit. In exUSSR countries in 90-s hundreds of banks were founded. It was profitable to create banks. But financial system doesn’t require such amount of banks. Most of them were merged or ended its life. Most robust survived. Some cryptocurrency analytics predict the same reduction of blockchains. Can some particular blockchain merge other blockchains covering all the market? It seems no. Because unlikely one particular blockchain is capable to support all required characteristics. “Ratio of Ether’s market cap doubled Bitcoin in the last [year](https://cointelegraph.com/news/ratio-of-ether-s-market-cap-doubled-bitcoin-in-the-last-year-pantera-capital)”. But Bitcoin’s difficulty of introducing changes is itself useful property. Ethereum is more centralized is the sense that its founders can introduce changes on their discretion easily. Ethereum position itself as “moving fast” but this reduces its censorship resistance. Cryptocurrencies like Monero are not listed in some exchanges because their anonymity doesn’t comply with legislation restrictions of some countries. And therefore some projects support anonymity but allow to reveal private information. So, there is no universal thing and diversity of projects will exist. Reduction of similar projects are expected.

# References

|  |  |
| --- | --- |
| [BackSidechains] | Adam Back, Matt Corallo, Luke Dashjr,  Mark Friedenbach, Gregory Maxwell,  Andrew Miller, Andrew Poelstra,  Jorge Timón, and Pieter Wuille,  *Enabling Blockchain Innovations with Pegged Sidechains,* 2014,  [*https://blockstream.com/sidechains.pdf*](https://blockstream.com/sidechains.pdf) |
| [Bac02] | A. Back, *Hashcash — a denial of service counter-measure*, 2002, http://hashcash.org/papers/hashcash.pdf. |
| [Cha83] | D. Chaum, *Blind signatures for untraceable payments, Advances in Cryptology*  Proceedings of Crypto 82 (1983), no. 3, 199–203. |
| [CMCWETH] | CoinMarketCap, *What Is Wrapped Ethereum (WETH)?* ,  https://coinmarketcap.com/alexandria/article/what-is-wrapped-ethereum-weth |
| [Gri99] | Ian Grigg, Email correspondence, 1999, http://cryptome.org/jya/digicrash.htm. |
| [Nak09] | S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, https://www.  bitcoin.org/bitcoin.pdf. |