Digital Currencies and Cryptoassets

Ladislav Krištoufek

Charles University Prague

Diskusní fórum ČNB 2024
23 April 2024

Introduction

- We'll sprint through the historical context of Bitcoin emergence, its evolution, the role of Ethereum, towards stablecoins and CBDCs, laying the playground for the panel discussion.

Historical Context of Bitcoin (BTC) Emergence

- Bitcoin emerged in 2008, following the aftermath of the Global Financial Crisis. The crisis highlighted flaws in the traditional financial system, including centralized control, opacity, and susceptibility to manipulation.
- Satoshi Nakamoto's whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System", published in the same year, proposed Bitcoin as a decentralized alternative to traditional currencies, aiming to address the shortcomings exposed by the crisis.
- Key features of Bitcoin include its decentralized nature, built on blockchain technology, which allows for peer-to-peer transactions without the need for intermediaries.
- Significant milestones include the first Bitcoin transaction in 2009, the establishment of the first Bitcoin exchange in 2010, the Bitcoin Pizza Day in 2010 (first documented purchase of goods with Bitcoin), the rise of other cryptocurrencies (altcoins) such as Litecoin and Namecoin, the Mt. Gox exchange hack in 2014, and the increasing institutional interest in Bitcoin as a possible hedge against inflation and economic uncertainty.
- Even though the last two bull runs in Bitcoin are mostly remembered for non-Bitcoin phenomena, the current market mostly hovers around the spot ETFs (exchange-traded funds).

What Makes Bitcoin Possible (and Attractive) Money?

- **Decentralization**: Bitcoin operates on a decentralized network of computers, ensuring no single entity controls the currency.
- **Limited Supply**: With only 21 million bitcoins, Bitcoin is designed to be scarce, preventing inflation.
- **Divisibility**: Bitcoin is divisible into smaller units, allowing for microtransactions and flexibility in usage.
- **Portability**: Easily transferable across borders and jurisdictions using digital wallets and the internet.
- **Security**: Transactions are secured through cryptographic algorithms and verified by network nodes.
- **Anonymity and Privacy**: Transactions are pseudonymous, offering a level of privacy.
- **Immutable Ledger**: Once confirmed and added to the blockchain, transactions cannot be altered or reversed.
- **Global Acceptance**: Increasing acceptance by merchants and businesses worldwide contributes to its usability.

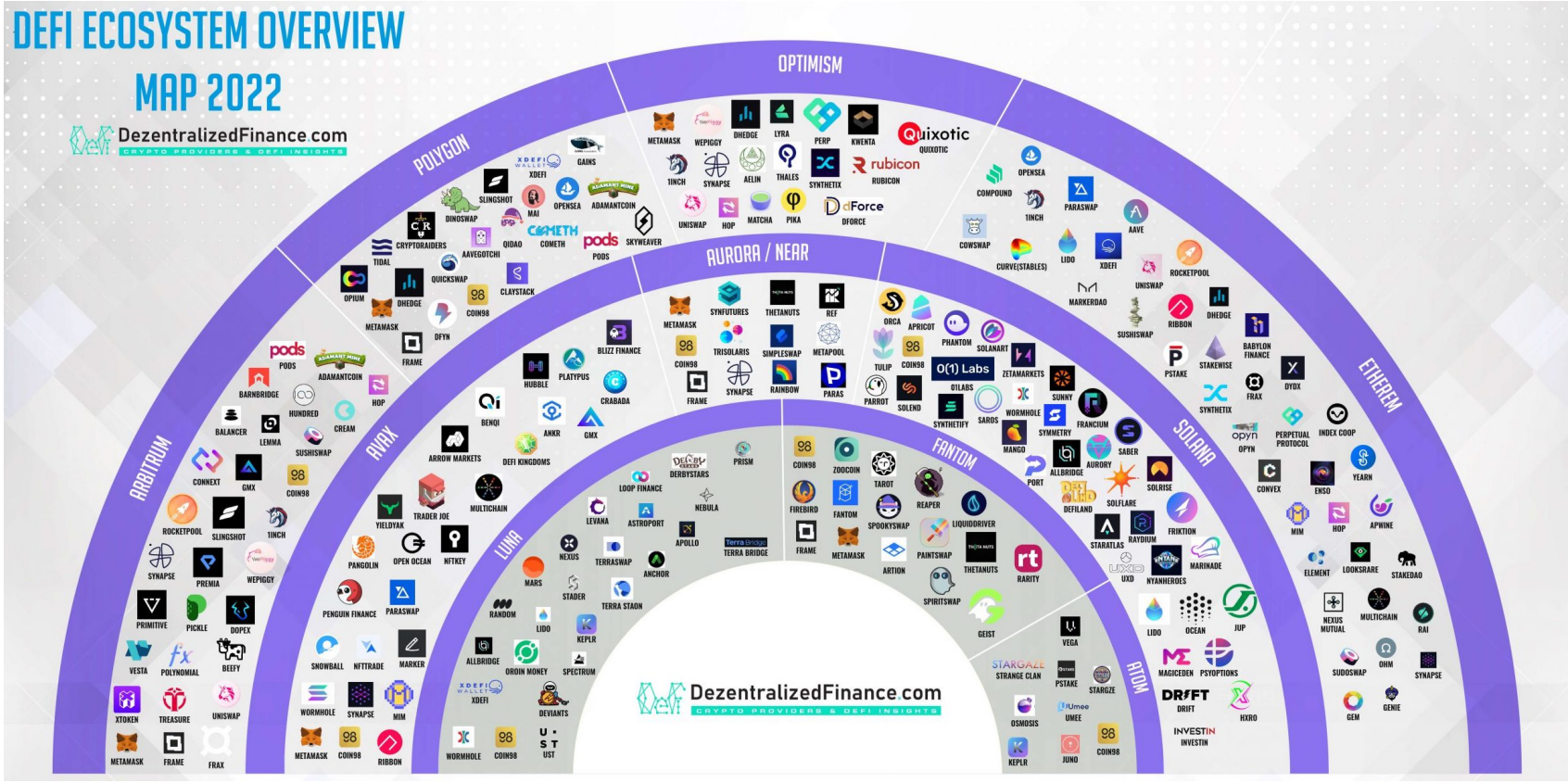
Limitations of Bitcoin as Money

- **Volatility**: Bitcoin's price is highly volatile, making it challenging to use as a stable medium of exchange and store of value.
- **Scalability**: The Bitcoin network has limited capacity to process transactions, leading to congestion and higher fees during periods of high demand.
- **Regulatory Uncertainty**: Bitcoin's decentralized nature and pseudonymous transactions have led to regulatory scrutiny and uncertainty, hindering its mainstream adoption.
- **Energy Consumption**: Bitcoin mining consumes a significant amount of energy, raising concerns about its environmental sustainability.
- **Privacy Concerns**: While Bitcoin transactions are pseudonymous, they are recorded on a public ledger, raising privacy concerns for users.
- **Irreversible Transactions**: Bitcoin transactions, once confirmed, cannot be reversed, posing a risk for mistaken or fraudulent transactions.
- **Adoption Barriers**: Bitcoin faces adoption barriers such as lack of infrastructure, limited merchant acceptance, and unfamiliarity among consumers.
- **User Experience**: The user experience of Bitcoin wallets and transactions can be complex and intimidating for non-technical users.

Ethereum (ETH): The Foundation of DeFi

- Ethereum is the leading smart contract platform and serves as the foundation for most DeFi projects. Its native token, ETH (Ether), is used for transaction fees (gas), collateral, and more.
- Ethereum Virtual Machine (EVM) is an environment in which all Ethereum accounts and smart contracts live.
- The success and growth of Ethereum have been instrumental in the rise of the DeFi sector.

It’s an intertwined multiverse of (more or less) decentralized protocols forming **DeFi**



Stablecoins: Stability in a Volatile Market

- Stablecoins are cryptoassets pegged to stable assets like the US dollar. They provide stability in the volatile crypto market and are used for trading, lending, and earning yield in DeFi.
- Examples of stablecoins include DAI (MakerDAO), USDT (Tether), and USDC (USD Coin). These stablecoins are widely used in DeFi protocols.

Types of Stablecoins

- Fiat-backed Stablecoins: These are cryptoassets that are directly pegged to and backed by real-world assets like the US Dollar or Euro. Example: USDT, USDC.
- Over-collateralized Stablecoins: These stablecoins are backed by other cryptoassets. The amount of cryptoasset held as collateral is more than the stablecoin's value. Example: DAI.
- Algorithmic Stablecoins: These stablecoins are not backed by any reserve. Instead, their stability is achieved through algorithms and smart contracts that manage the supply of the coin. Example: UST (Terra Luna).
- Hybrid Stablecoins: These stablecoins combine the features of the above types to achieve stability. Example: FRAX.

What Makes Stablecoins Money?

- **Price Stability**: Stablecoins maintain a stable value relative to a specific asset or basket of assets, reducing volatility.
- **Backed by Assets**: Many stablecoins are backed by assets held in reserve, providing stability and confidence in their value.
- **Transparency and Auditing**: Regular audits and transparent reporting of reserves (should) ensure trust and credibility in stablecoin operations.
- **Redeemability and Liquidity**: Stablecoins offer mechanisms for users to redeem them for underlying assets or fiat currency, providing liquidity and usability.
- **Global Accessibility**: Stablecoins can be transferred instantly and seamlessly across borders, enabling low-cost cross-border payments.
- **Smart Contract Capabilities**: Some stablecoins leverage smart contracts to automate functions and enhance efficiency and transparency.
- **Regulatory Compliance**: Stablecoins that comply with relevant financial regulations inspire greater trust and adoption among users and businesses.

Limitations of Stablecoins as Money

- **Centralization Risk**: Stablecoins issued and managed by centralized entities may pose counterparty risks.
- **Asset Backing Risks**: Stablecoins backed by assets are subject to risks associated with those assets, such as inflation and counterparty risk.
- **Regulatory Uncertainty**: Stablecoins may face regulatory scrutiny and uncertainty, impacting their availability and stability.
- **Redemption and Liquidity Risks**: Stablecoins may face challenges in redeeming them for underlying assets or fiat currency, leading to liquidity issues.
- **Smart Contract Risks**: Stablecoins relying on smart contracts are vulnerable to bugs or exploits, risking loss of funds.
- **Market Manipulation**: Stablecoin markets can be susceptible to manipulation, undermining their stability and credibility.
- **Counterparty Risks**: Users may face counterparty risks when dealing with issuers or exchanges holding their funds.
- **Limited Use Cases**: Stablecoins are primarily suited for use as a medium of exchange or store of value, limiting their utility for other purposes.

Central Bank Digital Currencies (CBDCs)

- **Definition**: CBDCs are digital representations of a country's fiat currency issued by the central bank. They are a form of legal tender and operate on blockchain or distributed ledger technology.
- **Types of CBDCs**:
  - **Retail CBDCs**: Accessible to the general public for everyday transactions, similar to physical cash or digital wallets.
  - **Wholesale CBDCs**: Restricted to financial institutions for interbank settlements, clearing, and other wholesale financial transactions.

  Examples:
  - **Retail CBDCs**:
    - e-Krona (Sweden)
    - Digital Yuan (China)
    - Sand Dollar (Bahamas)
  - **Wholesale CBDCs**:
    - Project Ubin (Singapore)
    - Bank of Canada's Project Jasper (Canada)
    - Project Stella (European Central Bank and Bank of Japan)

Advantages of CBDCs Compared to Bitcoin and Stablecoins

- **Central Bank Backing**: CBDCs are backed by central banks, providing them with the full faith and credit of the issuing government.
- **Legal Tender Status**: CBDCs have legal tender status within their jurisdictions, making them widely accepted for payments and financial obligations.
- **Price Stability**: CBDCs are designed to maintain a stable value relative to the national currency, reducing volatility and maintaining purchasing power.
- **Regulatory Oversight**: CBDCs are subject to regulatory oversight and compliance with financial regulations, addressing concerns associated with unregulated cryptocurrencies and stablecoins.
- **Interoperability**: CBDCs are seamlessly integrated with existing financial infrastructures, facilitating efficient cross-border payments and settlement.
- **Financial Inclusion**: CBDCs promote financial inclusion by providing access to banking services and digital payments for unbanked populations.
- **Monetary Policy Tools**: CBDCs enable central banks to implement monetary policy tools, such as interest rate adjustments and money supply control, more effectively.
- **Privacy and Security**: CBDCs can be designed with privacy-enhancing features and robust security measures to protect against fraud and cyberattacks.

Dangers of Central Bank Digital Currencies (CBDCs)

- **Financial Stability Risks**: Introducing CBDCs could disrupt traditional banking systems and monetary policy transmission mechanisms, potentially leading to financial instability.
- **Privacy Concerns**: CBDCs may raise privacy concerns due to centralized issuance and potential surveillance of transactions, posing risks to financial privacy.
- **Cybersecurity Vulnerabilities**: CBDCs are vulnerable to cyberattacks, hacking, and data breaches, threatening the security and integrity of digital currency systems.
- **Operational Risks**: Implementing and managing CBDC systems involves operational complexities, including technology infrastructure and regulatory compliance, which may lead to operational failures or system outages.
- **Monetary Policy Challenges**: CBDCs could pose challenges to monetary policy implementation, including managing interest rates, controlling money supply, and addressing liquidity needs.
- **Financial Inclusion Barriers**: Despite their potential to promote financial inclusion, CBDCs may exacerbate existing inequalities if access barriers or digital literacy challenges prevent marginalized populations from participating fully in the digital economy.
- **Dependency on Technology Providers**: Central banks may rely on technology vendors or third-party service providers to develop and maintain CBDC infrastructure, introducing dependency risks and potential conflicts of interest.

Contacts:

- Twitter: @lkristoufek
- E-mail: LK@ruk.cuni.cz