FEDERAL RESERVE BANK of ST. LOUIS

CENTRAL TO AMERICA'S ECONOMY®

Dialogue with the Fed

The Blockchain Revolution: Decoding Digital Currencies

Fernando M. Martin
Assistant Vice President
Federal Reserve Bank of St. Louis

The views expressed here are my own and do not necessarily reflect the views of the Federal Reserve Bank of St. Louis, the Federal Reserve System, or the Board of Governors.

Introduction

Interest in blockchain technology and its applications continues to grow.

- cryptocurrencies, stablecoins, decentralized finance, CBDC

In part, driven by speculation, regulatory arbitrage and technology enthusiasm.

Ultimately, the future of blockchain applications will depend on their ability to be secure, efficient and cheap.

Key elements of blockchain revolution:

- Front-end: permissionless access to money, payments and finance
- Back-end: decentralized database management

Roadmap

1. Cryptocurrencies & Blockchain
2. Stablecoins
3. Decentralized Finance (DeFi)
4. Central Bank Digital Currency (CBDC)

Cryptocurrencies & Blockchain

We already have digital money

Most money balances are in the form of digital dollars held in bank accounts.

A bank account exists in an electronic ledger.

Accounts are credited and debited according to our instructions

- sent as *cryptographically* secure messages over the internet.
- messages are executed by trusted third parties in the banking system

We trust banks to keep our accounts true and safe.

In a sense, we have had "cryptocurrencies" for a long time. What is new?

Cryptocurrencies and blockchain

Every money and payments system relies on trust.

With cryptocurrencies, the digital ledger containing money accounts is managed by a community of volunteers (instead of a bank).

This digital ledger is called a blockchain (in reference to its peculiar structure).

The protocols governing how the blockchain is updated and maintained are enshrined in open-source code (full transparency).

Ultimately, users must trust the mathematical structure embedded in the database and the computer code governing its maintenance.

The double-spend problem

Managing a digital ledger without a delegated accounts manager is not trivial

- ledger should truthfully record credits and debits
- need to prevent the fabrication of histories

How to prevent users from spending digital dollars twice?

- easy to make a copy of a digital file before transferring it
- Bitcoin was the first system to solve this problem for digital money *without* a trusted intermediary

Communal record-keeping

Cryptocurrencies follow a communal record-keeping model

- similar to small villages
- histories are known by all members of the community
- shared responsibility

Key: open, shared ledgers are very difficult to alter without communal consensus.

How blockchain technology works

For cryptocurrencies, the database is called the blockchain.

- Basically a ledger of money accounts, each with a unique address.

These accounts are like post office boxes with transparent windows:

- anyone can look in
- no one has access without the correct password
- account name is pseudonymous

Cryptoassets are thus digital bearer instruments (cryptocurrencies = digital cash).

Front-end: cryptoassets are permissionless

No permission is needed to acquire or spend cryptoassets:

- no need to disclose personal information to open an account
- just need an internet connection

A wallet is the software that is used to communicate with the system miners.

- Generates a public address (location) and a private key (password)

"Front-end" experience is very similar to online banking...

...but there is no service department to call if the private key is lost or stolen!

Back-end: database management

One key innovation is how the database works (the "back-end").

Computer code determines who is permitted to write to the database and how this effort is rewarded.

Can these protocols process payments and manage money accounts more securely, efficiently and cheaply than conventional systems?

Cryptocurrency applications

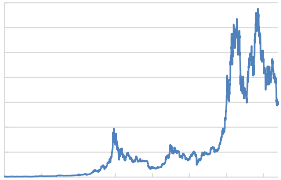
Recording money balances requires a monetary unit (e.g., U.S. dollar).

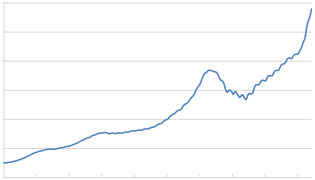
For cryptocurrencies, this unit is the native token (e.g., bitcoin, ether).

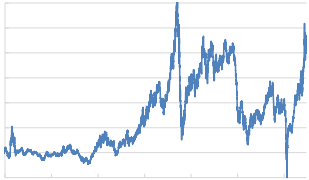
From an economic perspective, native tokens looks like a foreign currencies.

An ongoing challenge: exchange rate volatility.

Can you spot the cryptocurrency?

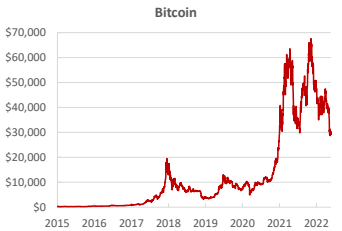


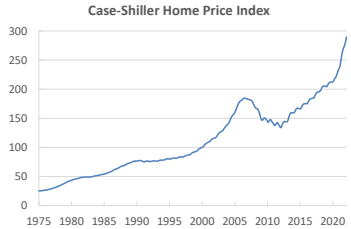


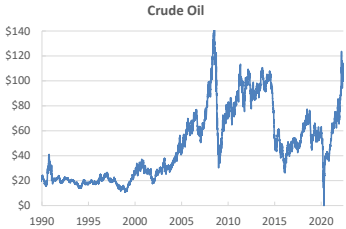


Source: Yahoo Finance and FRED.

Can you spot the cryptocurrency?







Source: Yahoo Finance and FRED.

Bitcoin—U.S. dollar exchange rate

Source: Yahoo Finance.

Ether—U.S. dollar exchange rate

Source: Yahoo Finance.

Stablecoins

Stablecoins

Cryptocurrencies suffer extreme price volatility.

- makes them highly unsuitable as payment instruments

A stablecoin is a cryptocurrency that ties its value to an asset outside its control.

Which asset?

- US dollar, the unit of account in the US and the world's reserve currency
- other currencies, including cryptocurrencies
- commodities
- other assets

Stablecoins and financial stability

Stablecoins are similar to bank deposits or money market mutual funds.

Why choose stablecoins over traditional financial arrangements?

- Efficiency vs. regulatory arbitrage

Unless fully-backed, stablecoins are potentially prone to "bank runs."

Possibility of systemic risk if stablecoins become large enough and sufficiently interconnected with traditional finance.

Decentralized nature of stablecoins makes regulation a challenge. Though many stablecoins submit themselves to regulation.

Decentralized Finance

Smart contracts

Decentralized Finance (DeFi) relies on smart contracts:

- computer programs designed to execute an agreed-upon set of actions
- pre-blockchain example: vending machines

Smart contracts allow interested parties to engage in secure financial transactions without the participation of third parties.

Applications go beyond financial transactions.

Smart contracts vs. traditional finance

In traditional finance, many third parties are involved in a transaction: intermediaries (bank or broker), appraisers, loan servicers, asset custodians, etc.

In a smart contract, the entire agreement is specified as part of the computer program and stored on a blockchain.

Blockchain handles the faithful execution of contract—no need for third parties.

What if elements of the contract (e.g., collateral) do not live on a blockchain?

Asset tokenization

Asset *tokenization* involves converting ownership of an asset into digital tokens.

In principle, allows physical assets to "live" in the blockchain.

Enforcement of property rights a ongoing challenge.

Digital tokens also have various non-financial applications.

Popular: non-fungible tokens (NFTs) which serve as certificates of authenticity.

Decentralized Autonomous Organizations

A DAO is an organization represented by a computer code, with rules and transactions maintained on a blockchain.

That is, DAOs are governed by smart contracts.

Traditionally, board of directors play a critical role in corporate governance.

DAOs offer an alternative model: decentralized consensus.

How are cryptoassets actually traded?

Most popular way is through centralized exchanges (CEX):

- work like a traditional broker
- exchange acts as custodian—client does not own cryptoassets
- face same trust and security issues as traditional intermediaries

Decentralized exchanges (DEX):

- rely on smart contracts; peer-to-peer transactions
- traders keep custody of their funds and interact directly with smart contracts

Central Bank Digital Currency

Central Bank Digital Currency (CBDC)

A CBDC is a digital liability of a central bank that is widely available to the general public.

Banks and a few other agencies are permitted to have accounts at the Fed. These "reserve accounts" function as digital currency.

Should we make reserve accounts more broadly accessible in the form of CBDC?

General public already has access to digital currency in the form of bank deposits.

Why create a CBDC?

Safety? Deposits are *de facto* government liabilities.

- deposits already insured (up to a limit)
- the Federal Reserve is the lender of last resort

Counterparty risk?

- access to insured accounts may be delayed during a crisis
- thus, the existence of (collateralized) money markets used by corporations

Efficiency?

- U.S. payment system could use some improvement
- but is rapidly evolving at the wholesale level (e.g., FedNow)

Conclusions

Blockchain applications

Future of blockchain applications will depend on their ability to be secure, efficient and cheap.

DeFi still in its infancy but developing exponentially.

Front-end: permissionless access to money and payments systems and finance

Back-end: decentralized database management

- supply chain management
- proof of authenticity
- resilience

Ability to write history is a tremendous power

Individual and group histories are important for coordinating economic activity.

Modern societies devote considerable resources to maintaining reliable records.

Blockchain technology is a challenge to traditional forms of record-keeping.

Competitive pressures will further drive innovation...
...consider the impact of the telegraph, telephone, computer and internet.

Expect even more dramatic changes...though the future remains uncertain.