The Genesis Block

An introduction to blockchain, cryptocurrency, and more…

Paul Bances + Liam DiGregorio

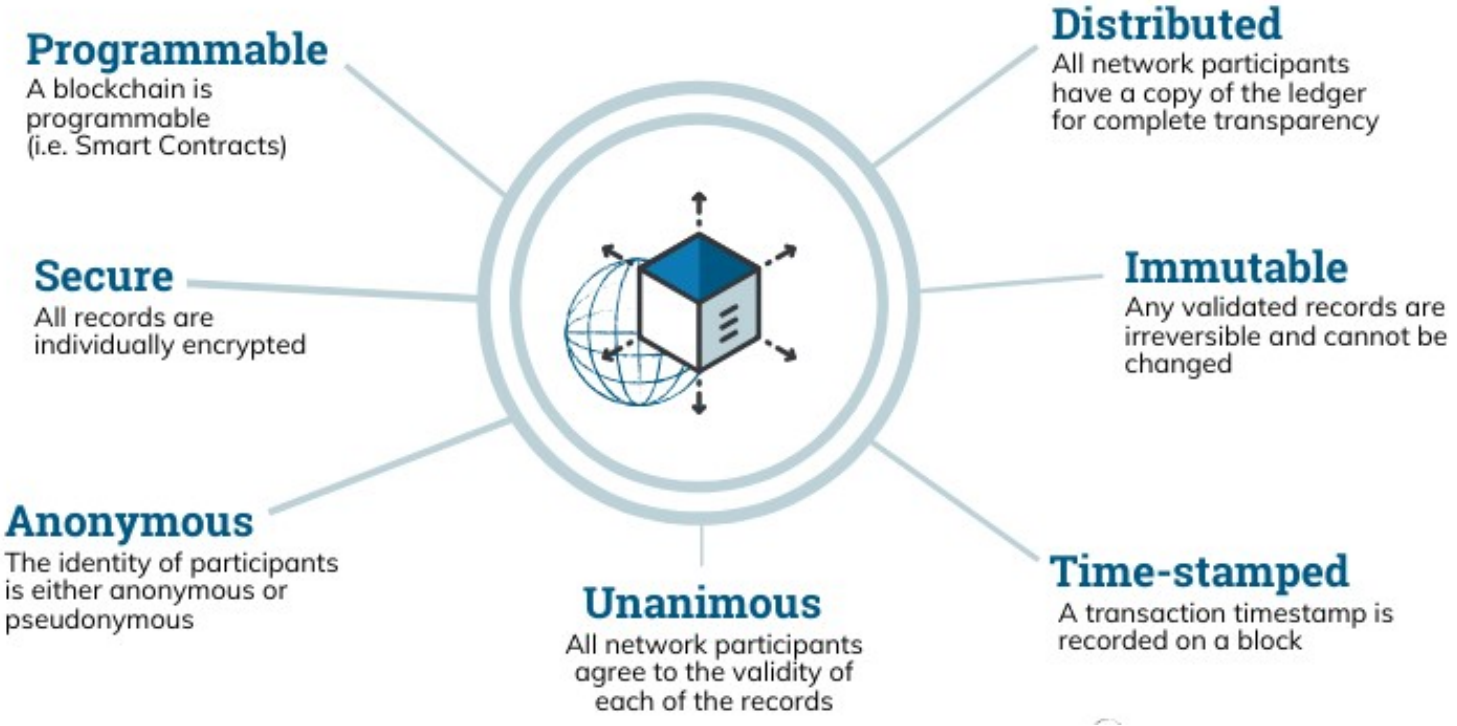
What is blockchain?

What are Blockchains?

Blockchain owes its name to the manner in which it stores data, namely that the information is packaged into *blocks*, which link to form a *chain* with other blocks of information.

- **Blockchain** is a system of recording information in a way that makes it difficult or impossible to change or forge.
- A blockchain is a **digital ledger of transactions**, which is shared by all parties in a **distributed network**. The information is not stored in a single place, but across the participants in the peer-to-peer network. The decentralized database managed by multiple participants is known as **Distributed Ledger technology (DLT).**
- A blockchain database of transactions is split into **blocks.** Each block in the chain contains a set of transactions. Blocks are validated by the **nodes** of a network. The records on a blockchain are secured through **cryptography.**
- When a new block is added to a chain, it contains a **cryptographic hash** of the previous block. It is this act of linking blocks into a chain that makes the information stored on a blockchain trustworthy.

The Properties of Distributed Ledger Technology (DLT)



Key Characteristics of a Blockchain

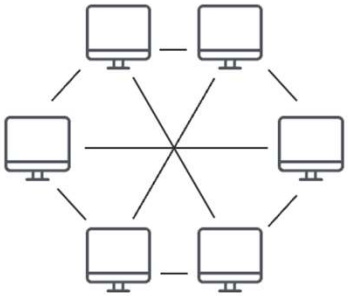
Decentralized control: Communal consensus, rather than one party's decision, dictates who gets to access or update the blockchain.

Tamper-evident: It's immediately obvious if data stored on the blockchain has been tampered with.

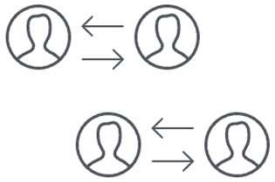
Nakamoto consensus: One has to provably spend resources when updating the blockchain.

What is Decentralization?

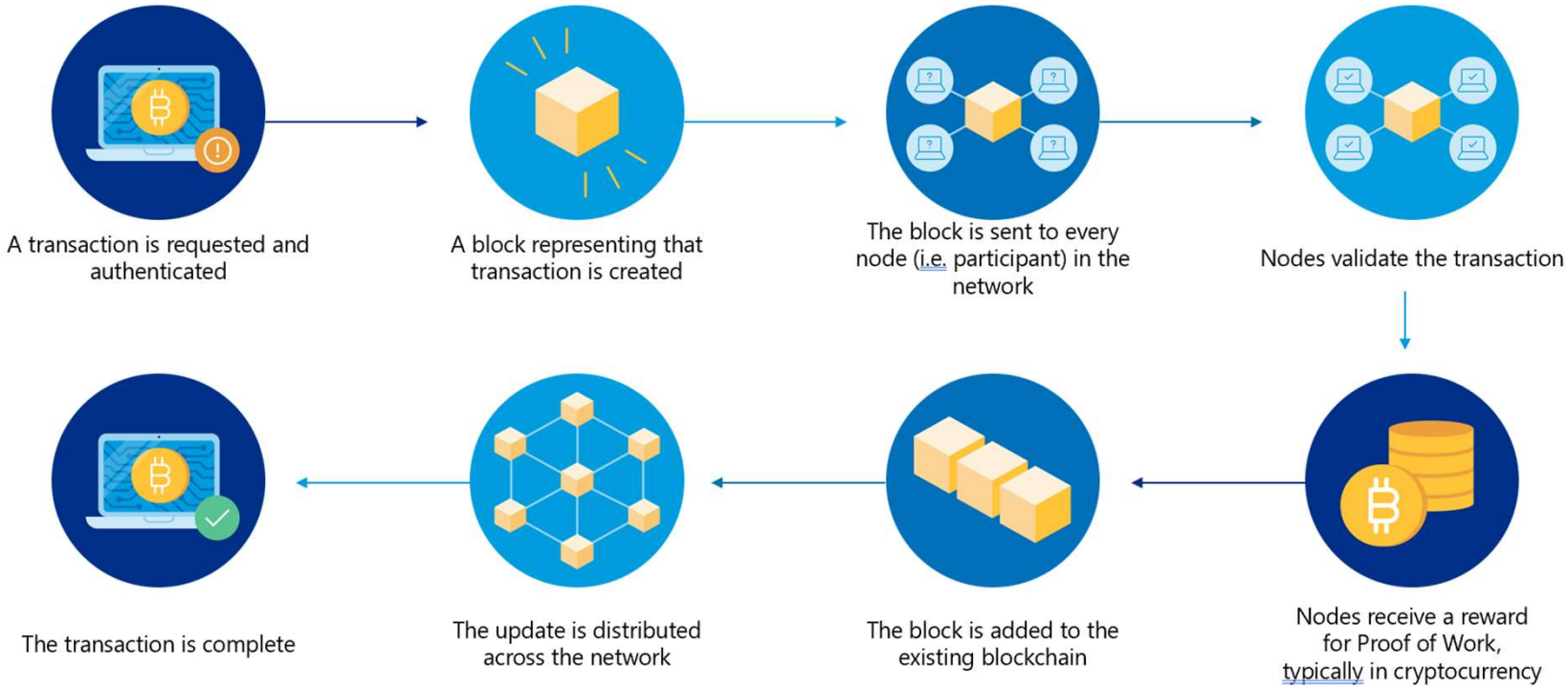
- Authorization according to an openly-known protocol
- Data is stored by the participants



- Think:
  - Peer-to-peer networking
  - Flat org chart
  - Pure democracy
  - Barter economy
  - Community



The expansion of crypto currencies has been the first use case for decentralized protocols



What is cryptocurrency?

What is cryptocurrency?

Cryptocurrency is a specific application use case for blockchain distributed ledgers. Cryptocurrency is a combination of cryptography and currency.

- The digital asset that is transacted is designed to work as a medium for exchange
- Supply is not determined by a central bank, but rather by the consensus algorithm
- Created and stored using blockchain technology to control creation of monetary units and verify asset transfer

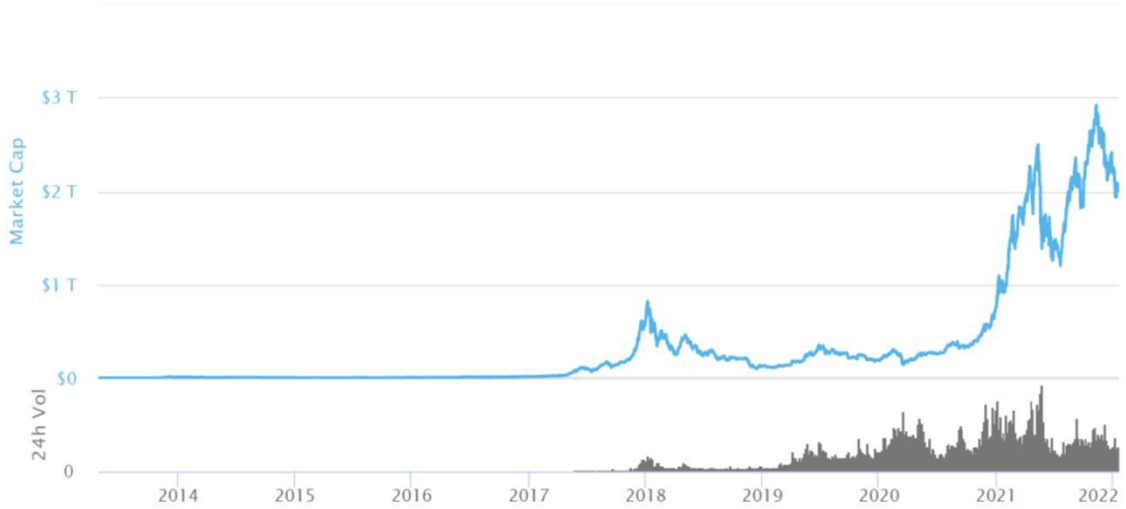
Cryptocurrencies can be used to make payments and purchases, although much of the interest today is in investing:

- Common cryptocurrencies today are Bitcoin, Ethereum, XRP, Bitcoin-cash, Litecoin, Cardano, Algorand, etc. They focus different purposes: investment, financial products, payments, stability, etc.
- 2021 saw the rise of "meme coins" such as Doge coin and Shiba Inu coin
- Today, the total cryptocurrency market exceeds $2 trillion!

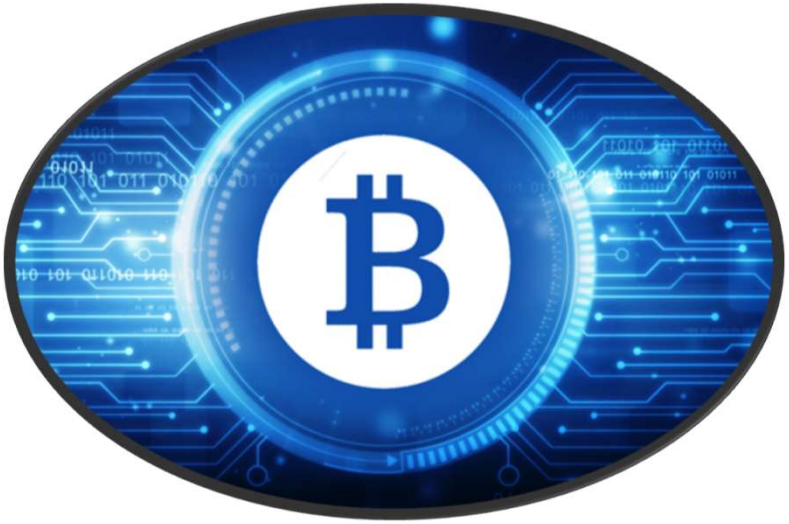
Cryptocurrency market cap experienced tremendous growth during the last 2 years

- Today, Bitcoin's market cap is ~$800bn, representing ~40% of the total cryptocurrency market
- Ether's market cap ~$370bn representing ~19% of the total cryptocurrency market

(*www.coinmarketcap.com*)



Bitcoin Components



Identity
Making an account in the system

Transactions
Sending and receiving Bitcoin

Distributed Ledger
Recording transaction history

Trustless Consensus
Agreeing on changes to the ledger

Public Keys
Private Keys
Wallets

- Each identity is represented with a unique **public key**
- A corresponding **private key** acts as a key to “unlock” the public key and your money
- Unique private key generated randomly; public key derived from private key
- Public key for ***receiving***, private key for ***redeeming***

Bitcoin Wallets

To secure our **identity**, we need to secure our **private key**

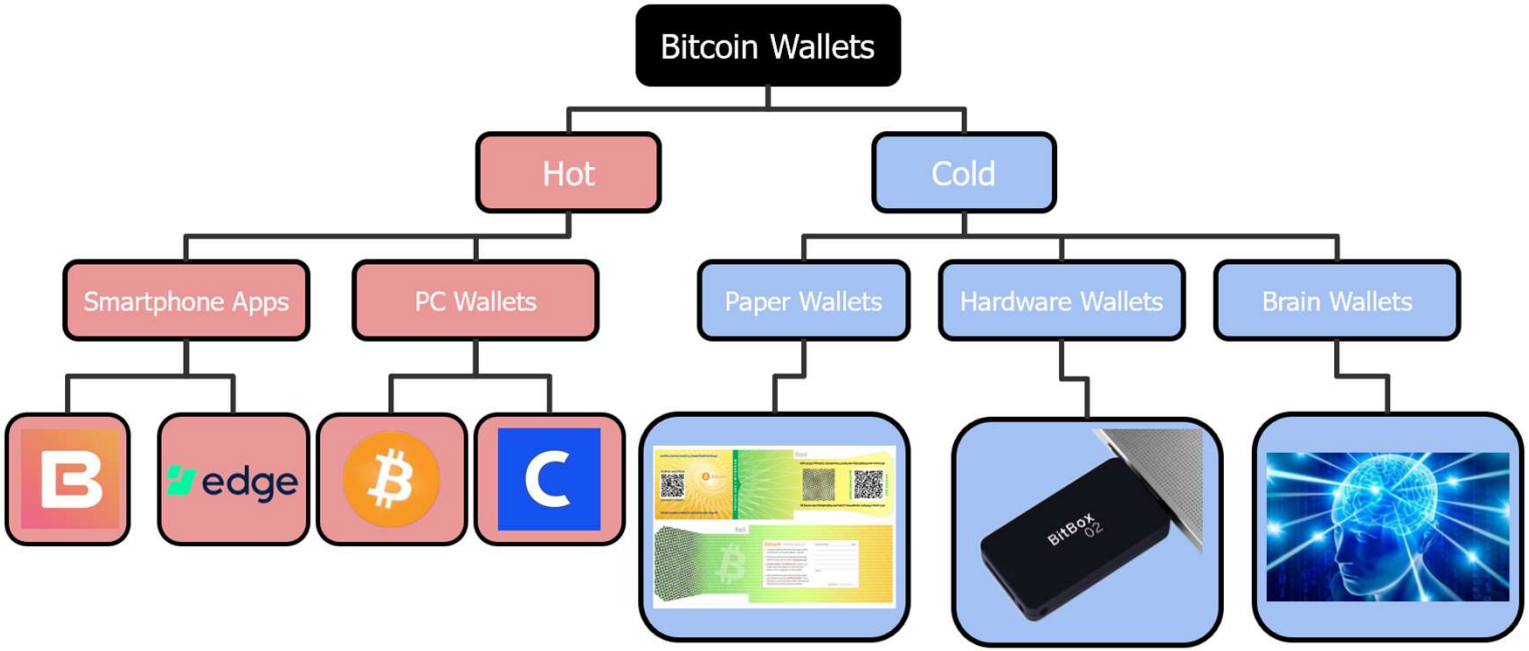
How do we manage all of our keys? With wallets!

ADDRESS:
1JJQmRbU9JT9mfxjp756Y
MuxV6yksKtbk5

PRIVATE_KEY:
L1fm3iAFdDHwSD3CZuZm
Wp54GXpQ6QzUjmrACVfKK
E8BkggW99u3

What do **wallets do**?

- Provides a user interface to the blockchain
- Keep track of your private key
- Store, send, receive, and list transactions
- Maybe some other fancy functionalities



Hot vs. Cold Wallets

CRYPTOGRAPHIC HASH FUNCTIONS

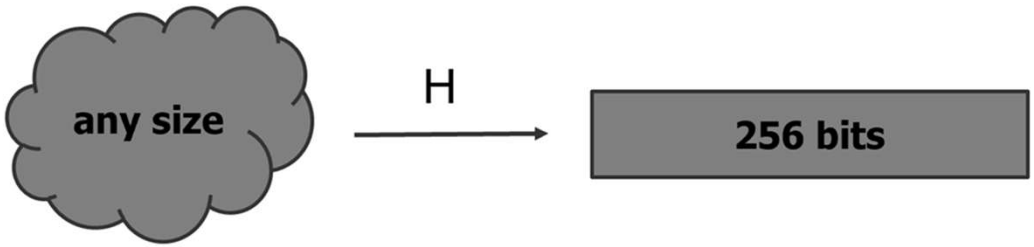
How do we ensure trust in communication in a trustless environment?

⇒ With **cryptographic hash functions**

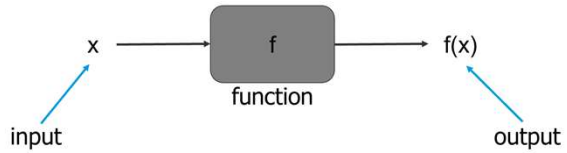
USED HIGHLY IN DIGITAL SIGNATURES

Image source: https://spiritegg.com/wp-content/uploads/2016/03/63180952_fingerprint_types624.jpg

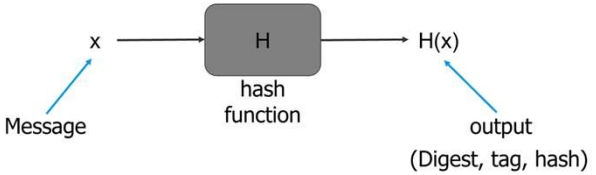
CRYPTOGRAPHIC HASH FUNCTIONS



CRYPTOGRAPHIC HASH FUNCTIONS



CRYPTOGRAPHIC HASH FUNCTIONS



#CRYPTOGRAPHY

CRYPTOGRAPHIC HASH FUNCTIONS

Cryptographic hash function:

A hash function with three special properties:

- Computationally Efficient
- Collision resistance
- Hide information

The equivalent of **mathematical fingerprints/identifiers**

Image source: http://chimera.labs.oreilly.com/books/1234000001802/ch08.html#_proof_of_work_algorithm

```
I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...
I am Satoshi Nakamoto16 => 8fa4992219df33f50834465d3047429...
I am Satoshi Nakamoto17 => dca9b8b4f8d8e1521fa4eaa46f4f0cd...
I am Satoshi Nakamoto18 => 9989a401b2a3a318b01e9ca9a22b0f3...
I am Satoshi Nakamoto19 => cda56022ecb5b67b2bc93a2d764e75f...
```

Ethereum vs Bitcoin...What is the difference?

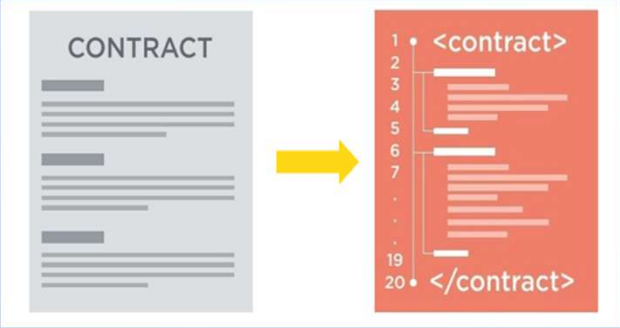
Bitcoin

- The "Gold Standard" of blockchains
- Asset: Bitcoins
  - Primary purpose of the Bitcoin blockchain
- Simple and robust
- Stack-based, primitive scripting language, not Turing-complete
- UTXO-based

Ethereum

- Smart Contract Blockchain Platform
- Asset: Ether
  1. Fund computation
  2. Align incentives
- Complex and feature-rich
- Turing-complete scripting language
- Account-based

Smart Contracts



A smart contract, like any contract, establishes the terms of an agreement. But unlike a traditional contract, a smart contract's terms are executed as code running on a blockchain like Ethereum. Smart contracts allow developers to build apps that take advantage of blockchain security, reliability, and accessibility while offering sophisticated peer-to-peer functionality — everything from loans and insurance to logistics and gaming.

Ethereum Smart Contracts Purposes

- Ethereum Contracts generally serve four purposes:
  - **Store and maintain data**
    - Data represents something useful to users or other contracts
    - Ex: a token currency or organization's membership
  - **Manage contract or relationship between untrusting users**
    - Ex: financial contracts, insurance
  - **Provide functions to other contracts**
    - Serving as a software library
  - **Complex Authentication**

What is a stablecoin?

What is a central bank digital currency?

What is a stablecoin?

A rapidly growing area in the crypto space: stablecoins

What is a Stablecoin?

- **Stablecoins** are cryptocurrencies designed to maintain a **stable market price** and be **resistant to volatility**
- Stablecoins **mix the benefits of a cryptocurrency** (24/7, low-cost transfer, privacy, etc.) with **the stability of fiat currencies**
- Most stablecoins have their **values fixed by pegging them to the price of another asset** - such as a fiat currency (U.S. Dollar) or a commodity (gold)
  - By being pegged to real-world assets, they avoid the volatility of other cryptocurrencies such as Bitcoin

- **Current market cap of stablecoins is ~$53B (www.cryptoslate.com)**

Current Market Cap of Stablecoins: ~$160bn!

Source:
Bitcoin.com: Stablecoin Supply Doubles in 3 Months as Combined Market Cap Surpasses $20B - Bitcoin News
Cryptoslate.com: Stablecoin Cryptocurrencies | CryptoSlate

What is a central bank digital currency?

Emerging Area: Central Bank Digital Currencies (CBDC)

CBDC Overview

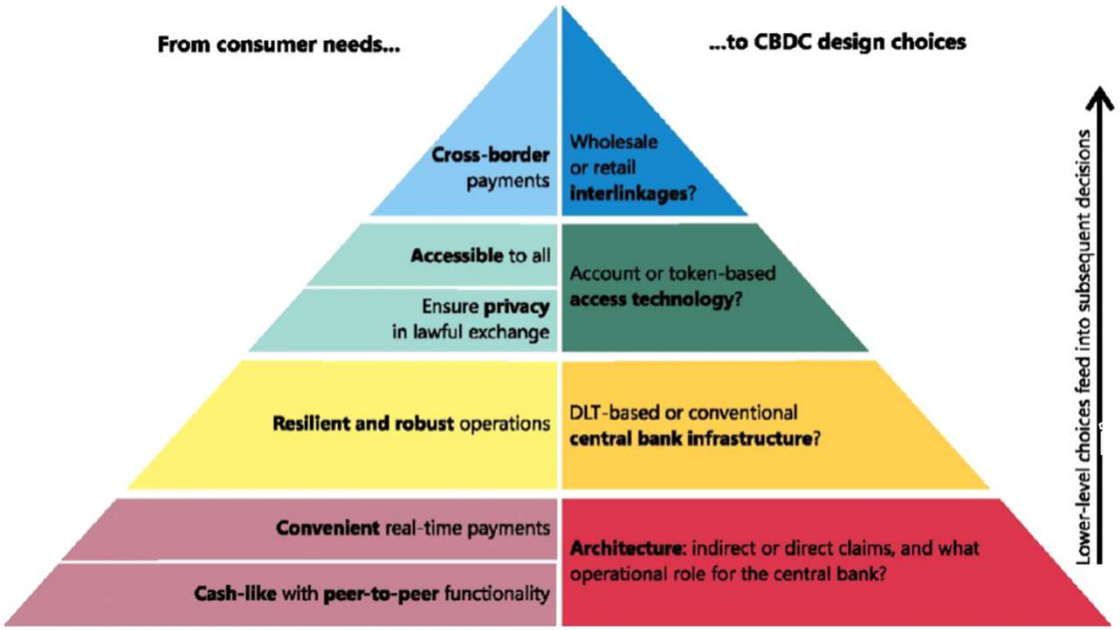
- A new variant of central bank money different from physical cash, that can be used by households and businesses to make payments and store value
- CBDCs hold the promise of increasing financial stability and payments efficiency, safety and robustness in both developed and emerging economies; and inclusion (especially in emerging economies).
- Numerous central banks and multi-lateral institutions are evaluating use cases and working on pilot programs for digital currencies that can serve as a mor efficient form of fiat currency.

Central Bank Motivations behind CBDC efforts include

- More efficient form of fiat currency
- Address trend towards digitization
- Preserve monetary system stability
- Compete against private sector
- Access to consumer data
- Promote Financial inclusion

What is a central bank digital currency?

Emerging Area: Central Bank Digital Currencies (CBDC)



Other Hot Topics

Fungible Assets

Assets that are capable of mutual substation, interchangeable

Examples: oil, cash, cryptocurrencies

Non - Fungible Assets

Assets that are incapable of mutual substitution, non interchangeable

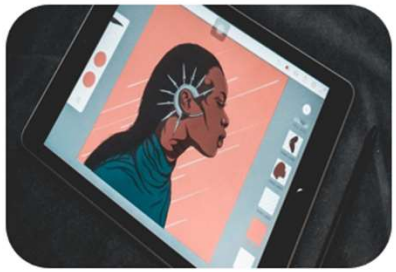
Examples: art, land deeds, collectibles, credentials

NFT Applications

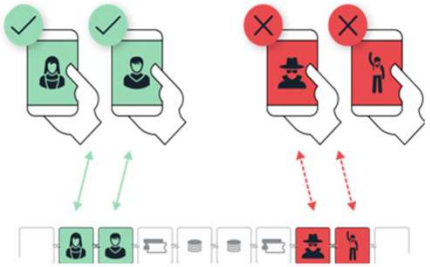
While being unique, NFTs have a diverse and broad spectrum of applications

Retail - Coupons, Merchandise for Merchants

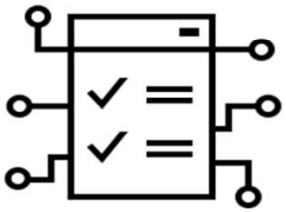
Music

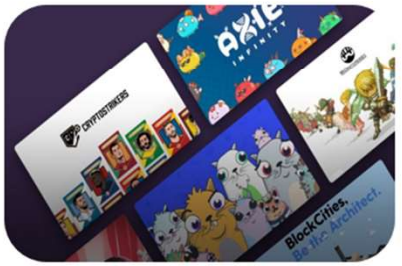


Digital Art



Ticketing Experiences





Decentralized Finance (DeFi) Defined

- **DeFi:** Digitally-native financial services built on open blockchain networks
- **Liquidity Mining:** Earning interest from DeFi applications – typically for providing capital (supplying liquidity) to the application
- **Yield Farming:** Structuring holdings and deposits to maximize yield

A case study for DeFi - Aave

Aave is a money-market like smart contract that enables users to borrow or lend digital assets.
Key Aspects:

- Users can deposit/withdraw, borrow/repay at any time
  - Upon withdrawal, depositors (lenders) immediately collect their principal + Interest
- Smart contract charges a supply-and-demand based rate for borrowing
  - Interest rates increase with utilization rates (utilization rates = amount currently borrowed/total lending supply)
- Interest is paid pro-rata to capital providers (lenders)

Why is this important?

Why is this important?

- Early promise of decentralized protocols as an enabling technology (Web3)
- Interest in and demand for BTC and other cryptocurrencies continue to grow
- Continued push in retail user enablement
- Landscape is evolving rapidly in all areas
- Increased funding leading to greater innovation
- Increasing corporate/institutional interest – fueling the ecosystem development
- Growing regulatory/government/central bank interest and attention


Thank you