Bitcoin

A non-expert's explanation

David Toms

February 19, 2025
OLLI-GMU Investment Forum

Disclaimer: I am not a certified financial analyst.
Any trading decisions you make are your responsibility

Introduction

Scope of crypto markets:

- There are 9,000+ crypto coins available for purchase operating on 1000+ networks, worldwide
- Total crypto coin market value = $3.7T
- Bitcoin holds 60%
- Crypto coin prices and future waiting for clarity from Trump administration
- Trump has requested a study be conducted about a sovereign wealth fund

What is Bitcoin?

- Bitcoin is a digital currency that runs on block chain technology
- Bitcoins are “non-fungible”
- It is secure and independent of any government or institution
- There is a maximum limit of 21M bitcoins, of which 19.5M have been “mined”
- It is considered a “store of value”, like gold, because it is not subject to any currency devaluation via inflation
  - Indeed, it is most recently uncorrelated to the S&P500
- Block chain is the ledger for all transactions, worldwide
- All transactions and block chain data are encrypted by both public and private keys
- All block chains (ledgers) are distributed equally to independent processing nodes located globally
- We do not know for sure who invented bitcoin

What is “Fungibility”

- In economic theory, the term **"fungible"** refers to goods or assets that are **interchangeable** with others of the same type and have a standardized value. Fungible items are identical in their essential properties, making them easily replaceable or exchangeable.
- **Key Characteristics of Fungibility:**

1. **Uniformity**: Every unit is the same as every other unit (e.g., one ounce of gold is identical to another ounce of gold of the same purity).
2. **Divisibility**: They can be divided into smaller parts without losing value (e.g., a dollar can be divided into cents, and its value remains proportional).
3. **Ease of Exchange**: Fungible items can be traded or substituted without differentiation.

- **Examples of Fungible Goods:**
- **Commodities**: Gold, silver, oil, and other raw materials are fungible.
- **Stocks**: Shares of the same company and class are interchangeable.
- **Non-Fungible vs. Fungible:**
- In contrast, **non-fungible items** are unique and cannot be substituted on a one-to-one basis. For example, real estate, artwork, and non-fungible tokens (NFTs) are non-fungible because their value is based on specific, unique characteristics.

How do you own bitcoin?

- Every bitcoin owner has a digital wallet, which is protected by both a public key and private key (password)
- A single Bitcoin is divisible into 100 million smaller units called **satoshis**.
- Transactions in blocks often involve fractions of Bitcoin, such as 0.001 BTC or even less.

What are Stablecoins? (e.g. Tether)

- A **stablecoin** is a type of cryptocurrency
- The value of the digital asset is supposed to be pegged to a reference asset, which is either fiat money, exchange-traded commodities (such as precious metals or industrial metals), or another cryptocurrency
- Stablecoins have yet to be proven useful or safe
- In practice, however, stablecoin issuers have yet to be proven to maintain adequate reserves to support a stable value
- There have been a number of failures with investors losing the entirety of the (fiat currency) value of their holdings.

Source: Wikipedia

What is block chain?

- Block chain is the ledger for tracking all bitcoin transactions, worldwide
- All bitcoin transactions are grouped into blocks within the ledger
- Each block has 1 MB of transactions
- Each transaction takes 250-300 bytes
- Some transactions can be much larger
- Thus, each block has typically 2000-3000 transactions
- **Blocks are maintained in sequence and are encrypted**
- **Each block is securely sequenced to the previous block**
- NSA developed an encryption algorithm called SHA-256, which is used to encrypt all transactions and prevent tampering
- The algorithm outputs a fixed length sequence of 64 characters (hash)

Bitcoin nodes

- There are almost 21000 nodes operating globally
- The purpose of a node is to capture and validate every transaction, worldwide
- Every node maintains the entire bitcoin ledger of all previous transactions
- A typical laptop computer with 500GB of extra memory can become a node.
- Many nodes run in the cloud on AWS
- Approx 2/3 of nodes are not accessible by the public
- Nodes are run on a volunteer basis, however, a node that uses a Lightning layer on top of the node software can receive small fees for micro transactions
- You can watch bitcoin transactions in real time at: https://bitnodes.io/

Bitcoin nodes

Reachable Bitcoin Nodes

Live Worldmap showing

Concentration by world region
(Largest in USA & Europe)

and

Table showing

Top 10 of 921 Countries rank-ordered
by number and percentage of Nodes in each
(Country n/a is #1, USA is #2)

Bitcoin mining

- About every 4 years, new coins are authorized automatically by the network, most recently April 2024. Each new block has a unique hash identifier.
- It is expected that all 21M coins will be discovered by year 2040
- Miners have developed software that solves complex hash (encryption) puzzles to discover new coins.
- Mining requires an enormous amount of computing power
- Miners validate transactions and create new blocks. As a reward for their work, miners receive new Bitcoins (called the **block reward**) and transaction fees.
- When Bitcoin was launched in 2008, the reward for mining a block was **50 BTC**.
- This reward halves approximately every 4 years in an event called the **halving**.
- As of now (January 2025), the block reward is **3.125 BTC**.

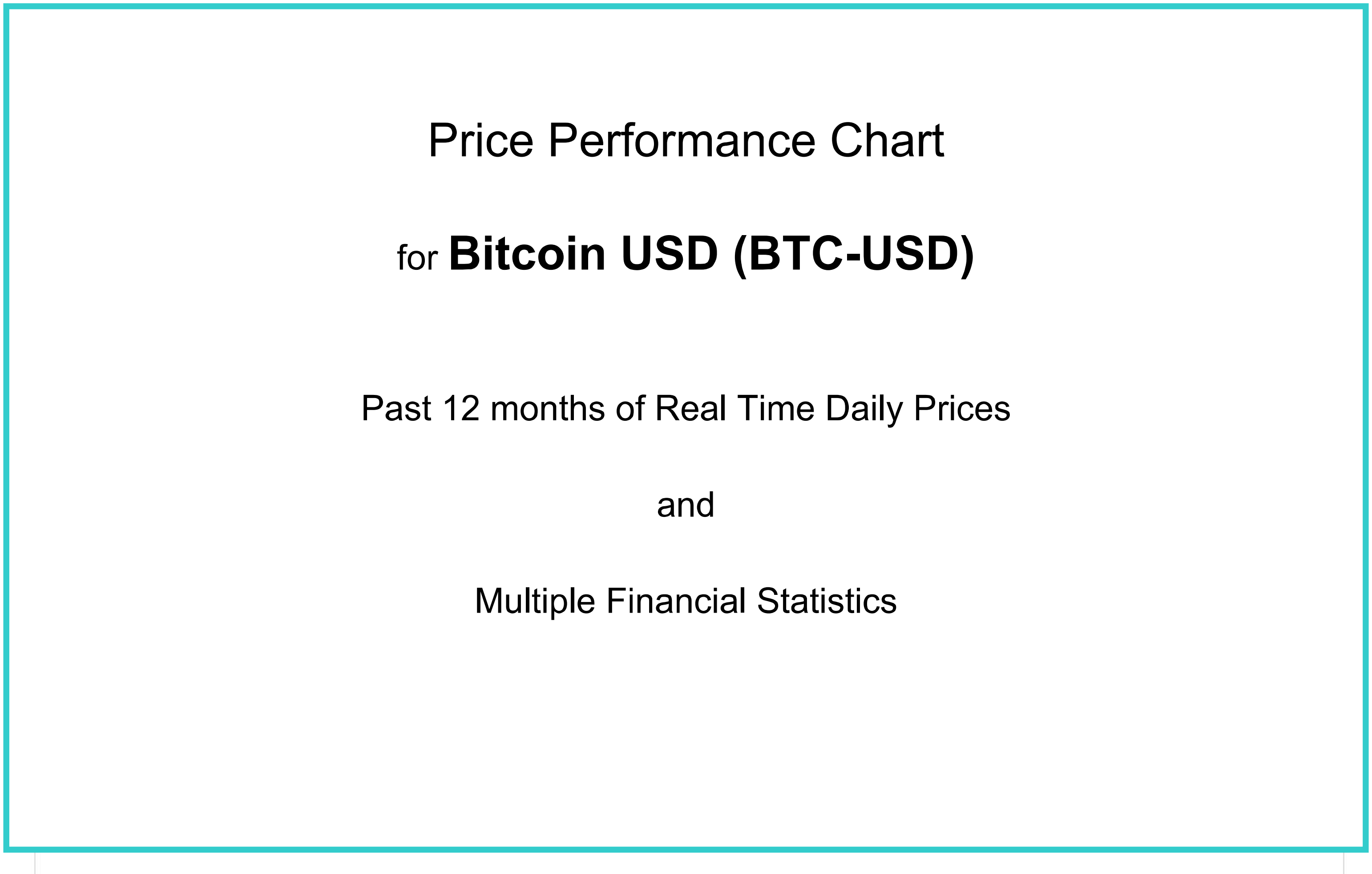
Bitcoin security

- Bitcoin operates on a decentralized network of nodes (computers) using blockchain technology.
- Attacking this network entails extremely high cost, making such an attack impractical
- No single entity, such as a government or corporation, controls the network. This reduces the risk of a single point of failure or centralized attack.
- All transactions are verifiable, reducing the risk of fraud.
- Once a block is added to the blockchain, it cannot be altered without redoing the work for subsequent blocks, making tampering extremely difficult.
- Transactions are signed using private crypto keys (passwords), ensuring that only the owner of the funds can authorize their transfer.
- Bitcoin's code is open-source, meaning anyone can review it for vulnerabilities. The community of developers and researchers continuously works to identify and fix potential issues.
- Bitcoin software is frequently updated

Bitcoin software maintenance

- Unlike traditional software projects, **Bitcoin has no central authority**. Development is guided by:
- **Consensus among developers and users** rather than a CEO or foundation.
- **Economic incentives** (users, miners, and businesses must voluntarily accept upgrades).
- **Security-first approach**, where changes undergo extensive testing.

BTC performance



Price Performance Chart

for **Bitcoin USD (BTC-USD)**

Past 12 months of Real Time Daily Prices

and

Multiple Financial Statistics

Fidelity Wise Origin Bitcoin Fund (ETF)

Price Performance Chart

for **Fidelity Wise Origin Bitcoin (FBTC)**

Past 12 months of Nasdaq Real Time Daily Prices

and

Multiple Financial Statistics

True story

Way back, when bitcoin was newly introduced, someone bought a pizza with 80,000 bitcoin   (spoiler: that's worth $8B now)

It is estimated that $2B in bitcoin have been permanently lost, mostly through forgotten passwords

- The future: It is expected that real assets will become digitized over time

    Stocks, bonds, real estate, et al

- GLTA!

Bitcoin mining, cont’d

- The mining computers take a previous block’s hash, add a random number to it, re-hash that and see if that matches the hash of a new block. If a match is found, the miner is rewarded.
- Block Hash=SHA−256(Previous Hash+Merkle Root+Nonce+Time stamp)
- The point is, every block is linked to every previous block.
- Any tampering with any block causes the entire network to invalidate the tampered block and all subsequent blocks