

Cryptocurrency

Aidan O'Hara and Tevin Parathattal

January 14, 2025



Why does Crypto Matter?

- SMIF does not trade cryptocurrencies as of this moment
- Crypto markets still influence:
 - Equity valuations
 - Risk sentiment
 - Liquidity cycles
- Understanding crypto improves macro and market awareness



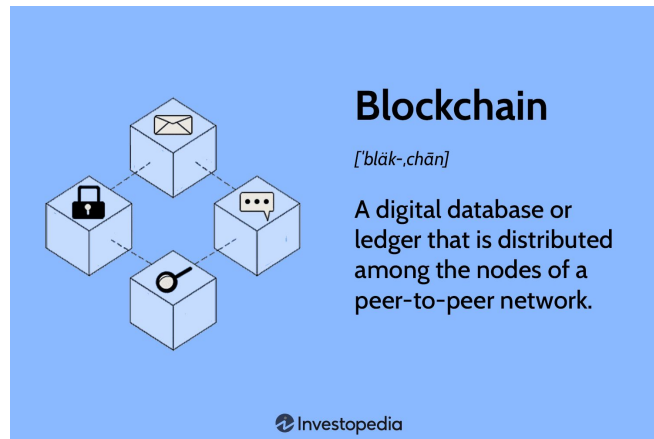
What is Cryptocurrency?

- A digital asset operating without a central authority
- Transactions occur on decentralized networks
- Ownership recorded cryptographically
- Prices driven by supply, demand, and market sentiment
- Cryptocurrency is treated as an asset, not the currency it is meant to be.
 - For reference, when we measure the value of USD, we price it against everyday goods to see how much we can buy with USD. With crypto we ask ourselves, how much crypto can we buy with USD?



What is Blockchain?

- Public, immutable transaction ledger
- Transactions grouped into blocks and linked chronologically
- No single point of control or failure
- Transparency enables real-time data analysis
- Each full node contains a list of every transaction that has happened on the network



Cryptocurrency as an Asset

- Traded primarily for price appreciation on third-party exchanges.
- Exchanges own the private keys to the crypto, not you unless you run a full node.
- No cash flows, dividends, or yield (outside of staking mechanisms)
- Valuation is driven primarily by bid/ask price just like any other equity. Some reasons for differing prices can be:
 - Liquidity conditions
 - Risk appetite
 - Design of the network
 - Market narratives/sentiment
- Exhibits extreme volatility and asymmetric return profiles



Cryptocurrency as a Currency

- Designed to facilitate peer-to-peer transactions
- Enables transfers without banks or payment intermediaries
- Settlement occurs directly on the blockchain
- Transactions are irreversible once confirmed
- Price volatility limits effectiveness as a medium of exchange
- Cryptocurrency is not necessarily the most user-friendly and requires a lot of the individual



Market Structure Differences

- 24/7 trading
- Fragmented venues
- Higher retail participation – you can buy infinite fractions of crypto, not the same for shares
- Faster feedback loops
- Tokenization are traditional exchanges' response to crypto's 24/7 availability



Exposure to SMIF

- Exposure occurs indirectly through public equities
- Crypto volatility can:
 - Increase earnings volatility
 - Drive compression or expansion
- Correlation with equities rises during market stress
- Regulatory headlines can rapidly reprice exposed stocks



Breaking Down Bitcoin

Creator Of Bitcoin?

Bitcoin was created by an anonymous person or group known by the pseudonym **Satoshi Nakamoto**, who published the white paper in 2008 and launched the system in 2009, but vanished by 2010, leaving their true identity unknown.

Why Disappear?

Nakamoto disappeared, ensuring Bitcoin's decentralization.

As of recently, there was a man named Satoshi Nakamoto, but he denies all ties to creating cryptocurrency.

What Is The “White Paper”?

Bitcoin: A Peer-to-Peer Electronic Cash System,” outlining a decentralized digital currency system to solve online payment trust issues without banks, using blockchain technology.

Satoshi Nakamoto’s Legacy...

Nakamoto’s anonymity and the technology’s structure embody Bitcoin’s core principle of decentralization: no single point of control or authority.



What are the Technicals Behind Bitcoin?

- Bitcoin is a decentralized ledger maintained by a network of nodes
- Transactions are signed messages, not physical coins
- Uses an UTXO model: funds are tracked as unspent outputs, not balances
- Transactions specify inputs, outputs, and digital signatures
- Valid transactions are grouped into blocks and added via proof-of-work
- Security comes from computational cost and economic incentives



Proof of Work v Proof of Stake

Proof of Work (PoW)

- Miners compete using computational power
- Security comes from energy and hardware cost
- Sybil resistance through real-world expense
- Used by Bitcoin

Key Difference

- PoW secures the network through **external cost**
- PoS secures the network through **internal capital risk**

Proof of Stake (PoS)

- Validators selected based on staked capital
- Security comes from economic penalties
- Lower energy usage
- Used by many newer blockchains

