



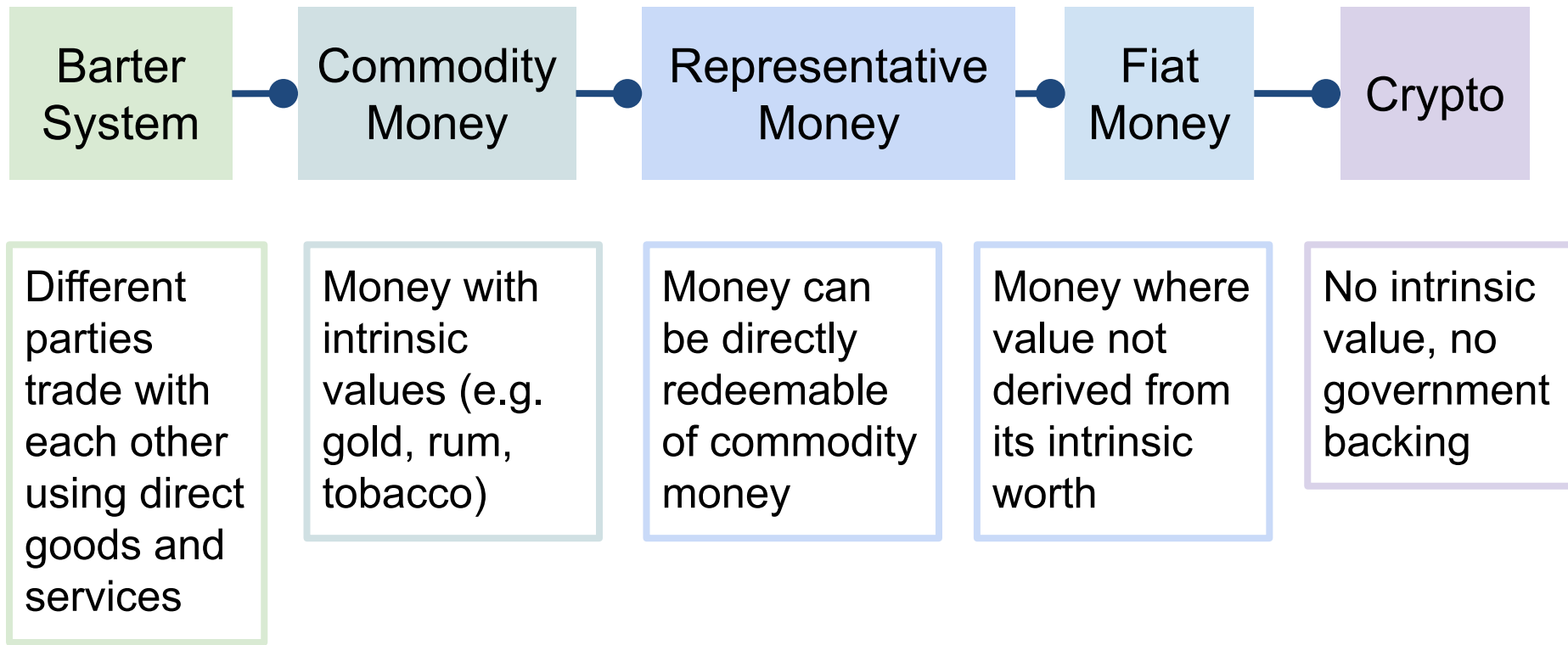
Cryptocurrency and the Cryptocurrency Crisis

Luke Marushack, Tiantian Wei, Yuchen Yang, Yutan Zhang, Jenna Zhao



UNIVERSITY OF
NOTRE DAME

The Evolution of Money



Introduction

- Ancient Stone currency on Yap Island in Micronesia.
- Stones don't move; put marks on the stone for transaction
- Richest family's Fei is in the Ocean.



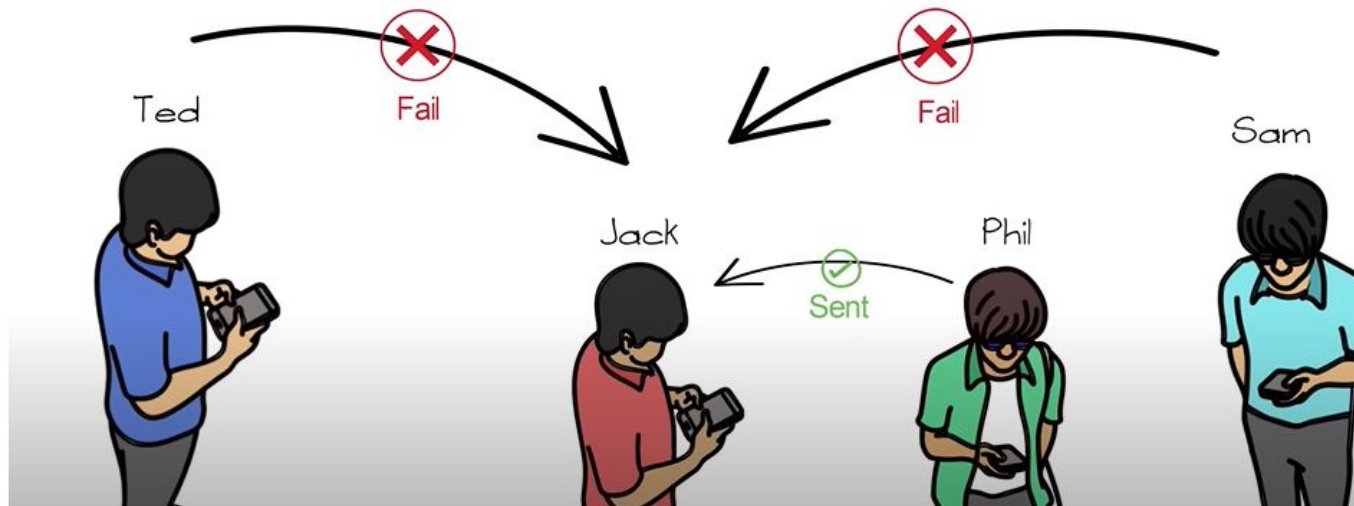
figure from: <https://arkeonews.net/rai-stones-and-bitcoin-similarity/>

Online money transfer:

- Technical Issues
- Accounts hacked
- Transfer limit exceeded
- Invisible to the public

How crypto might help:

- Transaction record inscribed in blocks
- Blocks linked to each other
- Ledger publicly distributed





Speculative Bubbles

Bubbles are characterized by:

- ❖ Overvaluation to an unsustainable level
- ❖ Frenzy of buying fueled by FOMO
- ❖ Strong overall economic performance
 - Excessive optimism
 - Easy access to credit
 - Low interest rates

When bubbles burst:

- ❖ Demand for asset inevitably ceases to increase
- ❖ Investors sell holdings
 - Sharp price decrease
- ❖ Negative financial results
 - Economic downturns
 - Panic selling

Historical Bubbles





How Does the Crypto System Work

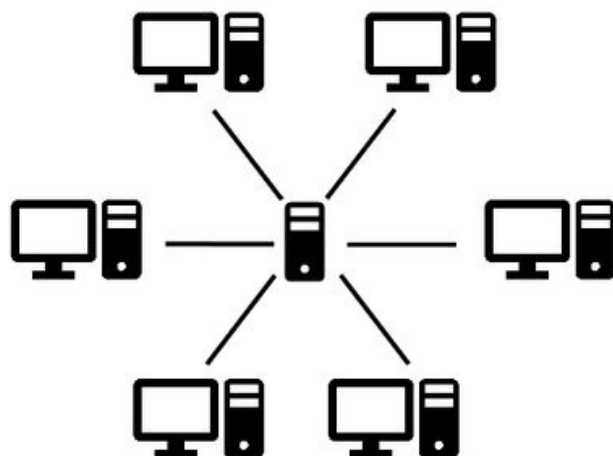
How Does the System Work

- ❖ A decentralized peer-to-peer network (the Bitcoin protocol)
- ❖ A public transaction ledger (the blockchain)
- ❖ A set of rules for independent transaction validation and currency issuance (consensus rules)
- ❖ A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)

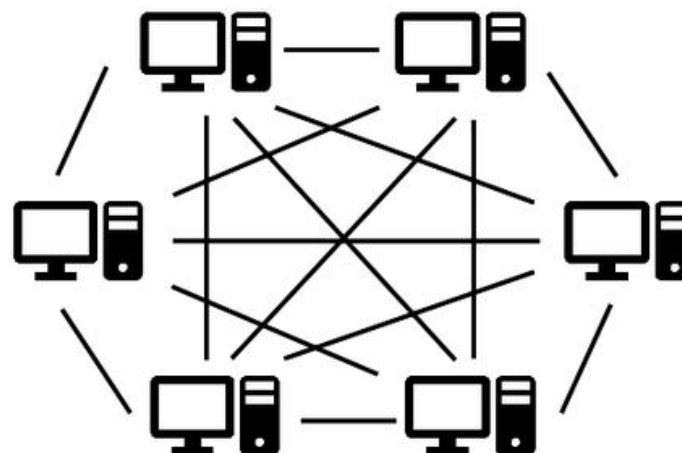
How Does the System Work

Decentralized peer-to-peer network:

- ❖ Peers have equal capabilities and authority without a central control
- ❖ Makes communication and sharing easier; anonymity



Client-Server network



P2P network

How Does the System Work

Public transaction ledger (the blockchain)

- ❖ Each block contains a set of transactions
- ❖ The network collaboratively adds and verifies blocks, and every node has equal access to the blockchain
- ❖ Can only add blocks, cannot delete a block
- ❖ Consider the longest chain the most secure



How Does the System Work

A set of rules

- ❖ Miners compete to solve a computational intensive puzzle to put their block on the blockchain
 - Miners use ASICs(Application-Specific Integrated Circuits) chips
- ❖ The blockchain contains a reward for the successful miner: 6.25 bitcoin
- ❖ New block every 10 minutes
- ❖ Forking - longest chain to be valid
- ❖ Transaction is verified by 6 blocks - considered irreversible

How Does the System Work

Proof-of-Work algorithm

- ❖ Bitcoin uses a PoW algorithm called SHA-256
- ❖ SHA-256 is deterministic, collision-resistant, irreversible
 - irreversible  rotate and shift operations
- ❖ Miners need to include block hash from the previous block, the Merkle root, timestamp, difficulty target, and a nonce
 - nonce - random number of 0's, require guess and check
- ❖ The most proof  the most safe



Advocations and Criticisms

Advocations and Criticisms

Advocations

- Revolutionizes remote transactions and enhances efficiency for global payments - no government interference
- Can be used by people with no bank accounts
 - e.g. El Salvador, 20% GDP rely on remittances, but 70% doesn't have bank account, 30-50% transaction cost
- Anonymity

Criticisms

- Need to find people willing to accept - if not, have to rely on an exchange with involved centralized financial institutions
- Difficulties in verifying daily transactions
 - El Salvador example - no merchants use Bitcoin; a block added each 10 min
- Scams and criminal activities
 - (Foley 2018) 46% of bitcoin has illegal activities

Some more criticisms

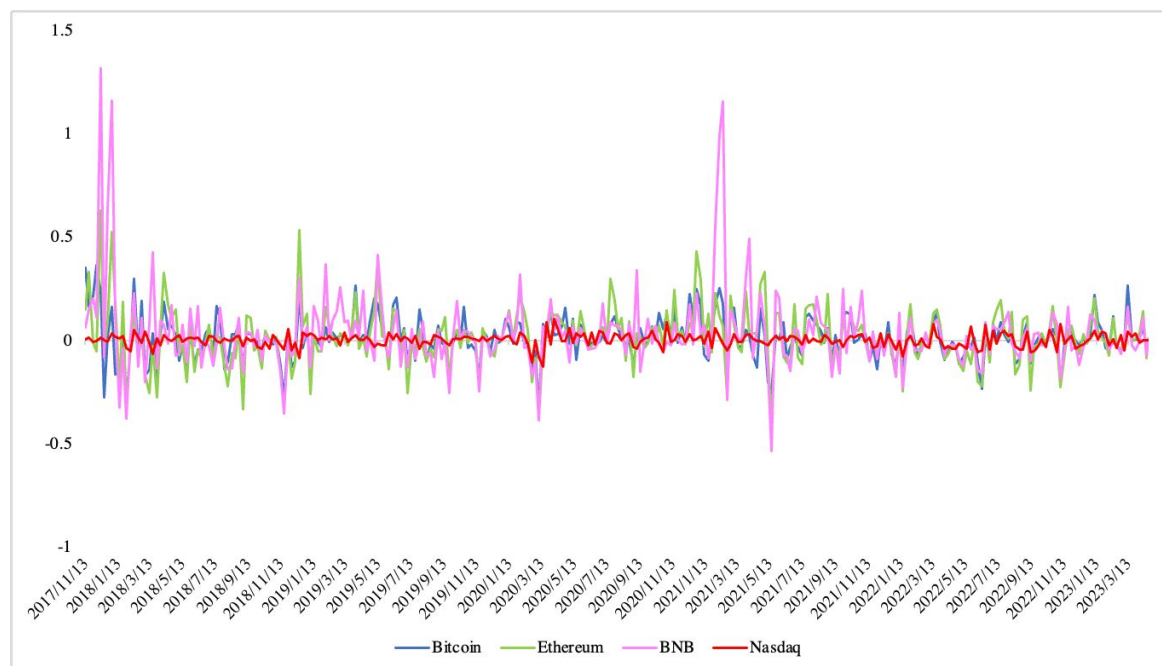
- No third party protection
 - ❖ Since only public key needed for transaction, receiver cannot block payment
 - ❖ Cannot revert transaction
 - ❖ Private key very long - once lost, cannot retrieve
- Potential of the system failing
 - ❖ Possibility of one individual (or a group) hacking the system
cost of computing power * number of blocks to be attacked ?= value of attack
(# ASICS * electricity cost)
- Can't be used in daily life like a fiat money
 - ❖ Medium of exchange: difficult to use in daily expenses (verification + commission)
 - ❖ Storage of value: too volatile to be a reliable storage medium



Crypto Valuation

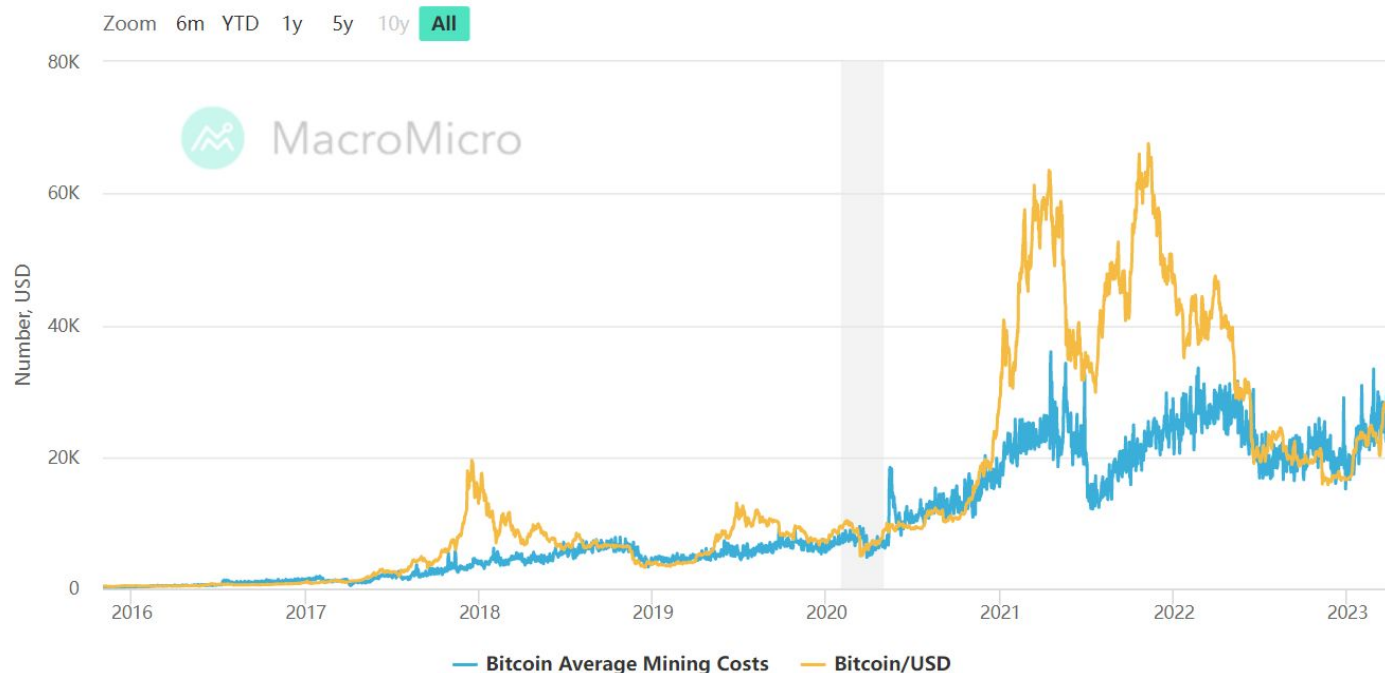
Crypto Valuation

- ❖ Significant price fluctuations compared to conventional financial instruments like stocks and bonds
- ❖ Shifting perceptions of market participants - the behavior, value, properties of cryptocurrencies
- ❖ Connection with economic activities - downturns, seek for safer assets and less favor cryptos



(Weekly Returns of Three Cryptos Verses that of Nasdaq Index)

Crypto Valuation



(reference: <https://en.macromicro.me/charts/29435/bitcoin-production-total-cost>)

- ❖ Fundamental valuation depends on mining costs - see the two converges
- ❖ (Take Bitcoin as an example) Only way to create Bitcoin is through mining - winning miner get mining rewards
 - mining cost: ASICs, power



The Cryptocurrency Crisis of 2022

The Cryptocurrency Crisis of 2022

Crypto Market: highly volatile, sharp fluctuations

February
2022

market start to price in the Fed Rate Hikes,
Bitcoin traded back at \$42,259 (once
peaked at \$67,802)

May
2022

the Fed increased benchmark interest rate
by 50 bps, speculative investments selloff

November
2022

the collapse of FTX crypto exchange
platform, largest crypto related bankruptcy



Subprime Lending Comparison

The Big Question:

- ❖ Can my counterparty pay up?
- ❖ A Brief Example (featuring options)

Liquidity Problems in Crypto

- ❖ FTX took investor crypto and deployed it elsewhere
 - Investors have trouble withdrawing funds
- ❖ Similarity to homeowners being unable to pay back loans

Speculative Decay

Fundamental Crypto Pricing

- ❖ Convergence of price and mining cost

Reasons for Buying an Asset:

- ❖ Rational: this is a necessary investment with solid fundamentals
- ❖ Irrational: this is only going to go up

Usage of Leverage

Bubbles:

- ❖ Low interest rates, high optimism, easy access to credit

Crypto Crash

- ❖ Cheap Robinhood margin trading

Subprime Crash

- ❖ 30-to-1 Lehman leverage

What does the Fed do?

- ❖ Use monetary policy to control inflation and unemployment
 - Expansionary
 - Contractionary
- ❖ Other tools
 - Open market operations
 - Reserve requirements
 - Discount rates

The Fed Intervenes

Crypto Crash

- ❖ Crypto is not legal tender
- ❖ Fed sees crypto as too risky

Subprime Crisis

- ❖ Lowered rates
 - ❖ Lended to banks
 - ❖ Purchased securities
-



Thank you!

