



Bitcoin

presented by Sam
GPI Fall 2020

The background is a solid blue color. In the top-right and bottom-left corners, there are decorative patterns of overlapping hexagons in various shades of blue and teal. Some hexagons are solid, while others are semi-transparent, creating a layered effect. Small white dots are scattered around the hexagonal clusters.

01

The Story

02

The Math


03

More Crypto



01

**The Story of a
Mystery Man**

The background is a solid blue color. In the corners, there are decorative patterns of overlapping hexagons in various shades of blue and teal, some with small white dots around them.

We have proposed a system for electronic transactions without relying on trust.

Satoshi Nakamoto

Why do we have banks? - Central Banks

- ❑ U.S. Federal Reserve (USD), European Central Bank (EUR)...
- ❑ Regulate money supply and financial stability
 - ❑ By monetary policies
- ❑ Represent trust in the currency
 - ❑ By the back of a government

Why do we have banks? - Commercial Banks

- ❑ JPMorgan Chase, Bank of America, Wells Fargo...
- ❑ Offer financial services such as lending and borrowing
- ❑ Provide means of electronic transactions

Who prevents bad things from happening?

- ❑ Scenario 1
- ❑ Tom buys ice-creams for the TAs
- ❑ Sam wants to pay Tom back
- ❑ But Sam has zero balance in his PNC account
- ❑ **PNC denies Sam's transfer request**

Who prevents bad things from happening?

- ❑ Scenario 2
- ❑ Tom takes the TAs to ice-cream shop
- ❑ Ice-cream shop only takes cash
- ❑ Sam wants to withdraw some cash from debit card
- ❑ But Sam still has zero balance in his PNC account
- ❑ **PNC denies Sam's withdraw at the ATM**

Who prevents bad things from happening?

- ❑ Scenario 3
- ❑ Tom takes the TAs to ice-cream shop
- ❑ Ice-cream shop only takes credit cards
- ❑ Sam's credit card has zero available limit left
- ❑ Card is denied at POS machine by issuing bank

Who prevents bad things from happening?

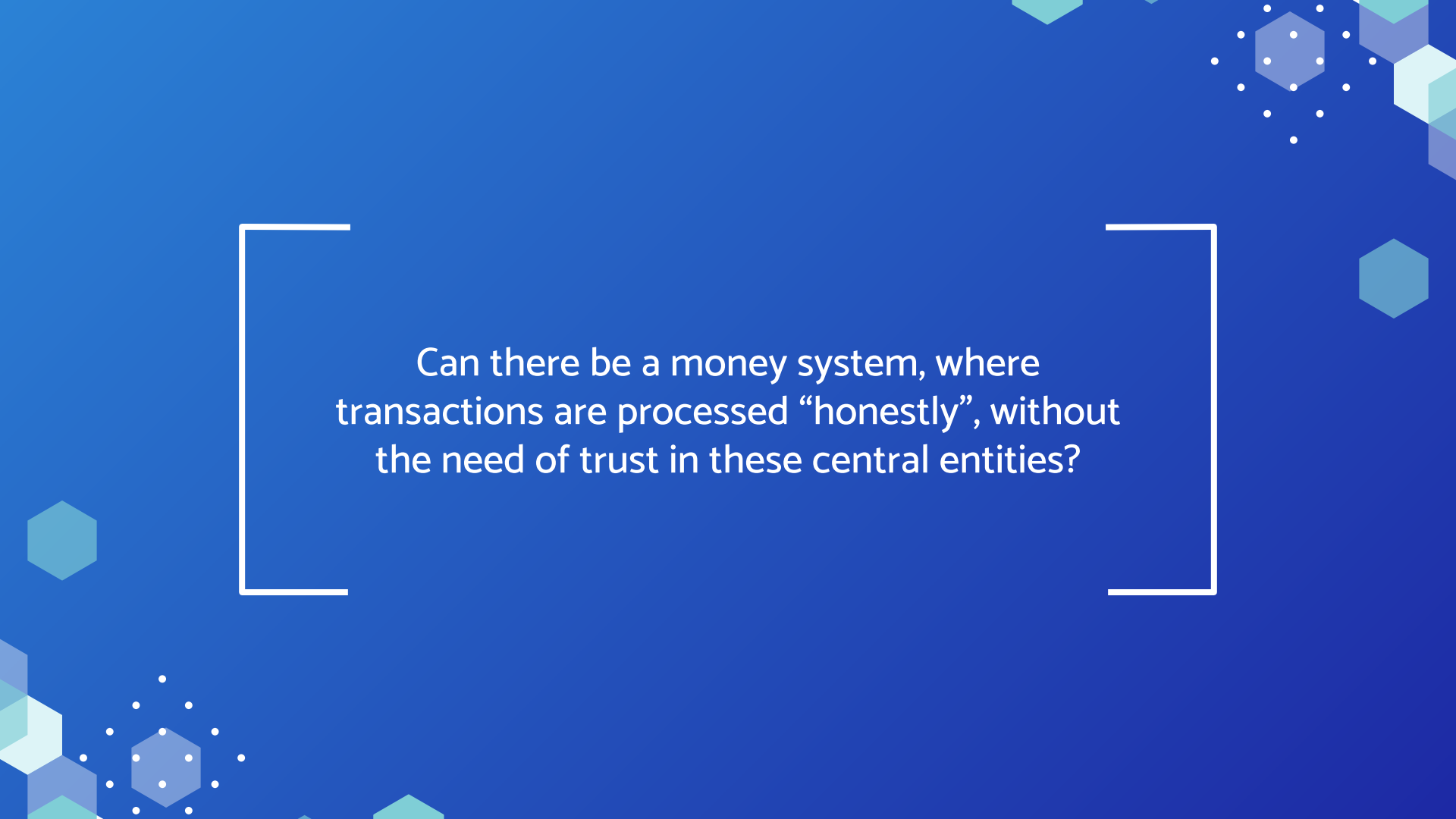
- ❑ Scenario 4
- ❑ The ice-cream shop is so good
- ❑ Sam goes there again and buys ice-cream with a PNC Visa credit card
- ❑ But the shop receives payments into their Chase account
- ❑ **Visa processes payment and routes money**

Who prevents bad things from happening?

- ❑ Scenario 5
- ❑ Sam travels to Europe and finds a good ice-cream shop
- ❑ But he spent all his euros buying macarons
- ❑ Luckily, the shop takes U.S. dollars
- ❑ **The U.S. government ensures value in dollars**

Lesson

- ❑ Many bad things can happen, but they don't
- ❑ Thanks to government, banks, payment processing companies
- ❑ Which all work together to prevent them



Can there be a money system, where transactions are processed “honestly”, without the need of trust in these central entities?

Core Ideas

- ❑ Bitcoin is a distributed digital ledger on a blockchain
- ❑ The ledger *is* the currency
- ❑ The ledger is a complete history of Bitcoin transactions ever made
- ❑ Transactions are verified with cryptography

The Ledger

- ❑ Distributedly stored on individual machines on the network
- ❑ As a blockchain - a chain of transaction blocks
- ❑ Each block contains some max number of transactions
- ❑ Each block “points” to the previous block (linked list)
- ❑ New transactions happen by being added to a new block.
- ❑ New blocks are added by “mining”

Mining

- ❑ Mining new blocks = verifying transactions in the blocks
- ❑ Anyone with computing power can be a miner
- ❑ A new block is only accepted with a **proof of work**
- ❑ Proof of work = generating a special hash
- ❑ This takes significant computing power to generate
- ❑ But easy to be verified by others

Mining Pools

- ❑ Initially, individuals have the computing power to mine
- ❑ Proof of work is designed to get harder and harder
- ❑ Mining pools aggregate computing power
- ❑ Then distribute results to all those contributed

Where do Bitcoins come from?

When a new block is created, a special transaction is included,
granting some Bitcoins to the miner responsible for generating the block

The miner can also select high fee transactions to include



Where do Bitcoins come from?

The mining reward by design decreases overtime, such that it halves every 210k blocks (roughly 4 years)

This means the introduction of new Bitcoins will eventually goes to zero!





02

**The Math that
replaces banks and
government**

Proof of Work

- ❑ Proof of work is how Bitcoin solves double-spending
- ❑ A new block is created with a special hash value
- ❑ The hash value must begin with some number of zeros
- ❑ The hash is computed by a cryptographic hash function
- ❑ Changing a single bit completely changes the hash
- ❑ Forging a series of blocks is exponentially hard



03

More Crypto

Other Cryptocurrencies

- ❑ Bitcoin Cash, Bitcoin SV
- ❑ Ethereum, Ethereum Classic
- ❑ Libre
- ❑ Litecoin
- ❑ Monero, Dash

Ethereum

- ❑ Blockchain is programmable
- ❑ Special languages such as Solidity
- ❑ Framework for creating Smart Contracts
- ❑ Programs run on “gas”

Other Applications of Blockchain

- ❑ Distributed storage
- ❑ Distributed applications (DApps)



THANKS

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.