PITCH DECK, BUILT FROM THE 2008 WHITEPAPER

Bitcoin: cash that moves without a middleman

A peer-to-peer electronic cash system. Payments go straight from one party to another, with no financial institution in between.

THE PROBLEM

Online payments run on costly trust

- Banks must mediate disputes, so no payment is truly final
- Mediation raises costs and kills small, casual payments
- Merchants ask customers for more data than they need
- A certain percentage of fraud is accepted as unavoidable

Cryptographic proof instead of trust

- Any two parties transact directly
- Transactions are computationally impractical to reverse, which protects sellers
- Routine escrow protects buyers
- A peer-to-peer timestamp server stops double-spending

HOW IT WORKS

Six steps run the whole network

1

New transactions are broadcast to all nodes

2

Each node collects them into a block

3

Each node works on a proof-of-work for its block

4

The winner broadcasts the block

5

Nodes accept it only if every transaction is valid

6

Nodes build the next block on top of it

An attacker falls behind fast

Attacker share of CPU	Blocks to wait for P < 0.1%
10%	5
15%	8
20%	11
25%	15
30%	24
35%	41

As long as honest nodes control most CPU power, the honest chain grows fastest and outpaces any attacker.

Incentives pay the network to stay honest

- The first transaction in each block creates a new coin for its creator
- That is how coins enter circulation, with no central issuer
- Later, transaction fees fund the work
- Once coins are issued, the system can be entirely inflation free

4.2 MB a year of headers

80 bytes x 6 x 24 x 365 = 4.2 MB

One block header is about 80 bytes. At one block every 10 minutes that is 4.2 MB a year, while 2008 computers shipped with 2 GB of RAM. Light clients verify payments with headers alone.

Public ledger, private people

- Every transaction is public, like a stock exchange tape
- Public keys stay anonymous, so no names are attached
- A new key pair for each transaction stops linking
- Privacy without a trusted third party

Hardware already outruns the ledger

- Storage grows about 1.2 GB per year (Moore's Law, 2008)
- Disk space is reclaimed with Merkle trees
- Nodes can leave and rejoin at will
- The network needs minimal structure

SUMMARY

Electronic transactions without relying on trust

Proof-of-work, an honest majority and simple incentives give anyone a payment network that no single party controls.