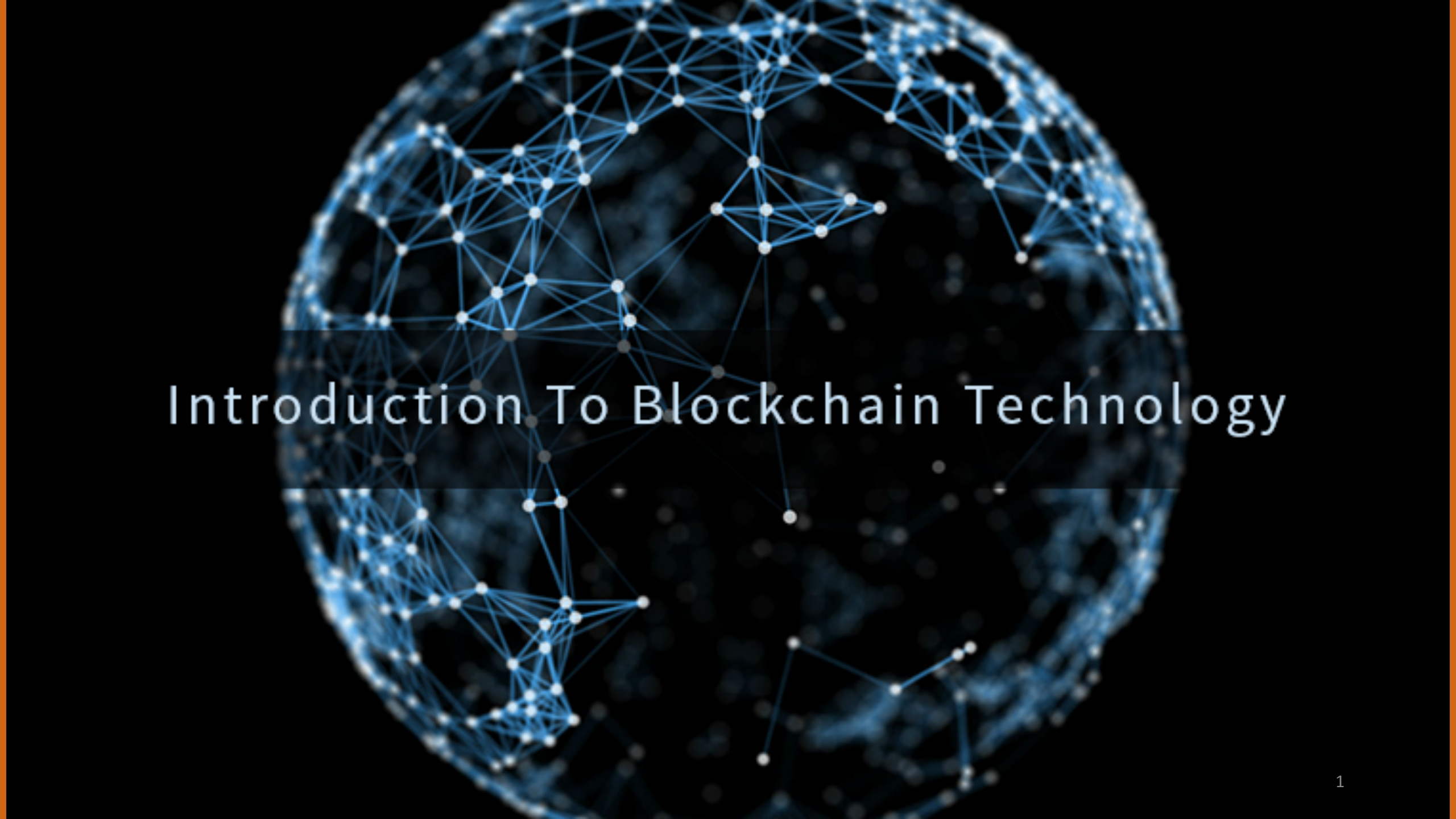


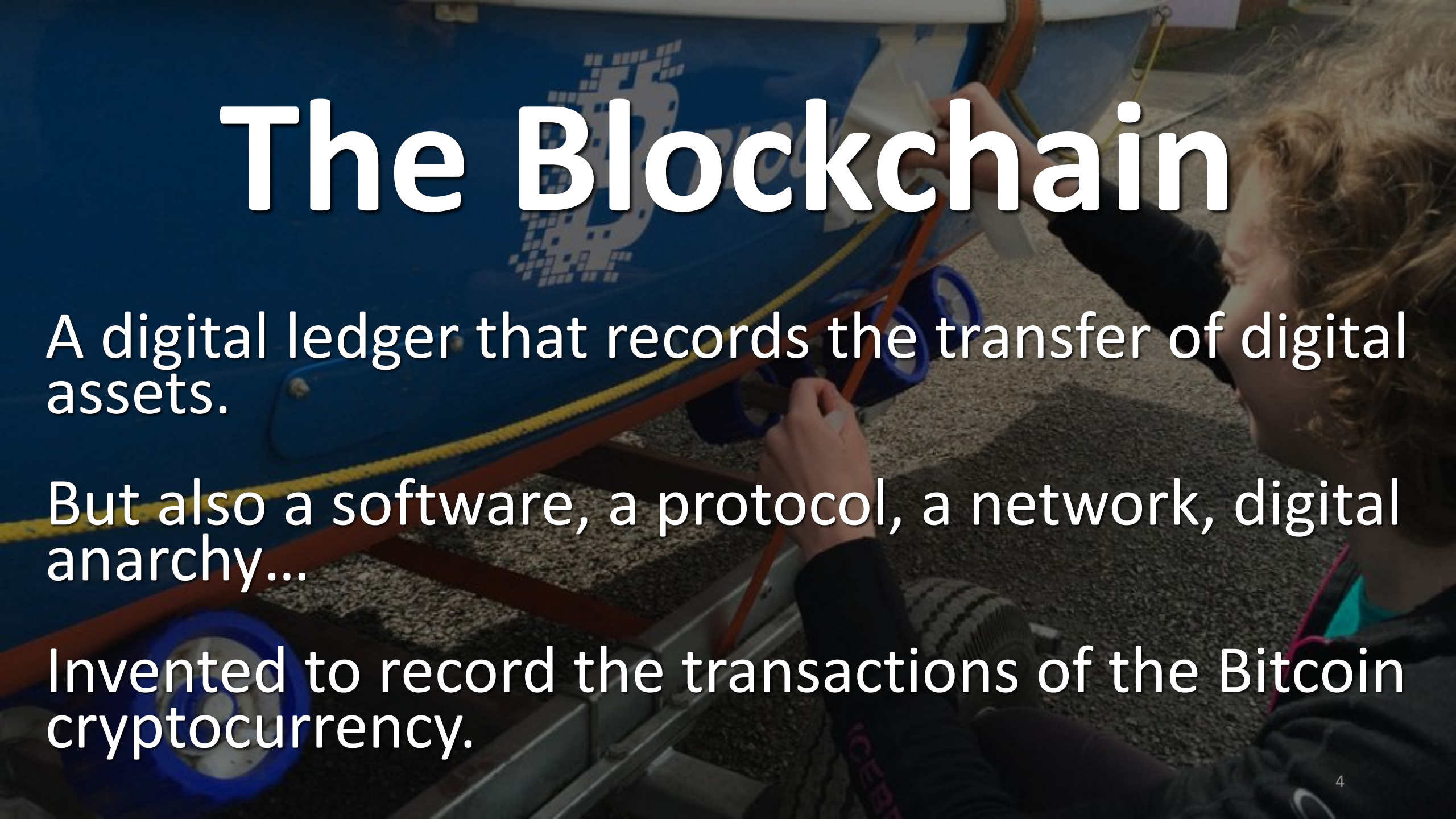
Introduction To Blockchain Technology

Martin Saint

Carnegie Mellon University
Africa College of Engineering

Overview

- What is the blockchain?
- How does it work?
- Why is there so much interest?
- Some example applications
- Implications of blockchain technology



The Blockchain

A digital ledger that records the transfer of digital assets.

But also a software, a protocol, a network, digital anarchy…

Invented to record the transactions of the Bitcoin cryptocurrency.

A Little History

Bitcoin and the blockchain were created in 2008 by Satoshi Nakamato

A Practical Example

- Alice wants to buy a Pycom from Bob over the Internet.
- Both have a Bitcoin wallet application on their smartphones.
- Alice sends the appropriate amount in Bitcoin to Bob's payment address.
- A distributed peer-to-peer network of computers running blockchain software verifies that Alice has the funds available, and transfers the correct amount to Bob.

Who Can You Trust?

“They say we’ll be your friends

We’ll stick with you till the end

Ah but everybody’s only

Looking out for themselves

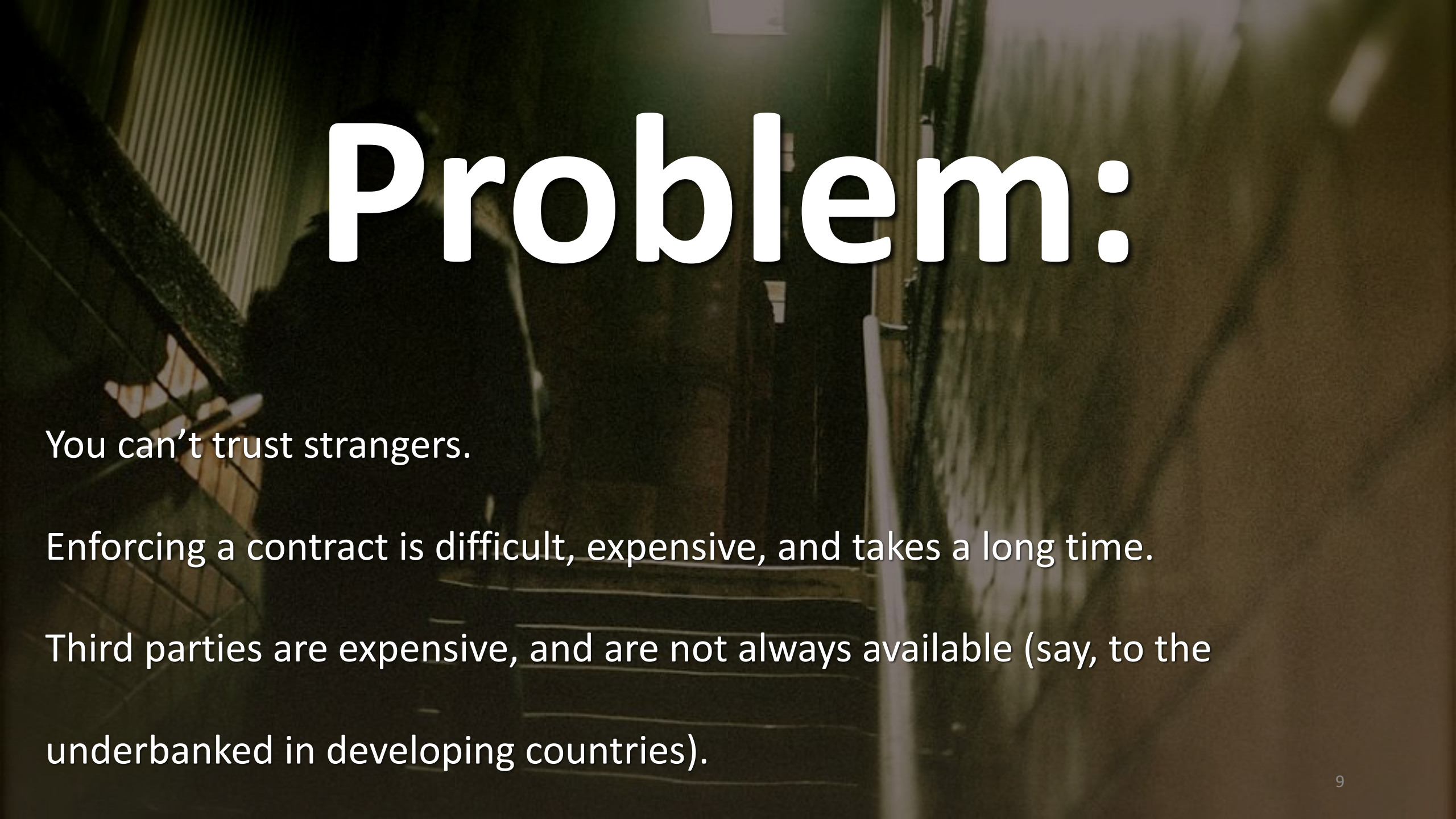
And you say well who can you trust…”

~ Cyndi Lauper - Money Changes Everything

Bringing Trust to Transactions, Traditionally

1. We can trust each other, maybe, if we meet in person and transact in common currency.
2. We can record our intentions in a contract that can be enforced through legal means if one party defaults.
3. We can involve a trusted third party, like PayPal or a credit card company to process the transaction.

In our example, Alice and Bob did none of these



Problem:

You can’t trust strangers.

Enforcing a contract is difficult, expensive, and takes a long time.

Third parties are expensive, and are not always available (say, to the underbanked in developing countries).

Trust Via Blockchain

Alice and Bob depended upon a distributed peer-to-peer network of computers running blockchain software to verify and enable the transaction.

Let’s Go A Little Deeper…

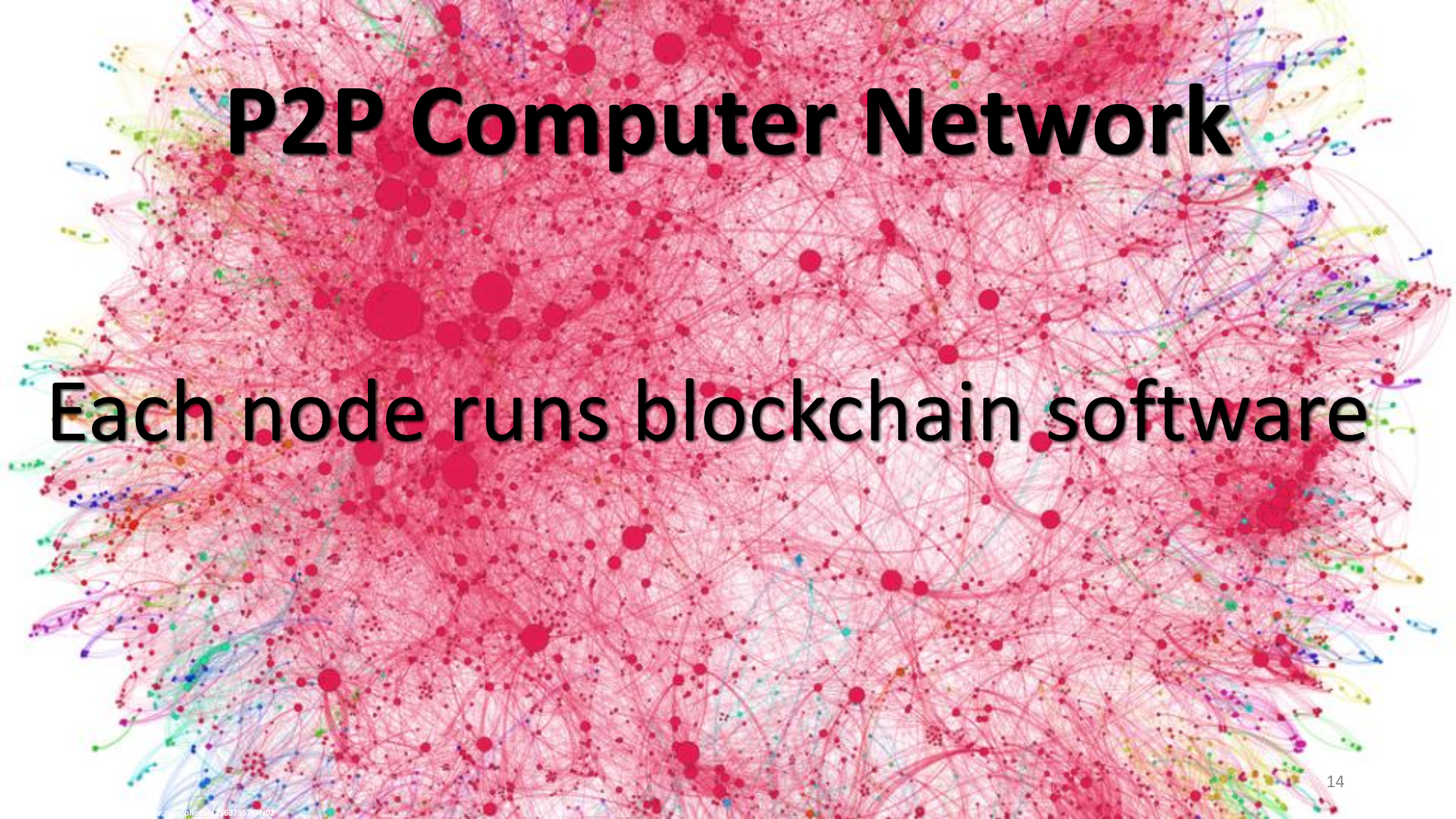
Three Technologies Underlying Blockchain

1. Private key cryptography
2. A distributed peer-to-peer network of computer nodes
3. Blockchain software

Private Key Cryptography

- public key + private key = digital identity
- Digital assets are sent to the public key address
- Unlocked with the private key

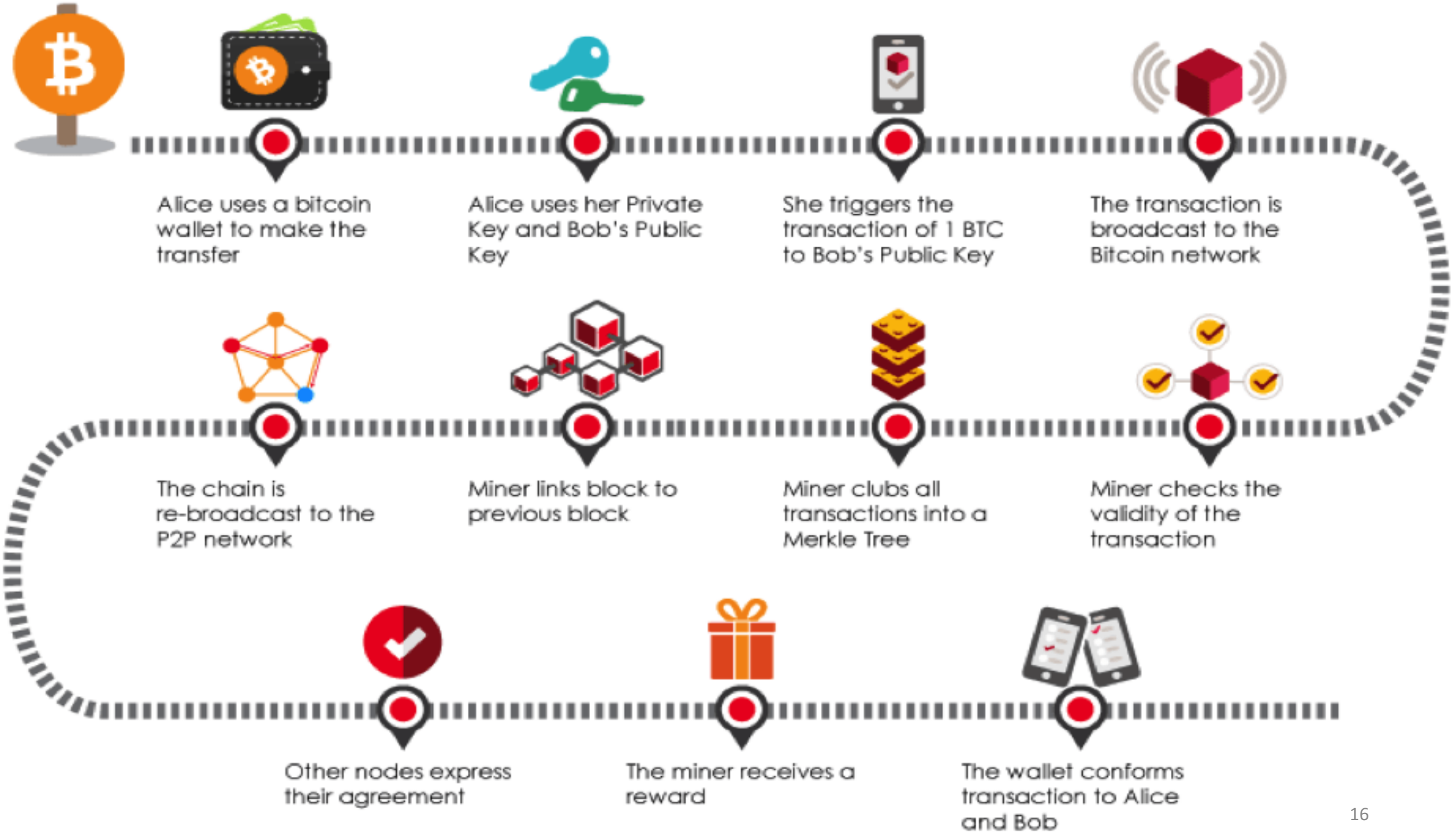
P2P Computer Network



Each node runs blockchain software

Blockchain Software

Verifies and permanently records each transaction


Alice uses a bitcoin wallet to make the transfer
Alice uses her Private Key and Bob's Public Key
She triggers the transaction of 1 BTC to Bob's Public Key
The transaction is broadcast to the Bitcoin network
Miner checks the validity of the transaction
Miner clubs all transactions into a Merkle Tree
Miner links block to previous block
The chain is re-broadcast to the P2P network
Other nodes express their agreement
The miner receives a reward
The wallet conforms transaction to Alice and Bob

More Details On Alice and Bob's Pycom Transaction

- Alice and Bob Agree on the Transaction
- Payments (or digital assets) are transferred to a public key address.
- Pseudonymous, but controlled by an individual via their private key.

Broadcast to the Blockchain Network

Each node holds a complete copy of all (Bitcoin) transaction since the beginning of time

Transaction is Validated

- Each computer node runs an algorithm to validate the transaction
- They also compete to be the first to solve a cryptographic puzzle that proves they have done the work to validate the transactions.
- The first node to solve the puzzle gets a reward.

Create a Block

- When the transaction is validated, it is combined with other transactions to create a "block" of data for the ledger.
- The process of verifying transactions, competing for the reward, and creating blocks is called "mining."

Add To The "Chain" of Previous Blocks

- The new block is added to the chain of blocks, thus it is called a blockchain.
- All nodes can check that the verification and posting process was done correctly.

Transaction Complete

The record of the transaction is permanent and cannot be altered.

Note that there was no trusted third party, only a network running blockchain software.

How is the Record Permanent?

The contents of each block, and the pointers to the previous blocks, are cryptographically hashed

What is a Hash?

A mathematical function that maps input data of arbitrary size (the message) to a fixed-size bit string output (the digest).

Properties of a Hash

- Deterministic: same message always results in the same hash
- Quick to compute
- Infeasible to generate a message from its hash value (not reversible)
- A small change to a message results in a completely uncorrelated digest
- Infeasible to find two different messages with the same hash value

A More Automated Transaction Example

- Imagine embedding computer code on the blockchain that acts as a “smart contract”
- Based upon a predetermined input (say, the first time a Pycom connects to the Internet)
- Contract logic could be checked and trigger an event (say, a payment from the chip vendor for intellectual property it has licensed)

So We Can Say The Blockchain Is

- A distributed, shared ledger
- A data structure (like a linked list with hashed pointers)
- A decentralized database
- A peer to peer network of decentralized computers
- A collection of software and protocols
- A trust layer for the web, and elsewhere

Why is there so much interest in the blockchain?

What The Blockchain Enables

- Time stamps
- A way to create and track digital assets
- Proof of ownership or rights (like intellectual property)
- Privacy, but also transparency
- Allows transactions to also contain rules for trust
- Self-executing, self-enforcing agreements
- Resistance to central points of failure, or censorship
- A way to conduct transactions without a trusted intermediary
- Decentralized services and governance

Potential Benefits

- Low cost
- Greater speed
- Trust and security
- Reliability
- Transparency
- Accuracy
- Permanent record
- Global
- Distributed/redundant
- Fault-tolerant/reliable
- No need for trusted intermediary or central authority
- Low barriers to use (device and Internet connection)
- Corruption resistance

Broad implications of the blockchain

- May eliminate a lot of intermediaries and intermediary services
- Will redefine how some processes operate
- Will require new regulatory and legal policies
- Will enable new services
- Will enable value to be created and transferred in new ways
- A way to bring trust to situations where it was previously not possible

Wallets
Software, Web & mobile wallets
Cold storage; multisig
Vaults

Financial Services
Bitcoin 'banking'
Remittances, money transfer & payments
ecommerce

Payments & Value Exchange
POS merchant & consumer services
Mobile payments
Peer-to-peer & distributed network integration

Exchanges
Trading, spot & forward exchanges
Stock exchanges
Currency exchanges & clearing houses
Interexchange - cryptoSWIFT

Trust & Verification
AML; KYC; verification; compliance; governance and risk management & regulation (of customers, merchants & service providers)
Consumer protection

The Blockchain & Big Data
Blockchain parsing & analysis
Internet of things, value exchange, smart contracts, databases & ledgers

Applications
Online gambling, gaming, betting & casinos
Social media integration
Mobile platform integration

Support Services
Recruiting, accounting, consulting, regulatory compliance & technical support
Security

News & Data Services
Pricing updates; aggregated info sources; trend analysis & news feeds

Mining
Rig manufacturers, distributors & users
Cloud & industrial mining pools
'Scrypt' mining

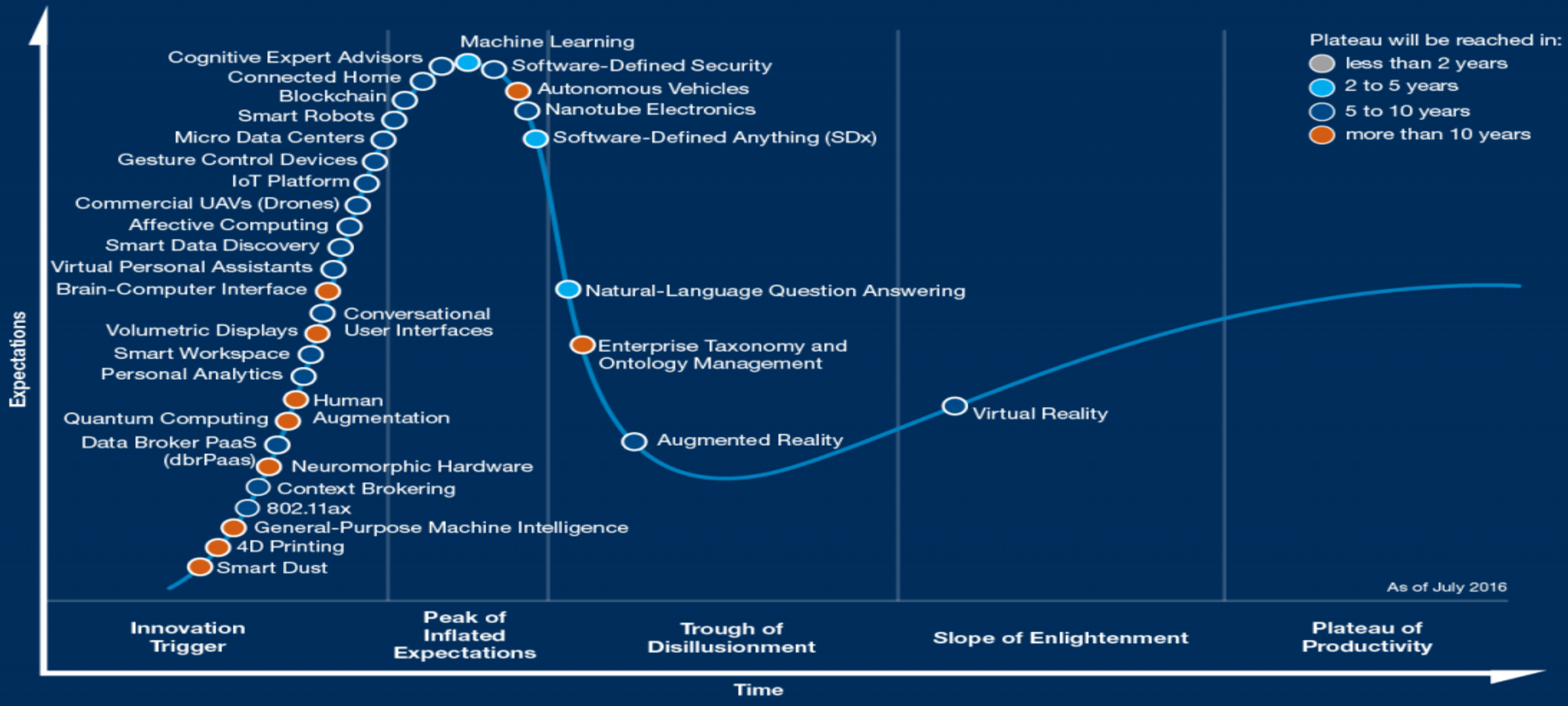
Infrastructure
Core & open source platforms
ATM's & POS
Peer-to-peer and distributed networks

Investments
ETFs &
Investment Trusts
Venture Capital
Crowdfunding

Unknowns

- Complex technology
- Challenges to implementation
- Regulatory implications
- Competing platforms
- Loss of control by governments and banks
- May enable new forms of crime and corruption

Gartner Hype Cycle for Emerging Technologies, 2016



Source: Gartner

Resource

The Princeton Bitcoin Book:

https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1

Martin Saint
msaint@andrew.cmu.edu

Carnegie Mellon University
http://www.cmu.edu/africa/