Trust at Scale

Exploring the power of decentralized consensus

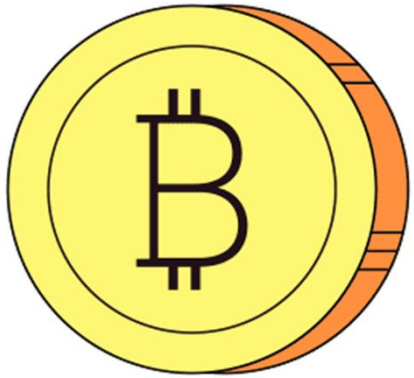
- What Blockchain is and is not
- Its applications and relevant industries
- Decentralized consensus
- Trust at scale
- Transferring trust from humans to computers

Hello!

I Am David Deborin

I try to combine software development and finance with a sprinkle of TRIZ

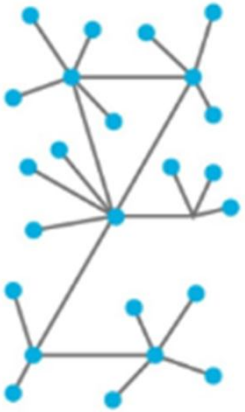
Blockchain ≠



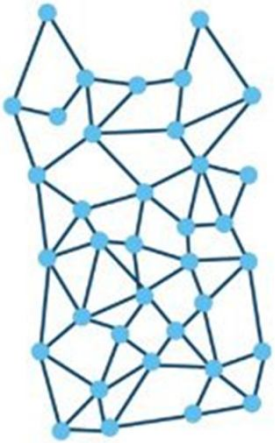
Key Terms

Centralized

Decentralized



Distributed

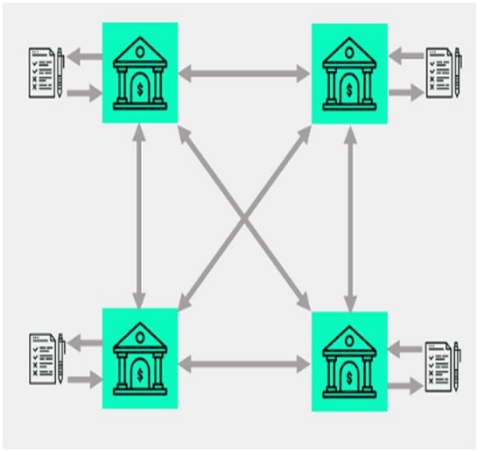


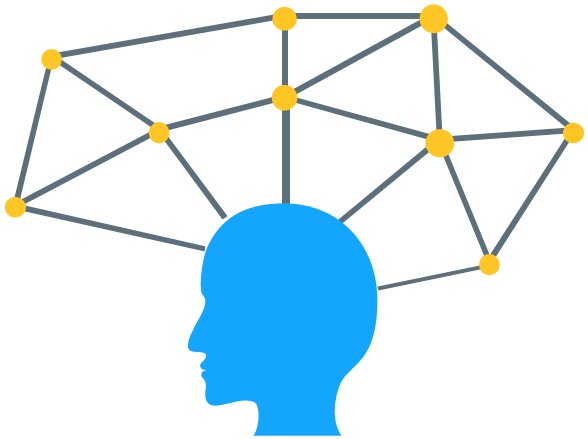
Key Terms

Immutable

Consensus

Distributed Ledger



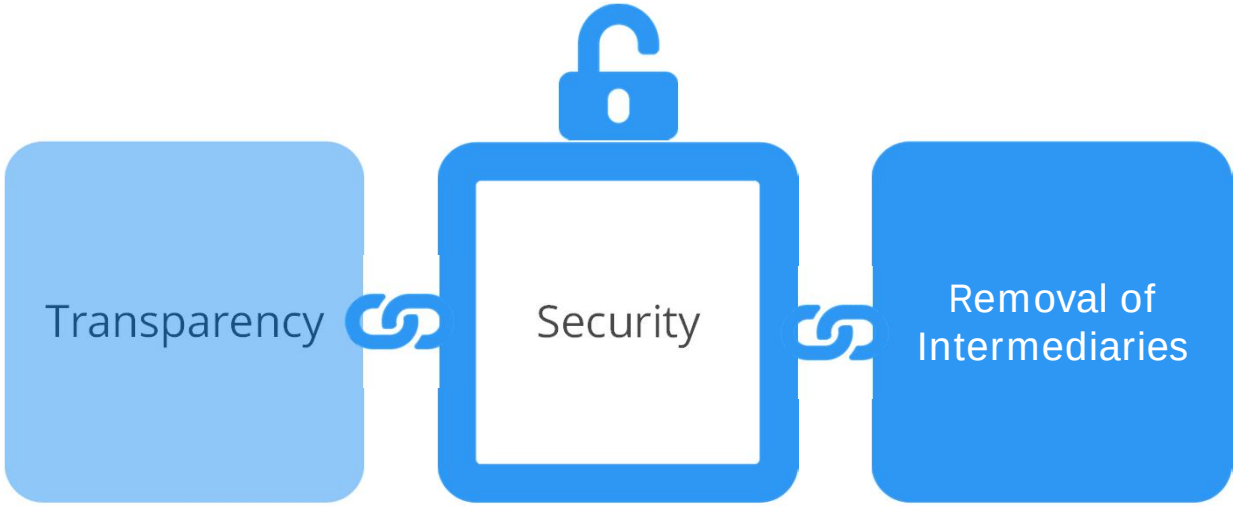


What is a Blockchain?

A chain of time-stamped, cryptographically secure, immutable blocks of consensus-validated digital data, existing in multiple synchronised, geographically distributed copies.

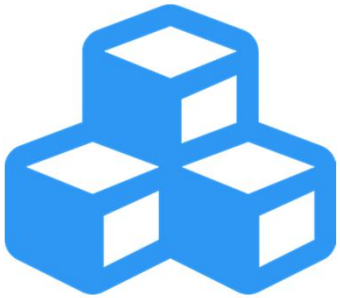
- Digital ledger
- Immutable
- **Decentralized**
- Cryptographically secure
- Distributed

Benefits of Blockchain



Transparency

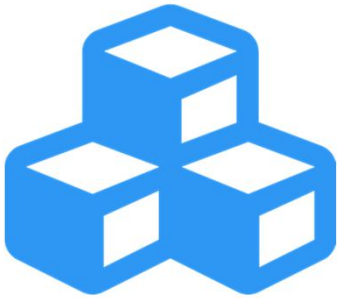
- Everyone has access to the data on the ledger
- Anyone can validate transactions or data
- Anyone can examine the Blockchain's history



Many cryptocurrencies, like the notorious Bitcoin, are open-source and strongly encourage contributions from the greater developer community.

Security

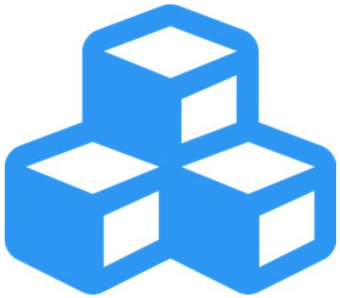
- The data is immutable
- No single point of failure or weakness
- Limitless number of copies or “backups”



Blockchain’s sole security vulnerability comes in the form of a 51% attack. A 51% attack is when a group of attackers control over 50% of the computing power and have the ability to tamper with new blocks.

Removal of Intermediaries

- Everyone has equal power to access & verify data
- Peer to Peer
- Reduces costs

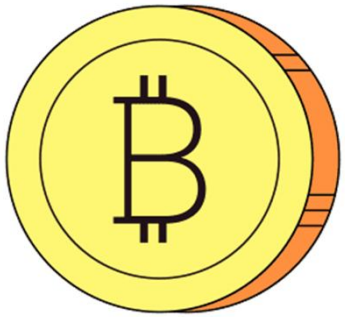


Participants in the Bitcoin network can send bitcoins, a form of digital currency, to each other quickly and cheaply without the need of a bank account.

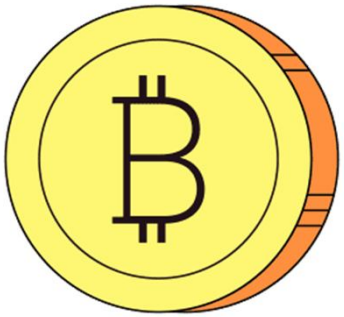
Summary

- Participants in a blockchain network are computers, NOT people
- Blockchain technology is made up of software/code
- Blockchain is an immutable, decentralized, and distributed ledger
- Main benefits are transparency, security, and removal of 3rd parties
- A solution to systems that lack trust

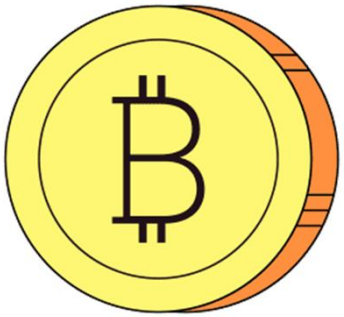
Global



Unbiased



Peer to Peer



Financial industry lacks trust

I send .0079 BTC to my friend my Michael

My bitcoin wallet address (public key)

Michael's bitcoin wallet address (public key)

3DREpgVRA8WaFJUXoVGC8NADL5hFNeEzYT (0.0079

3BqrTK4pDGLYsvunEUqufTu1erz7sDNASA

Hash values (Unique Identifiers)

Bitcoin Mining = Verifying Transactions

- Mining helps us reach consensus
- Miners are computers
- People setup and operate the computers
- Transactions are validated by code

Step 1: Verify that a group of transactions is valid

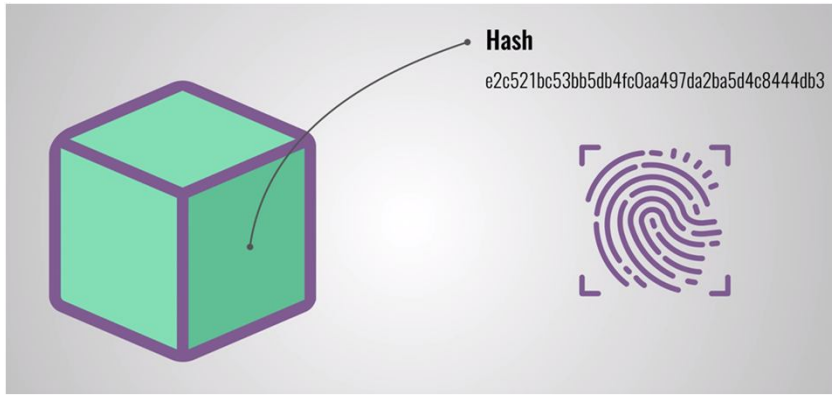
A.Our transaction is now in a pool of unconfirmed transactions

A.A miner will pick a group of unconfirmed transactions to verify

A.The Bitcoin protocol checks to see if the transactions are valid

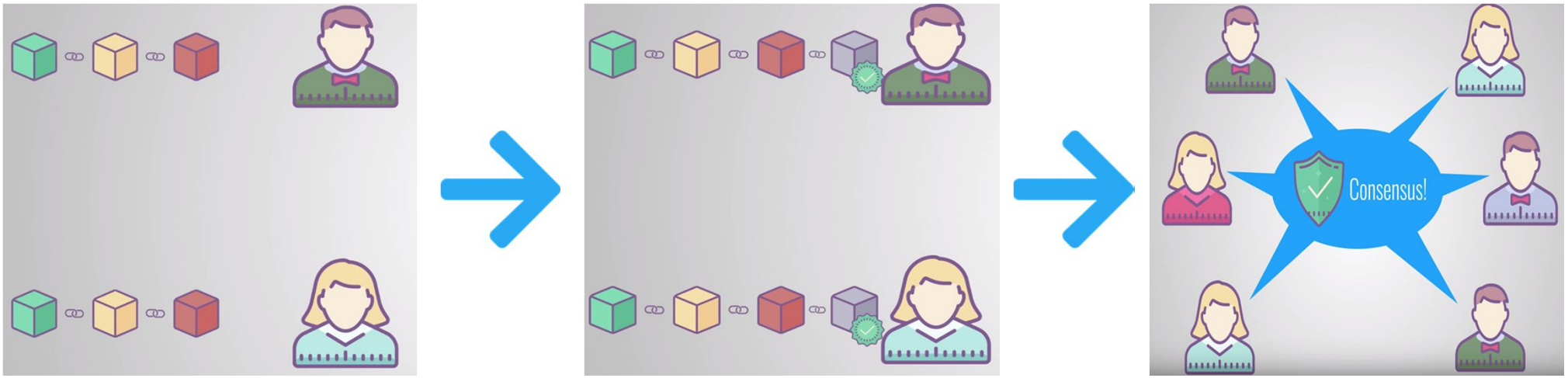
A.There are 20 rules each verification has to pass

Step 2: Solve a really hard math puzzle

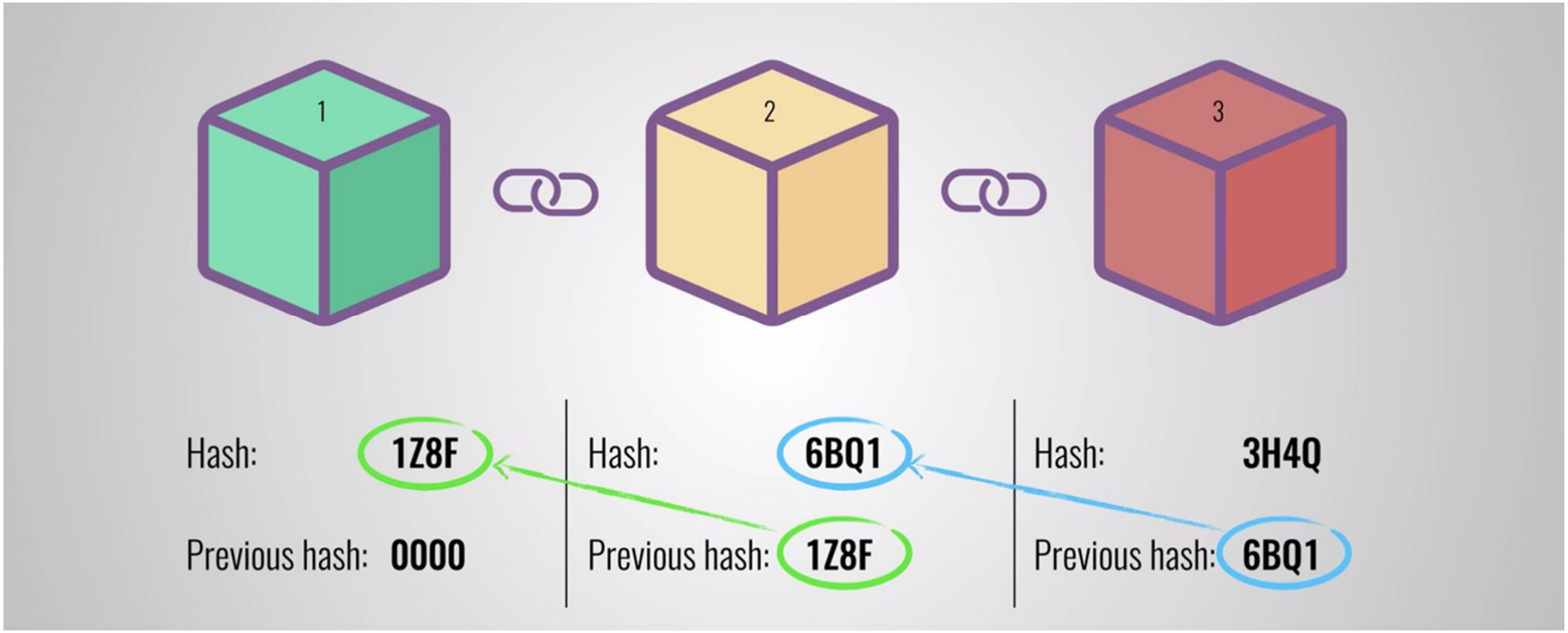


- Hash functions are deterministic
- The same input will always yield the same output
- A tiny change in input = huge change in output
- solution hash is very difficult to obtain, but easy to verify

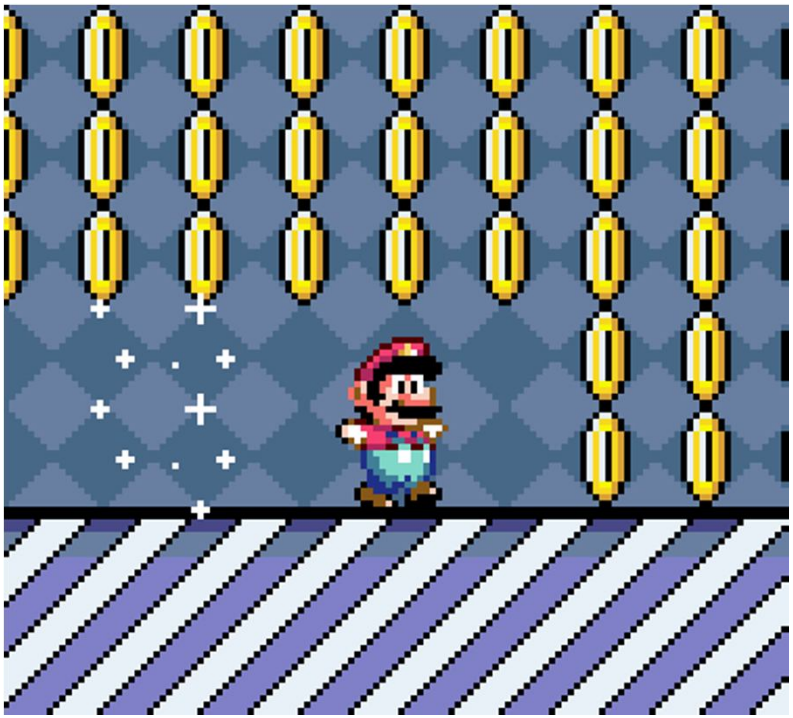
Step 3: Consensus



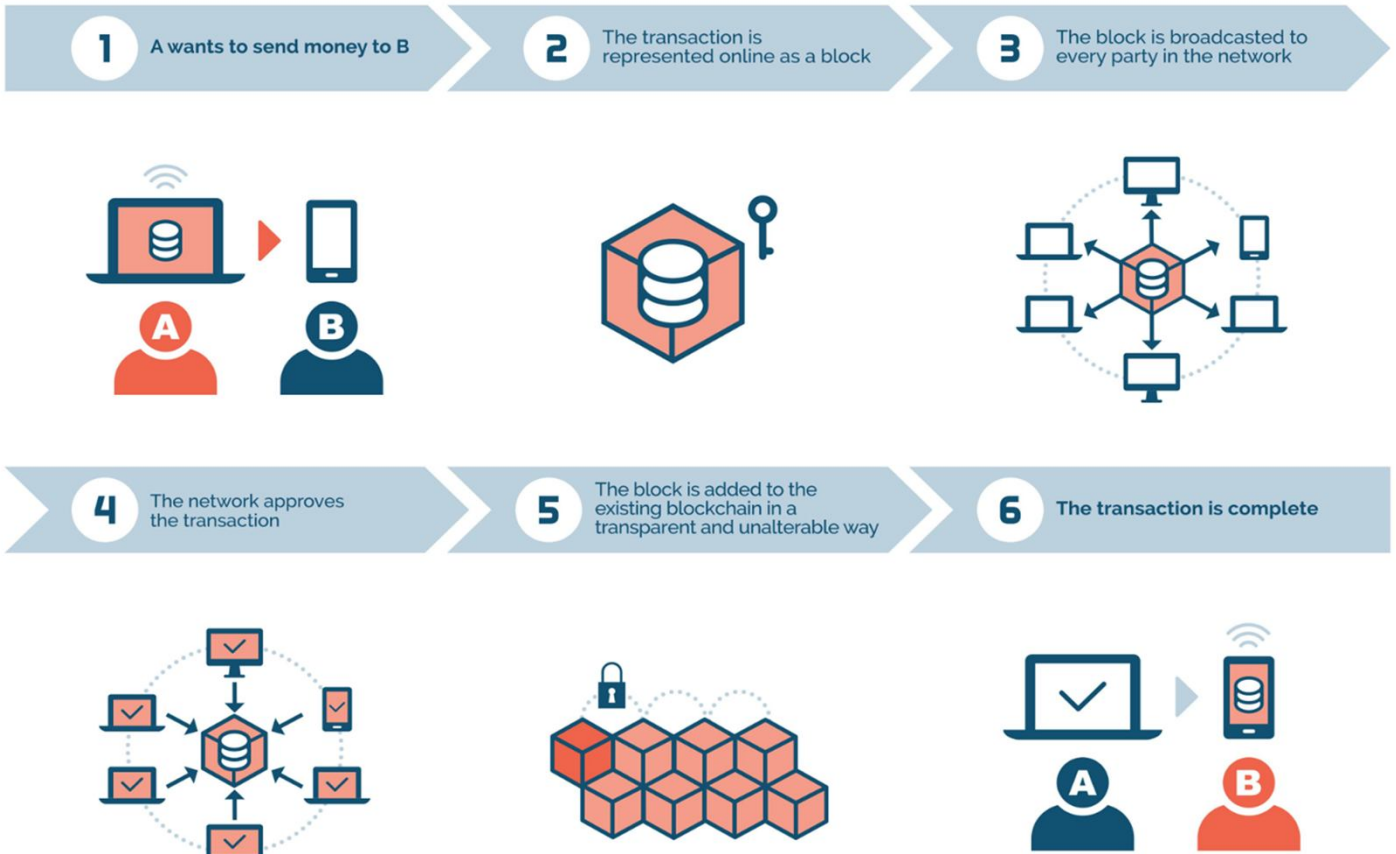
The Final Result



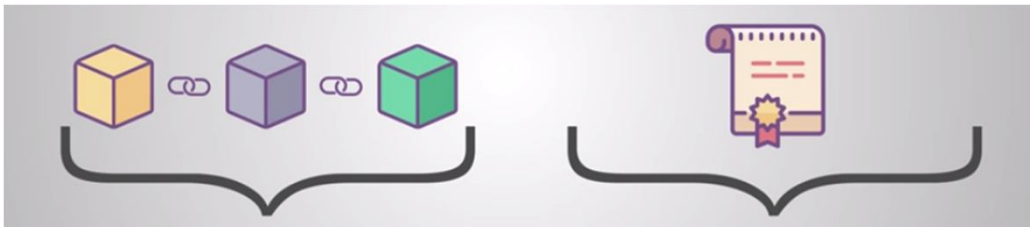
Step 4: Miners get rewarded



Bitcoin Blockchain Summary



Ethereum & Tokenized Solutions



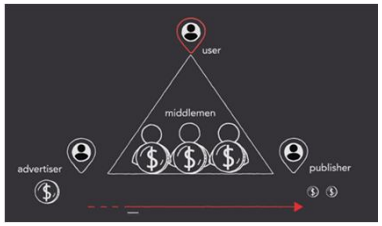
Blockchain

Smart contracts

Industry #1: Digital Advertising

PROBLEM

- Advertisers lose money from unidentified user attention (UA)
- Publishers don't get enough revenue
- Users don't trust fraudulent ads



SOLUTION

- Advertisers save money with transparent UA analytics
- Publishers will receive tokens based on UA
- Users can reward publishers with tokens

+ brave

Industry #2: Music

PROBLEM

- Unpaid royalties and lost revenue
- Illegal downloads and copies
- Copyright violations and theft

SOLUTION

- Instant and real-time monetization
- Transparent payments and purchases
- Transparent rights management

Internet of Things + Supply Chain

I want to track the journey a shipment of tomatoes has from France to Canada to the U.S.

We shouldn't need to trust the loader of the tomatoes to insert data on the blockchain.

Each block will contain the amount of boxes, weight, location, and time of each shipment.

These attributes should be obtained from internet-connected sensors.

Internet of Things Cont.

IOTA is based on a new distributed ledger, the Tangle, which introduces a new way of reaching consensus in a decentralized peer-to-peer system.

Secure. Scalable. Cheap.

Other applications

Audit trails
Accounting
Criminal activity

Voting

Smart property
Car odometers

Healthcare
You have the private key to a publicly accessible blockchain storing medical records. No hassle when switching doctors

Looking to the future

Blockchain was simply our first way to create decentralized consensus

Are high scale decentralized systems possible to achieve?

What systems severely lack trust?

Thanks!

David Deborin

LinkedIn: David Deborin

Gmail: daviddeborin@gmail.com

Friend me on Facebook!