Paycase

Blockchain 101:
Presented by: Michael Young, CTO and Game Master

What Paycase Does:

Why
Responsible Finance for Everyone

How
Social banking that enables the movement of money using non-traditional cash settlement mechanisms

What
Universal mobile banking (Apple IOS and Android), transparent money transmittance, same day settlement, global last mile delivery

Outline for the Exercise:

An overview of what a Blockchain is:

- Blockchain is a social construct
- Types of Blockchains
- Building blocks of a blockchain
- Secrets of a blockchain

Simulating a Blockchain:

- Volunteers
- Balloons, Boxes and complicated tape.

Blockchain is a social Construct: *It's behavioral*

- Blockchain is an immutable public or private information system where the participants post information and verify one another's activities
- Verification and changes to the construct (system) are done by group consensus
- Participants identity can be private or public, depending on the scheme
- Uses technologies over a decade old and even older

Just how old is the underlying technology?

- Encryption by cipher and secret codes - 1900BC, Egypt
- Polyalphabetic encryption, Arabs 800AD, Europe mid 1400s
- Modern mathematical Symmetric encryption by shared key algorithms, mid 1800s to today.
- Asymmetric public key encryption that blockchain depends, draft standard in 1975.
- Elliptical Curve cryptography 1985
- Hashcash, a proof of work scheme used originally for preventing email denial of service and spamming, 1997 (Adam Back)
- Early 2000's CPU power became cheap enough to support this on an average computer.

Types of Blockchain and what information we can put in them:

- Open Ledger (this is Bitcoin)
- Contracts that are static and interactive between parties (Ethereum)
    - **Inventories of long lived assets (deeds, certificates of ownership)**
    - **Identity / Registries (birth certificates, driver's licenses, etc.)**
    - **Long lived Supply chain items such as plane parts, drugs, designer products, etc.**
- Potentially Internet of Things, but diminishing returns on low value items, not all data is all that valuable. Remember data is cheap to store, but not cheap to secure.

This information can be public or private or a mixture of each.

Blockchain is not the same thing as Bitcoin!

- Bitcoin has its own structure to incite participants to behave cooperatively, it uses a type of of Blockchain.
- It’s an open ledger for a cryptocurrency
- Some participants are paid in that cryptocurrency
- There is a competitive mechanism in the scheme that makes some participants (Miners) use large amount of computing power
- The main goal of Bitcoin is to issue and move Bitcoin amounts around participants without allowing ANY PARTICIPANT to double-spend any given Bitcoin entry
- Bitcoin is actually terrible for the environment

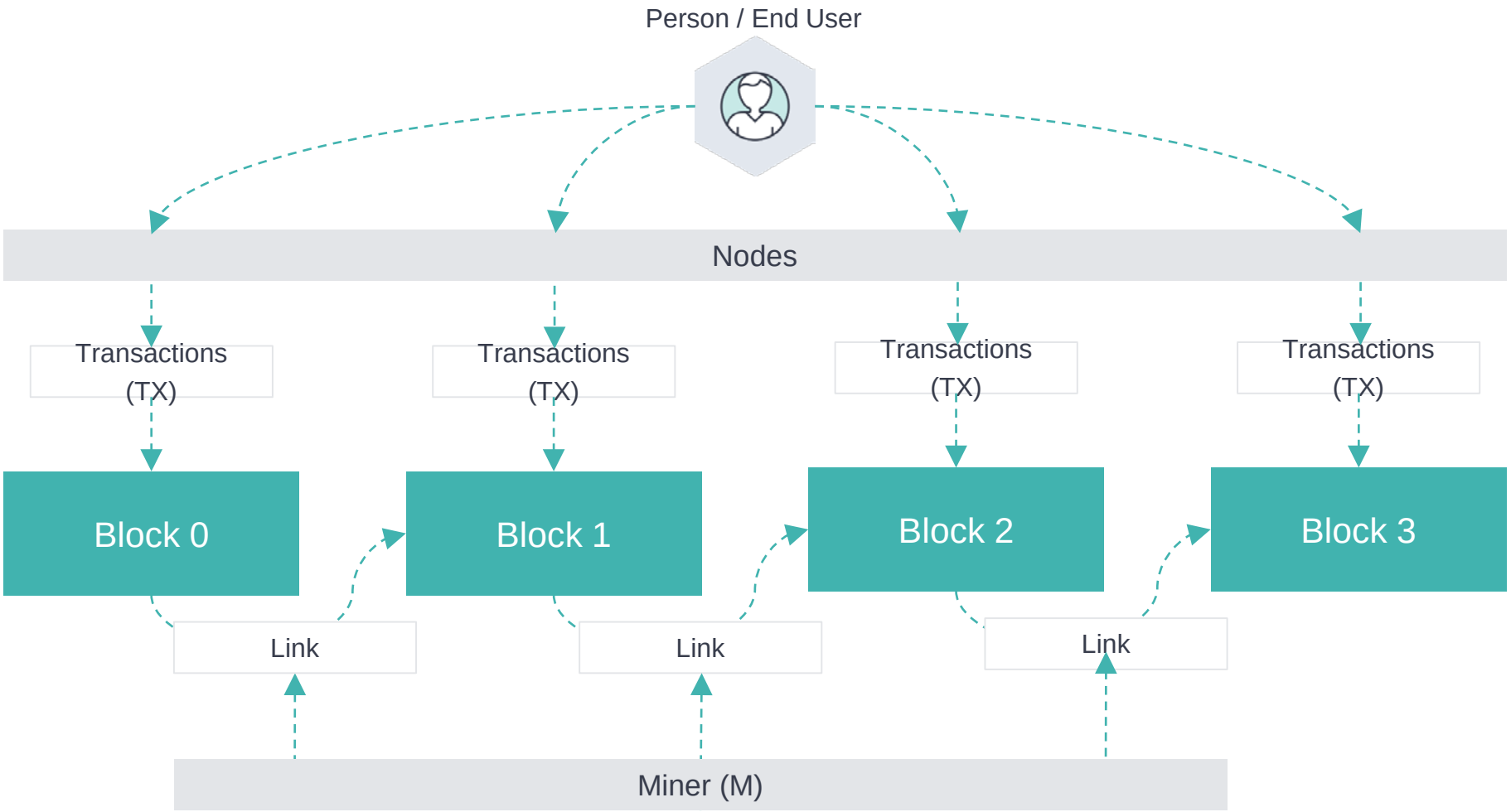
Blockchains can be completely co-operative and not incite large competitive uses of computing power.

Perimeter Security:

- Our important Data sits in systems/databases managed by trusted entities such as banks.
- What happens when that broad system gets compromised?
- How can blockchain be used to solve different types of secure data problems?

Building Blocks of the Bitcoin Chain:

- **Components:**
  - **Transactions**: credit only posted entries to the Blockchain
  - **Blocks**: Groups of transactions packaged together into an object (like a settlement period but approximately every 250 transactions and about 10 minutes between settlements).
  - **Node**: Operating software instance of the Blockchain, there are a few thousand running – these nodes are “the Blockchain”
- **Participants**
  - **End Users**: People/entities submitting transactions
  - **Node Operators**: People/entities operating a gateway for transactions to the Blockchain
  - **Miners**: People/entities validating groups of transactions into a “block” and linking each new block to the previous block


Person / End User
Nodes
Transactions (TX)
Transactions (TX)
Transactions (TX)
Transactions (TX)
Block 0
Block 1
Block 2
Block 3
Link
Link
Link
Miner (M)

Consensus versus Incentive:

Public:

- Bitcoin, and any public blockchain has to incite the Miners creating the blocks and verifying the transactions to do through be being rewarded. They compete for the reward by racing to solve a cryptographic puzzle, they check each other's work to make sure no one got the reward for invalid work – balance at work.

Private:

- Private blockchains miners are incentivized through other means, and so they are not competing and can approve a new block through consensus – imagine a group of 200 banks sharing the work of a blockchain that contains data relevant to that group of banks.
- Blockchain transactions can be verified and approved through independent 3rd parties in combination with the regular participants.

Block One Transactions:

- Michael has a balance of 100 Coins.
- Justin has a balance of 100 Coins.
- Nick has a balance of 100 Coins.

Block Two Transactions:

- Michael gives Justin 20 Coins.
- Justin gives Nick 40 Coins.
- Nick gives Michael 10 Coins.

Block Three Transactions:

- Michael gives Nick 20 coins
- Nick gives Justin 30 coins
- Justin gives Nick 10 coins

Block Four Transactions:

- Nick gives Michael 60 coins
- Michael gives Justin 10 coins
- Justin gives Nick 30 coins

Block Five Transactions:

- Michael gives Nick 30 coins
- Nick gives Justin 50 coins

Block Six Transactions:

- Nick gives Michael 100 coins

Our Final Balance:

Block	Michael	Justin	Nick	Total
1	100	100	100	300
2	90	80	130	300
3	70	100	130	300
4	120	80	100	300
5	90	130	80	300
6				0

Block 6 Transaction rejected - insufficient funds!

Blockchain 101 Concluded:

Thanks Everyone, here's more reading for you!

https://bitcoin.org/en/how-it-works

https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it

You can reach me at michael@paycase.com

Michael Young