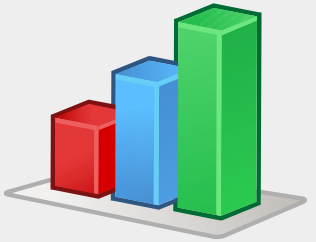
KATZ Club Crypto Primer

A Little About Me

- Software Engineer @ Microsoft in Pittsburgh
- Run https://chaintuts.com creating Bitcoin & blockchain related tutorials
- Here today with Rebecca White and Laura Taylor, founders of Blockchain in the Burgh!
  - Rebecca is an avid Litecoin fan and adoption enthusiast
  - Laura is a teacher and works with the DigiByte Awareness Team

A Poll...

- How many of you have heard of?
  - Bitcoin
  - Cryptocurrency: ETH, DGB, LTC, etc.
  - Blockchain
- How many of you have owned some?
- How many of you have used your own wallet or made a crypto purchase?



Some Crypto Basics

- What is a cryptocurrency?
  - Form of *peer-to-peer* digital cash
  - Money implemented as a computer protocol, rather than a government or corporate policy
  - Independent currency, not just a payment network like PayPal
  - Have some unique, useful problem-solving properties

Crypto’s Unique Properties

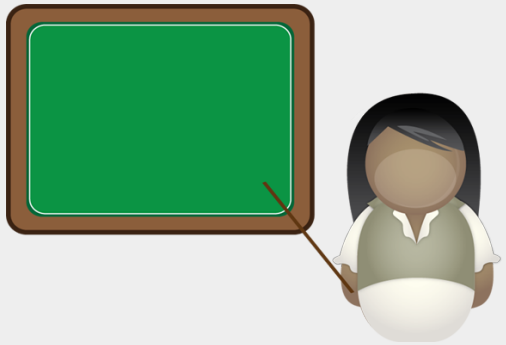
- Cryptocurrencies are *decentralized*
- Are *censorship resistant*
- *Are Global, peer-to-peer*
- These are the major *public* blockchains like Bitcoin, Ethereum, DigitByte
  - But there are other uses for private chains, etc.

Decentralized

- What is decentralization?
  - No gov’t or corporation controls Bitcoin
  - Instead, built on a network of people running open source software (individuals, miners, businesses)
  - Protocol is an agreed upon set of rules implemented in software
    - Transaction processing
    - Issuing currency
    - Etc.

Censorship Resistant

- Thanks to decentralization, we have censorship resistance
  - No central processing authority can freeze funds or stop transactions
  - Use of the network is *permission-less*
    - Exchanges, etc. have KYC/AML laws
    - The network itself has nothing – if you have bitcoin you can send it anywhere, anytime



Global & Peer-to-Peer

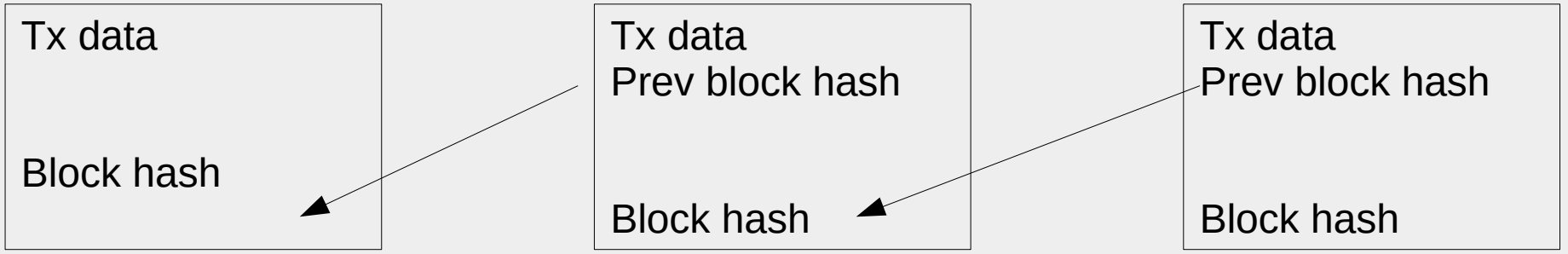
- This network is for everyone, everywhere!
  - Network operates 24/7/365
  - Operates without any concept of borders, whitelists, etc.
  - Simply people running a peer-to-peer software implementation – send directly to anyone, anywhere, anytime!

How Do We Get There?

- These amazing properties are by design – the system is built to be decentralized, peer-to-peer, and unstoppable!
  - Uses a proof-of-work blockchain for distributed consensus
  - Uses digital signatures to prove ownership securely

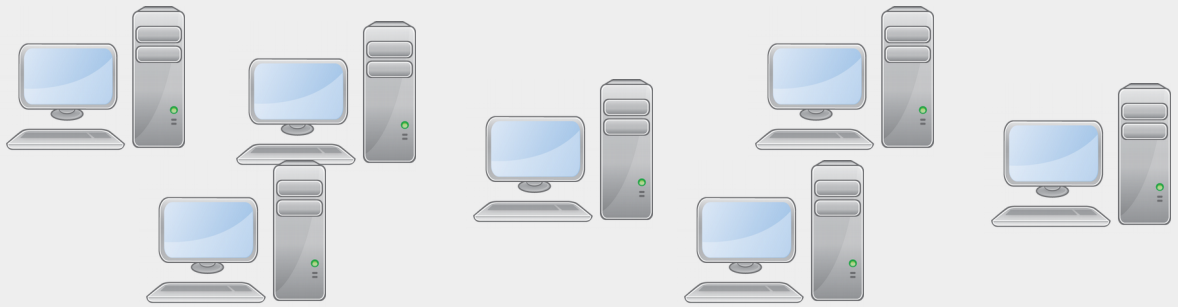
Blockchain

- A public record/ledger of all transactions (transfers) that have occurred
- A new “block” of transactions is batch processed every *N* minutes (chain dependent)
- Each block contains a link to previous block



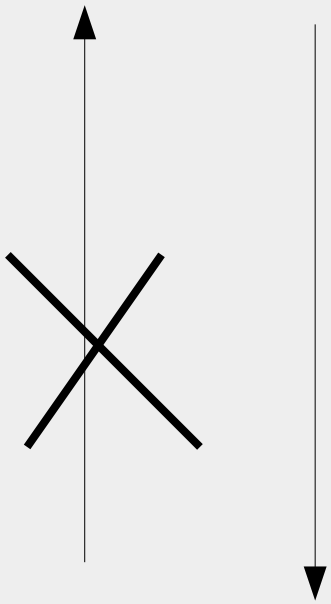
Proof-of-Work

- For a new block to be processed “mined”, must answer a hard guessing problem
- Uses a *lot* of electricity and computing power
- Once the problem is solved, anyone can verify the answer instantly (hence: “Proof-of-work”)
- Linking to previous blocks increases security of historical transactions



Digital Signatures

0x12351bc143badf2348fe38e8f8b785b...



One Way Algorithm
(Privkey to Address)

Anyone can verify you own a privkey given a *signature* and *pubkey*

NO revealing privkey!

PRIVATE KEY

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

PUBLIC KEY and ADDRESS

Will this be on the test???

- A little lost on the technical details?
  - DON’T FRET!
  - It’s important to know why cryptocurrencies have these amazing properties, not know all the details
  - Know what you need to know for *your use cases*

Use Cases

- Some discussion between myself, Rebecca, and LT...let’s chat!
- Some ideas to get started
  - Small business payments (@jonnylitecoin)
  - Global commerce and blockchain apps (DigiByte, DigiID)
  - Empowering individuals with *secure* digital money

Use Cases

- Some ideas to get started
  - Big business: frictionless settlement between institutions
  - Reduced costs for fraud (everything securely stored on chain, no storing private customer info)
  - Supply chain, healthcare, law...

Questions?

KATZ Club Crypto Primer

A Little About Me

- Software Engineer @ Microsoft in Pittsburgh
- Run https://chaintuts.com creating Bitcoin & blockchain related tutorials
- Here today with Rebecca White and Laura Taylor, founders of Blockchain in the Burgh!
  - Rebecca is an avid Litecoin fan and adoption enthusiast
  - Laura is a teacher and works with the DigiByte Awareness Team

A Poll...

- How many of you have heard of?
  - Bitcoin
  - Cryptocurrency: ETH, DGB, LTC, etc.
  - Blockchain
- How many of you have owned some?
- How many of you have used your own wallet or made a crypto purchase?

Some Crypto Basics

- What is a cryptocurrency?
  - Form of *peer-to-peer* digital cash
  - Money implemented as a computer protocol, rather than a government or corporate policy
  - Independent currency, not just a payment network like PayPal
  - Have some unique, useful problem-solving properties

Crypto’s Unique Properties

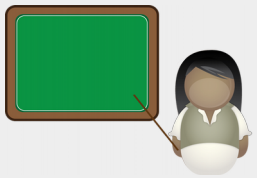
- Cryptocurrencies are *decentralized*
- Are *censorship resistant*
- *Are Global, peer-to-peer*
- These are the major *public* blockchains like Bitcoin, Ethereum, DigitByte
  - But there are other uses for private chains, etc.

Decentralized

- What is decentralization?
  - No gov’t or corporation controls Bitcoin
  - Instead, built on a network of people running open source software (individuals, miners, businesses)
  - Protocol is an agreed upon set of rules implemented in software
    - Transaction processing
    - Issuing currency
    - Etc.

Censorship Resistant

- Thanks to decentralization, we have censorship resistance
  - No central processing authority can freeze funds or stop transactions
  - Use of the network is *permission-less*
    - Exchanges, etc. have KYC/AML laws
    - The network itself has nothing – if you have bitcoin you can send it anywhere, anytime



Global & Peer-to-Peer

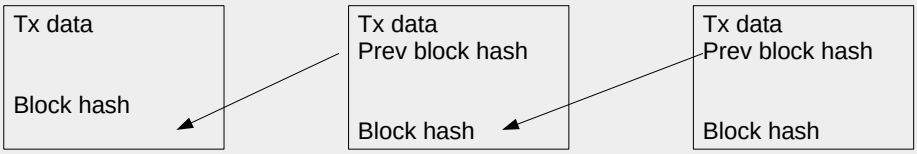
- This network is for everyone, everywhere!
  - Network operates 24/7/365
  - Operates without any concept of borders, whitelists, etc.
  - Simply people running a peer-to-peer software implementation – send directly to anyone, anywhere, anytime!

How Do We Get There?

- These amazing properties are by design – the system is built to be decentralized, peer-to-peer, and unstoppable!
  - Uses a proof-of-work blockchain for distributed consensus
  - Uses digital signatures to prove ownership securely

Blockchain

- A public record/ledger of all transactions (transfers) that have occurred
- A new “block” of transactions is batch processed every *N* minutes (chain dependent)
- Each block contains a link to previous block



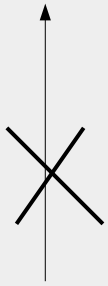
Proof-of-Work

- For a new block to be processed “mined”, must answer a hard guessing problem
- Uses a *lot* of electricity and computing power
- Once the problem is solved, anyone can verify the answer instantly (hence: “Proof-of-work”)
- Linking to previous blocks increases security of historical transactions

Digital Signatures

0x12351bc143badf2348fe38e8f8b785b...

PRIVATE KEY



One Way Algorithm
(Privkey to Address)

Anyone can verify you own a privkey given a *signature* and *pubkey*

NO revealing privkey!

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

PUBLIC KEY and ADDRESS

Will this be on the test???

- A little lost on the technical details?
  - DON’T FRET!
  - It’s important to know why cryptocurrencies have these amazing properties, not know all the details
  - Know what you need to know for *your use cases*

Use Cases

- Some discussion between myself, Rebecca, and LT...let’s chat!
- Some ideas to get started
  - Small business payments (@jonnylitecoin)
  - Global commerce and blockchain apps (DigiByte, DigiID)
  - Empowering individuals with *secure* digital money

Use Cases

- Some ideas to get started
  - Big business: frictionless settlement between institutions
  - Reduced costs for fraud (everything securely stored on chain, no storing private customer info)
  - Supply chain, healthcare, law...

Questions?