Blockchain™

or: How I Learned to Stop Worrying and Love the Bubble

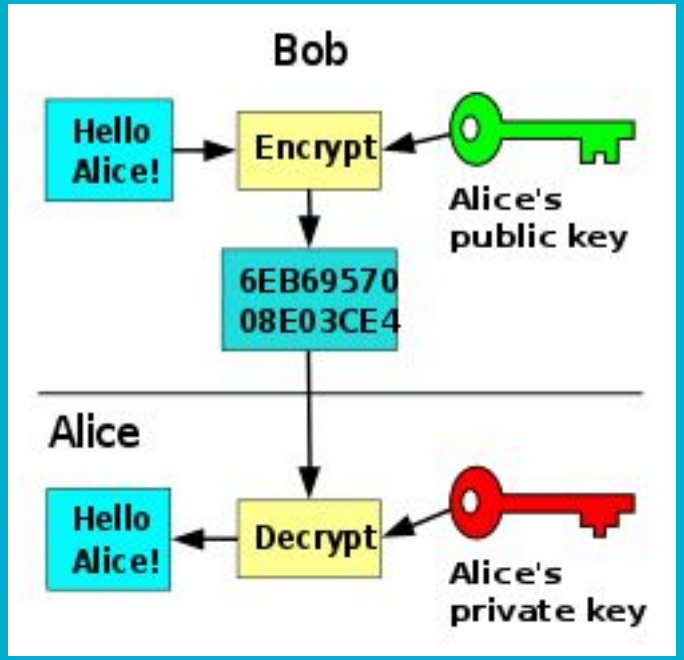
—

Claudia Richoux

29 January 2018, Asynchronous Anonymous

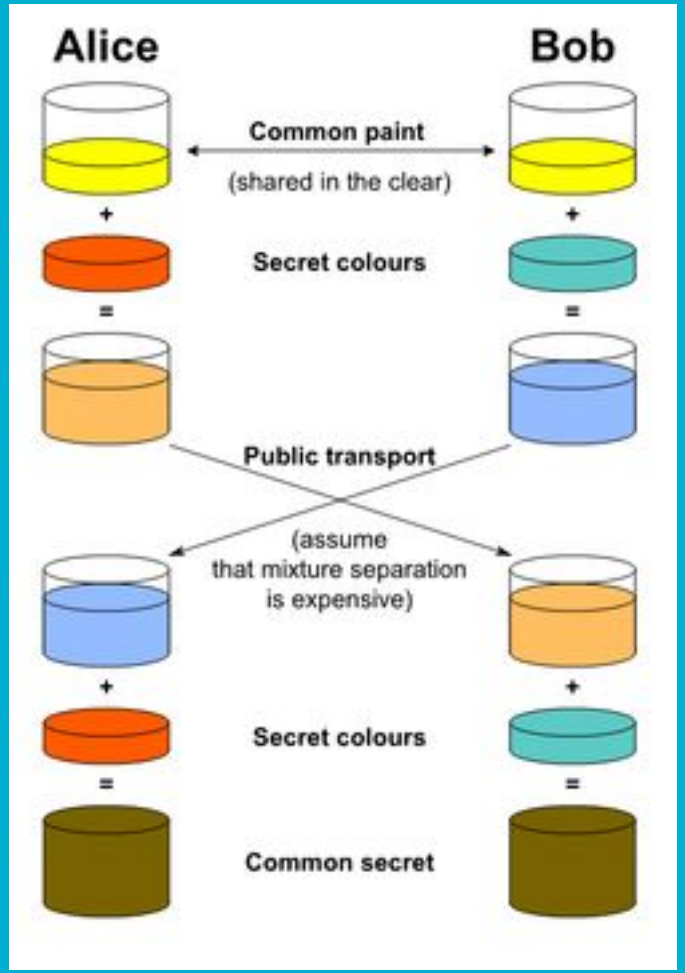
Cryptographic Background/History

Public-Key Cryptography



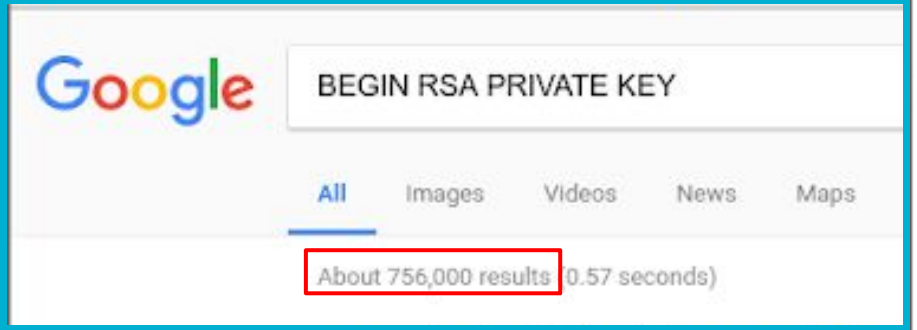
Diffie-Hellman Key Exchange

RSA (or other schemes)

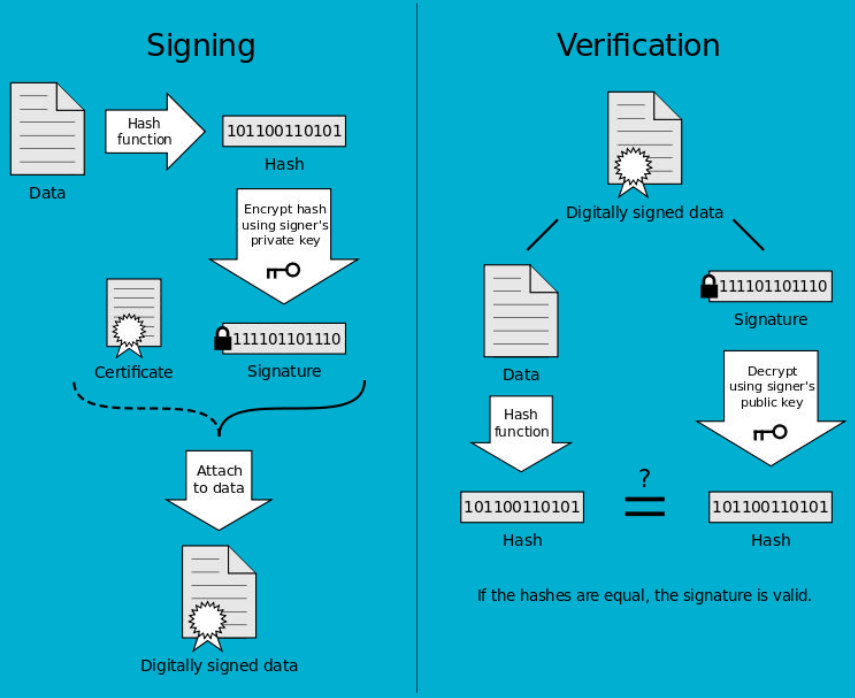


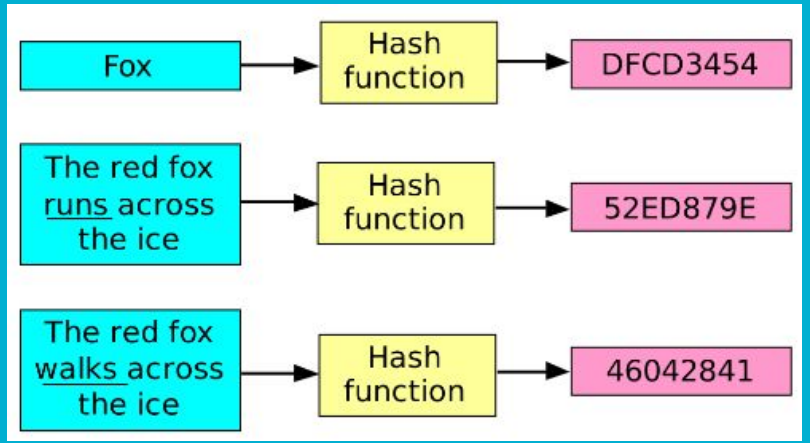
Crypto 101 Intermission

- Private Keys Are Private
- Public Keys Are Public
- Generate them on your own computer, then keep them safe!



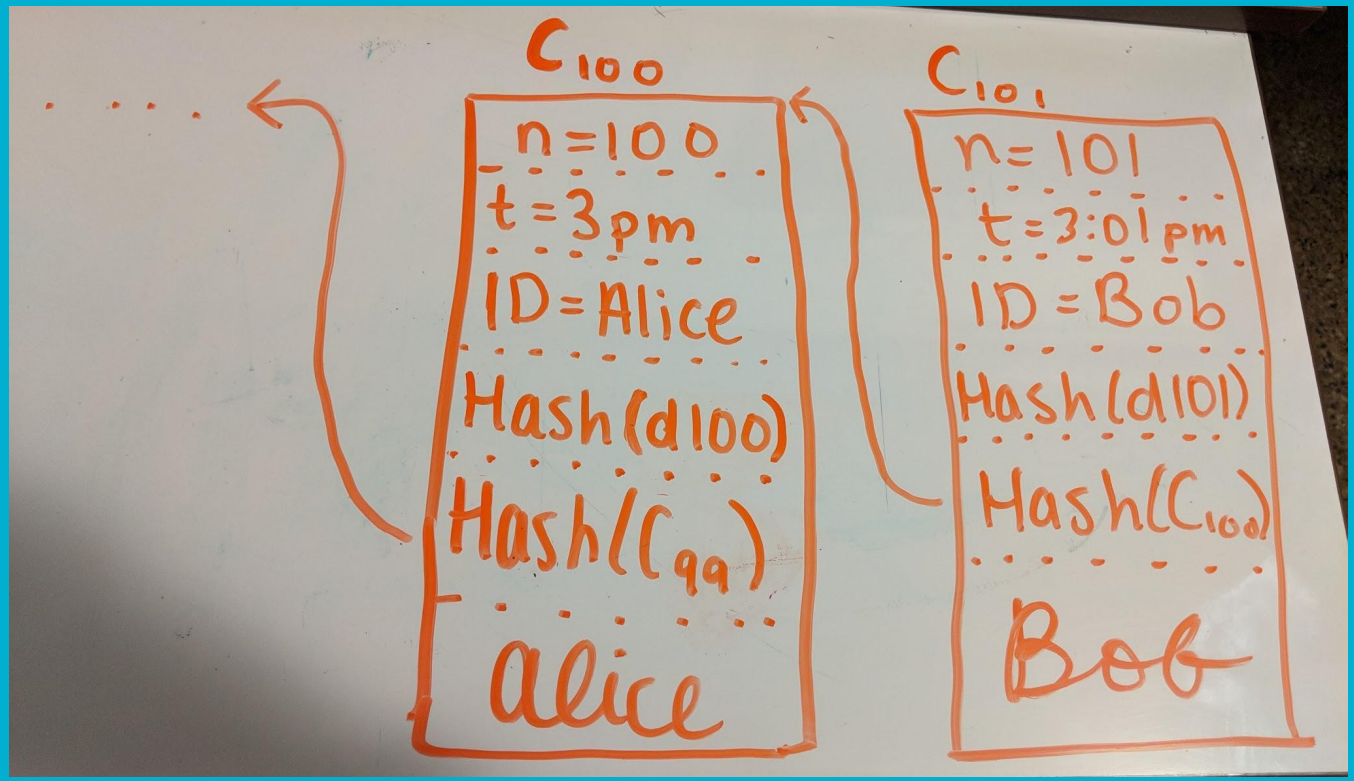
Basic Cryptographic Operations



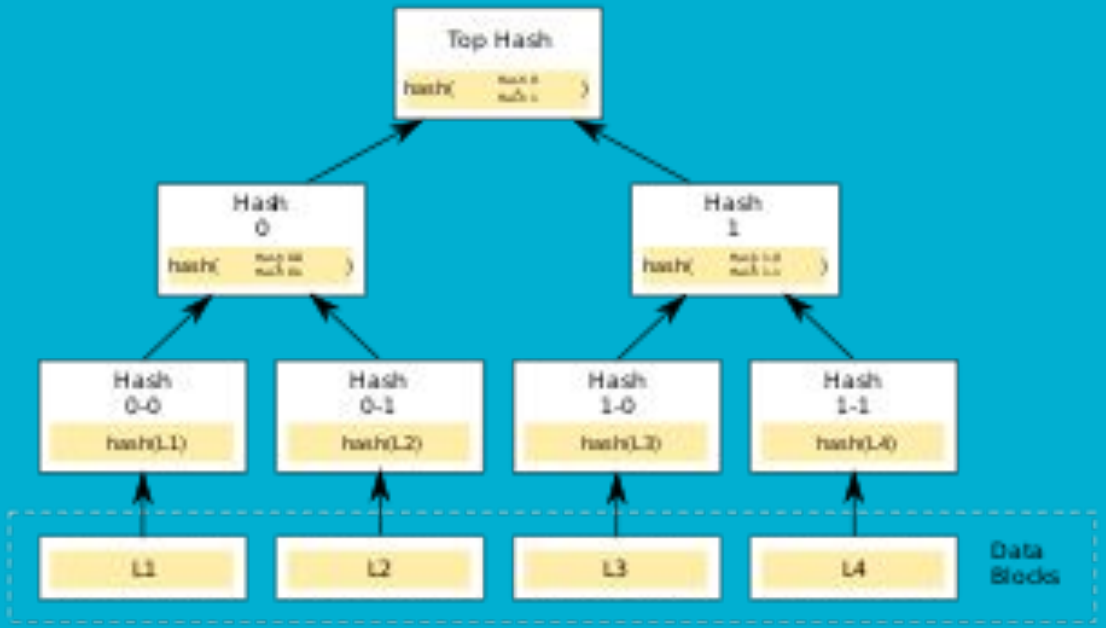


Blockchain 101

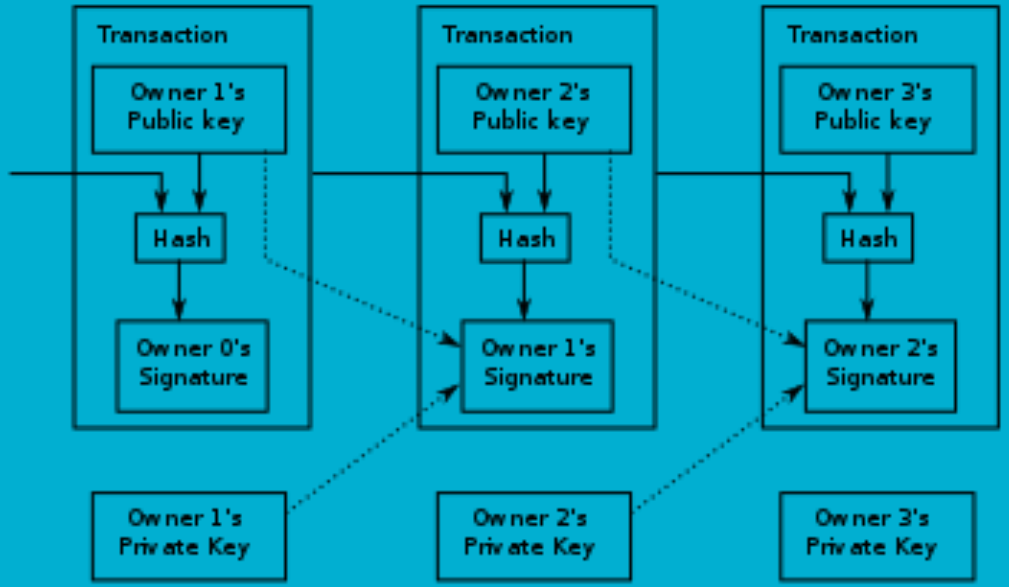
Blockchains Begin



Growing a Merkle Tree



Transactions



Mining

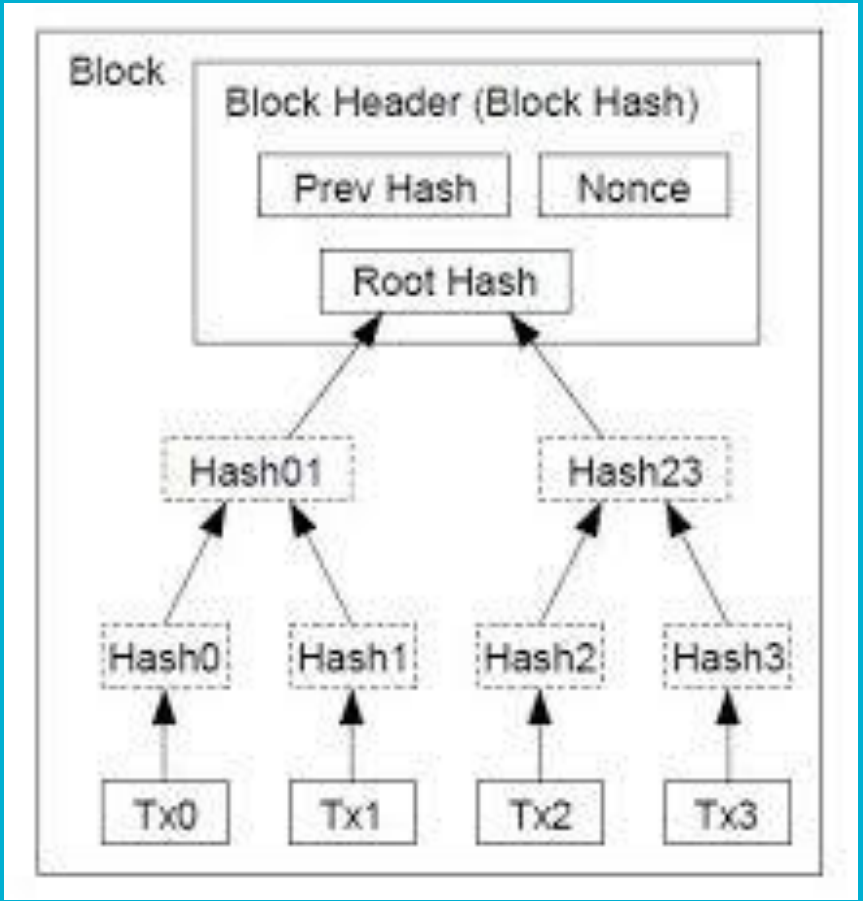
Proportion of hash-power: 0.2

Number of confirms: 10

calculate

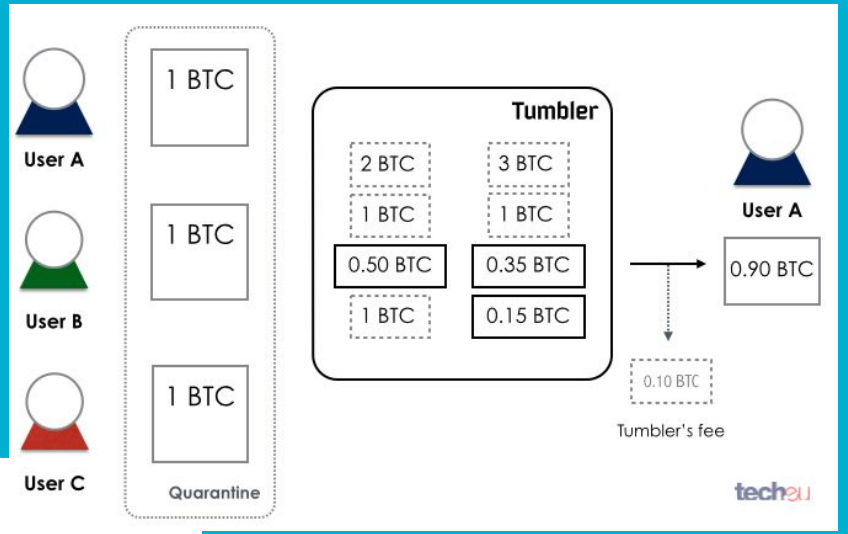
```
AttackerSuccessProbability(0.1,1)=0.204587
AttackerSuccessProbability(0.1,2)=0.0509779
AttackerSuccessProbability(0.1,5)=0.000913682
AttackerSuccessProbability(0.1,10)=1.2414e-06

AttackerSuccessProbability(0.2,1)=0.415899
AttackerSuccessProbability(0.2,2)=0.203929
AttackerSuccessProbability(0.2,5)=0.0274155
AttackerSuccessProbability(0.2,10)=0.00186695
```

Difficulty

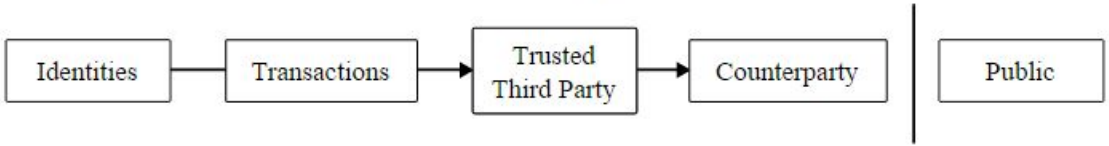

Block
Block Header (Block Hash)
Prev Hash
Nonce
Root Hash
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Wallets

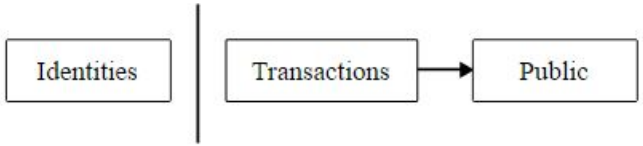
Privacy



Traditional Privacy Model

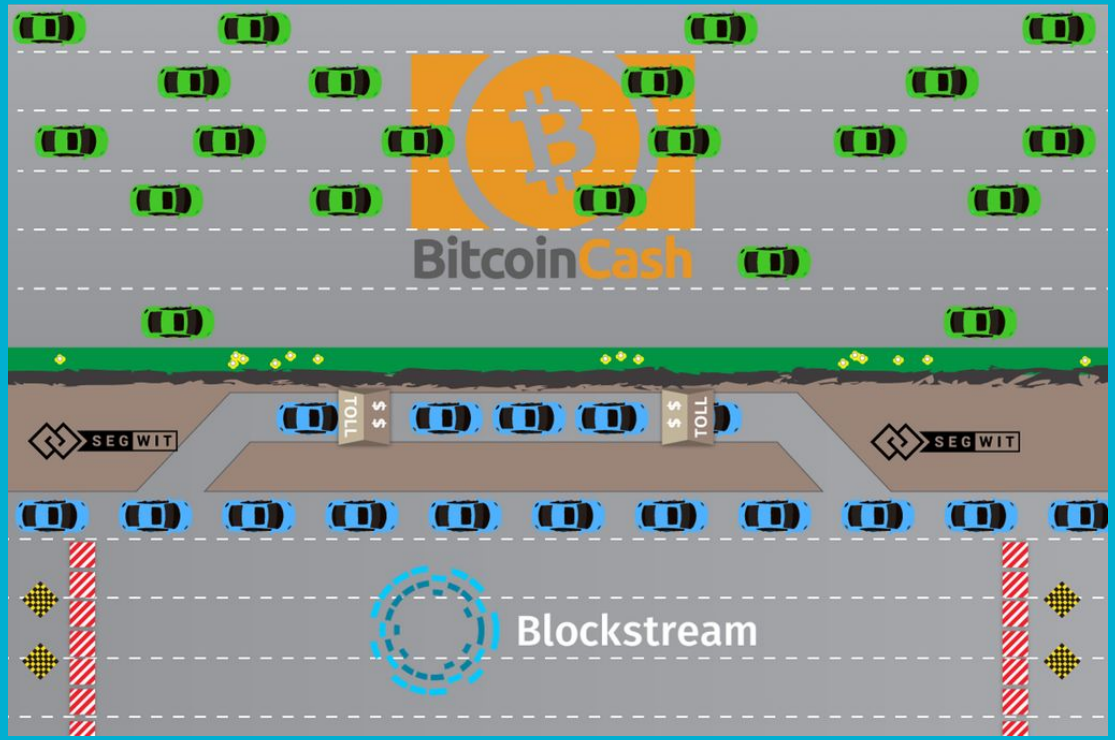


New Privacy Model



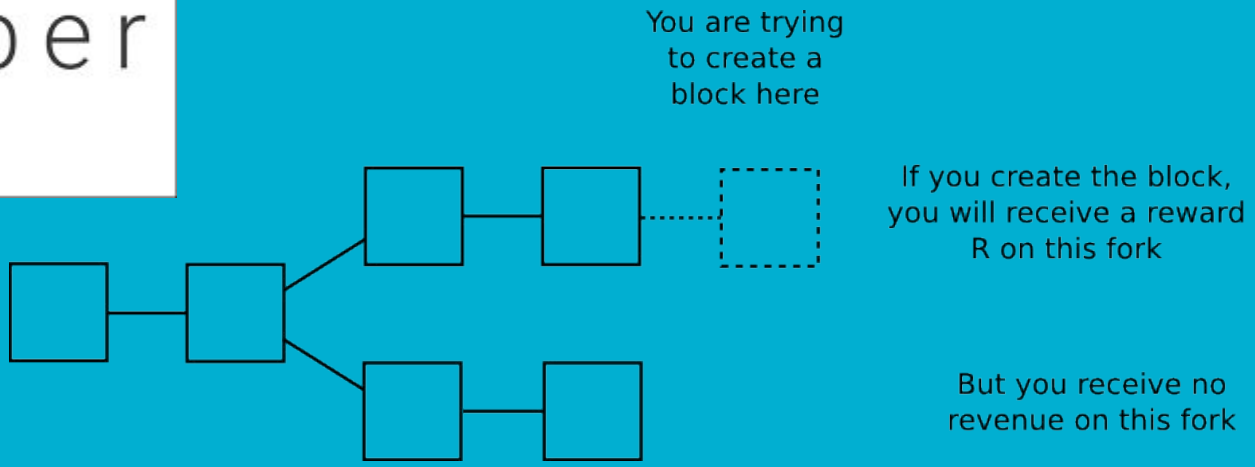
Block Size, SegWit, Lightning Network

(More drama and details here!)



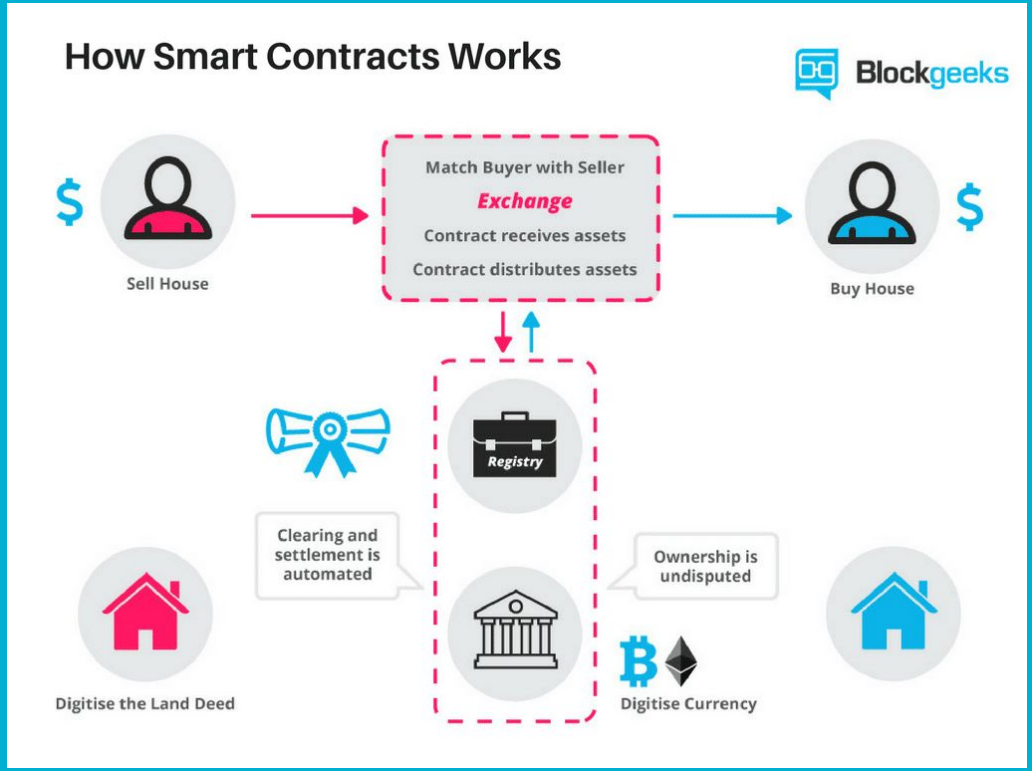
Blockchain 2.0

Proof of Stake



Ethereum and Smart Contracts

[Democracy Earth]



Estonia (AKA the future)

- New Yorker Story
- e-Estonia
- “the most advanced digital society in the world”

Blockchain of Today (yikes)

Please Don’t Blow Bubbles In My Currency (it is Rude)

A Tea Company's Stock Doubled When It Added 'Blockchain' to Its Name

Is this what the Bitcoin bubble looks like?

SHARE TWEET

Allie Conti
Dec 21 2017, 3:43pm

Do Not Go into Debt to Buy Bitcoin, You Idiots

A professor explains what's going on with the so-called cryptocurrency and why it's probably too late to make a fortune off of it.

SHARE TWEET

By Allie Conti; illustrated by Lia Kantrowitz
Dec 13 2017, 3:00pm

Miami's Wild Bitcoin Scene Doesn't Care About Your 'Bubble'

Despite warnings from experts and haters and the occasional plummet in value, the Magic City is going all-in.

SHARE TWEET

By Francisco Alvarado; illustrated by Lia Kantrowitz
Jan 16 2018, 1:25pm

Cryptocurrencies Are the New Black

Questions?

Slides are at
https://elgar.laudiacay.net/blockchain_talk.pdf