

Blockchain™

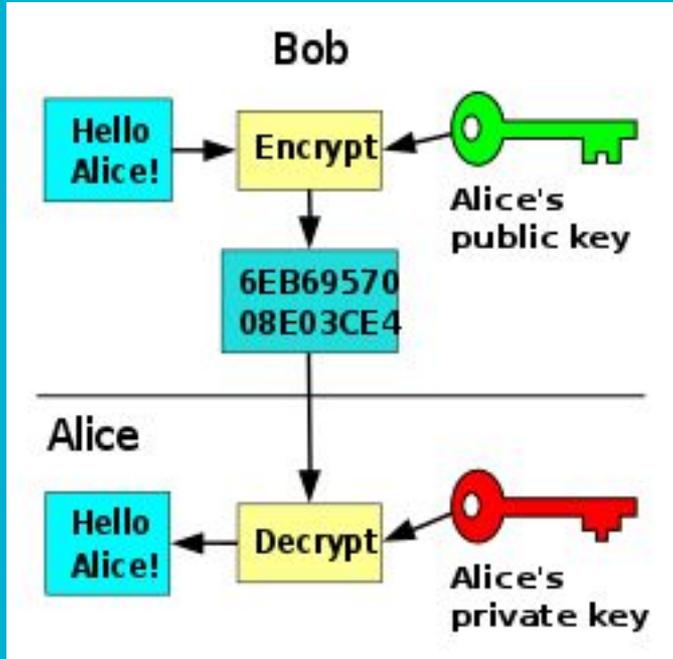
or: How I Learned to Stop Worrying and Love the Bubble

Claudia Richoux

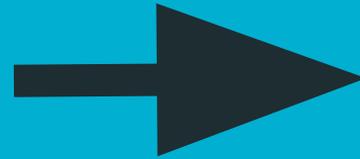
29 January 2018, Asynchronous Anonymous

Cryptographic Background/History

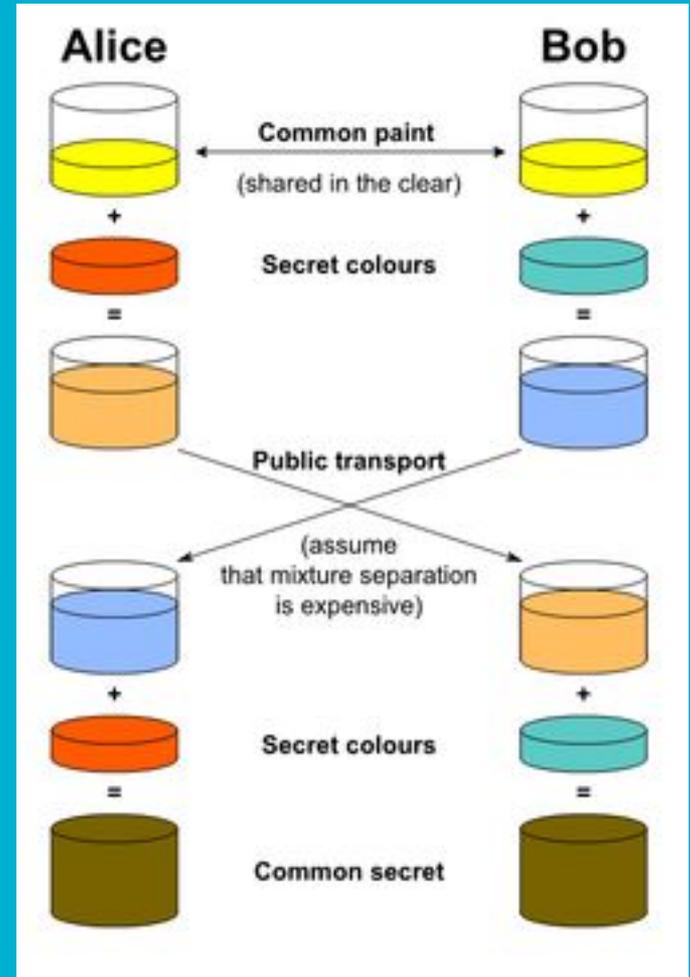
Public-Key Cryptography



Diffie-Hellman
Key Exchange

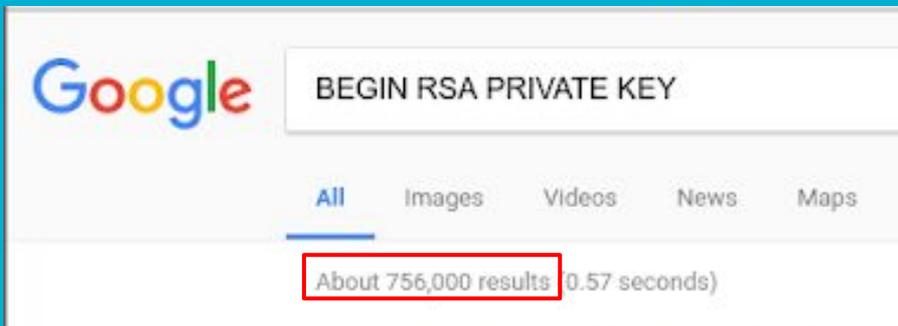


RSA (or other
schemes)



Crypto 101 Intermission

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



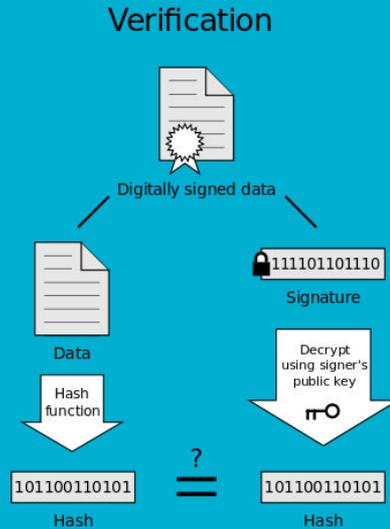
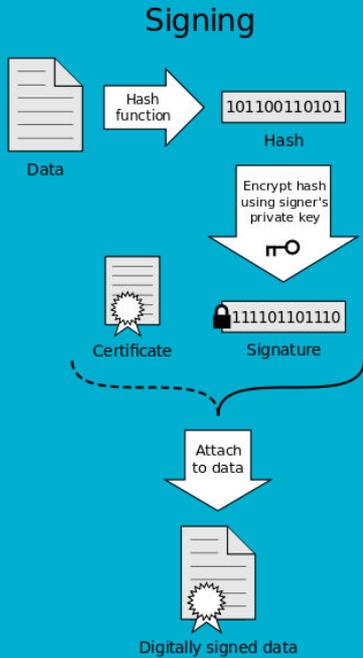
A screenshot of a Google search interface. The search bar contains the text "BEGIN RSA PRIVATE KEY". Below the search bar, there are tabs for "All", "Images", "Videos", "News", and "Maps". The "All" tab is selected. At the bottom of the search results area, a red box highlights the text "About 756,000 results" and "0.57 seconds".



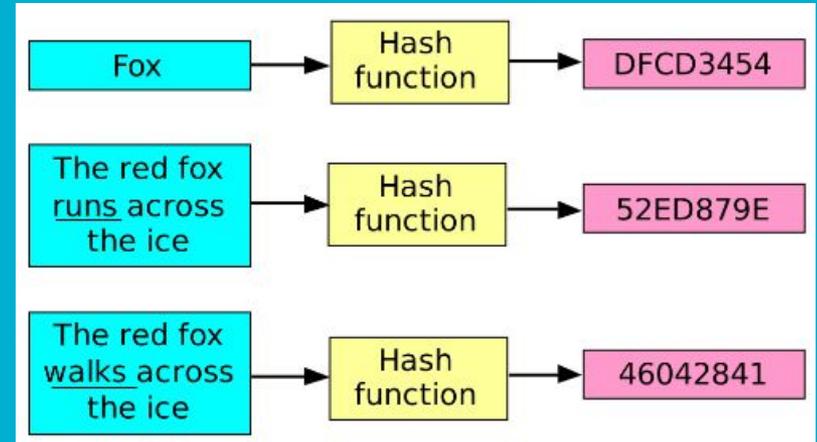
Search results for '0xec16663f3aa6334c'

Type	bits/keyID	cr. time	exp time	key expir
pub	2048R/3AA6334C	2016-02-12		
uid	Claudia Richoux (Hello!) <claudiacay@gmail.com>			
sig	sig3 3AA6334C	2016-02-12		[selfsig]
sig	sig 3C472B56	2016-02-17		Samuel Damashek <ssdamashek@gentoo.org>
sig	sig 83888769	2016-02-18		Fox C. Wilson <fwilson@fwilson.me>
	Policy URL: http://fwilson.me/keysigining-feb2016.txt			
sig	sig 73DD0719	2016-02-18		Fox Connor Wilson <fwilson@lessbroken.org>
	Policy URL: http://fwilson.me/keysigining-feb2016.txt			
sub	2048R/A51C7141	2016-02-12		
sig	sbind 3AA6334C	2016-02-12		[]

Basic Cryptographic Operations

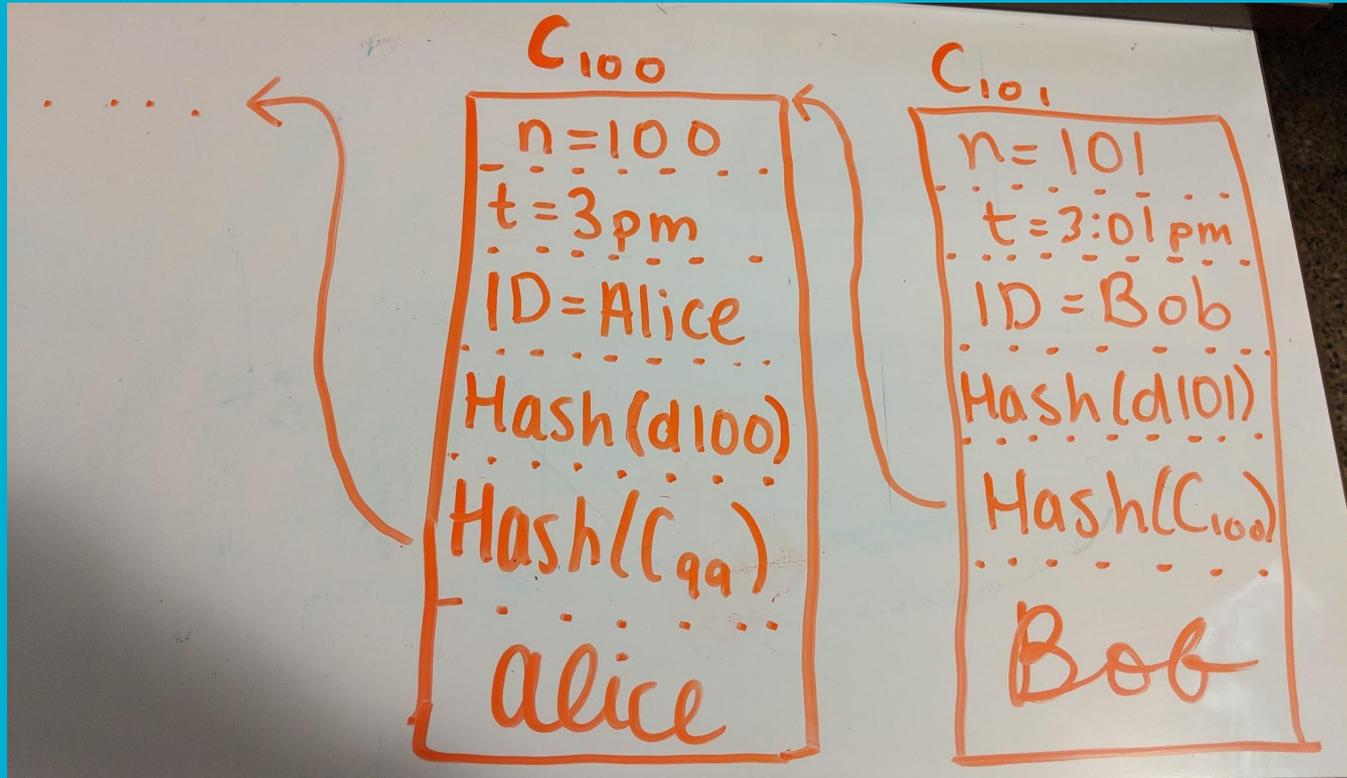


If the hashes are equal, the signature is valid.

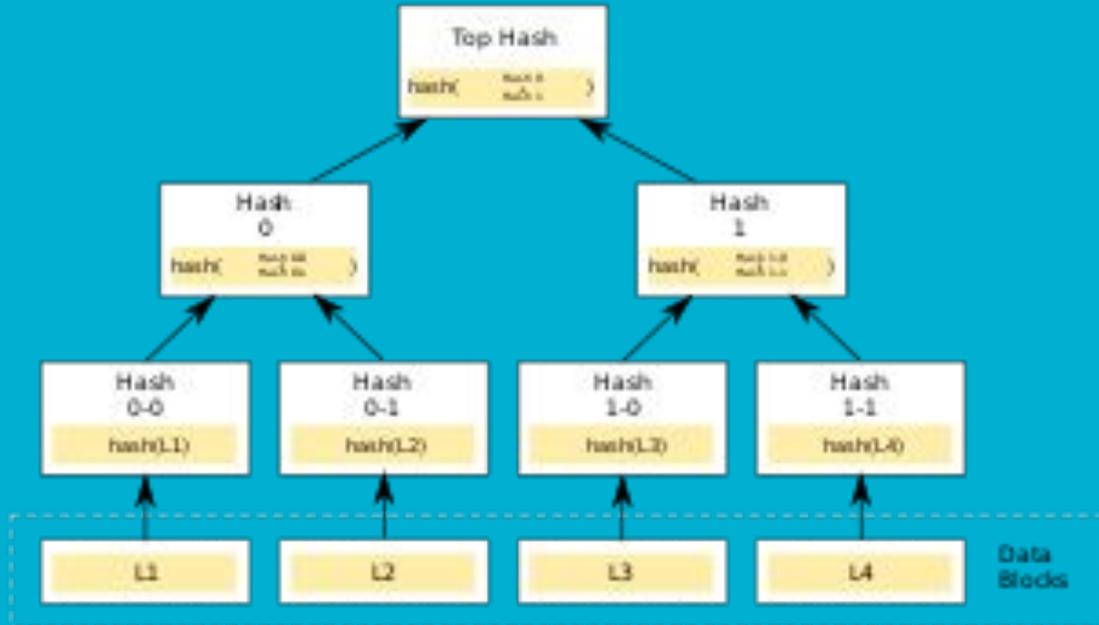


Blockchain 101

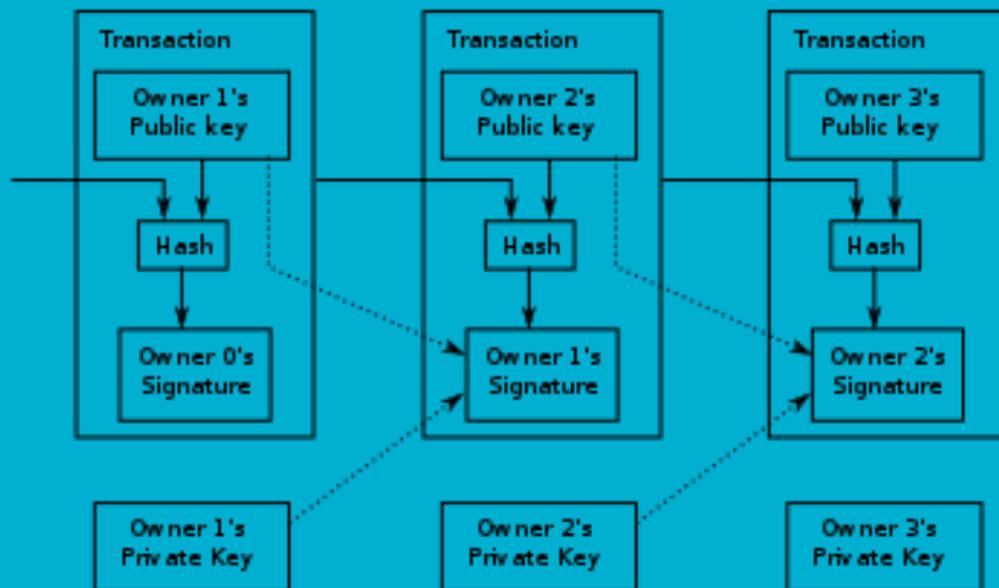
Blockchains Begin



Growing a Merkle Tree



Transactions



Mining



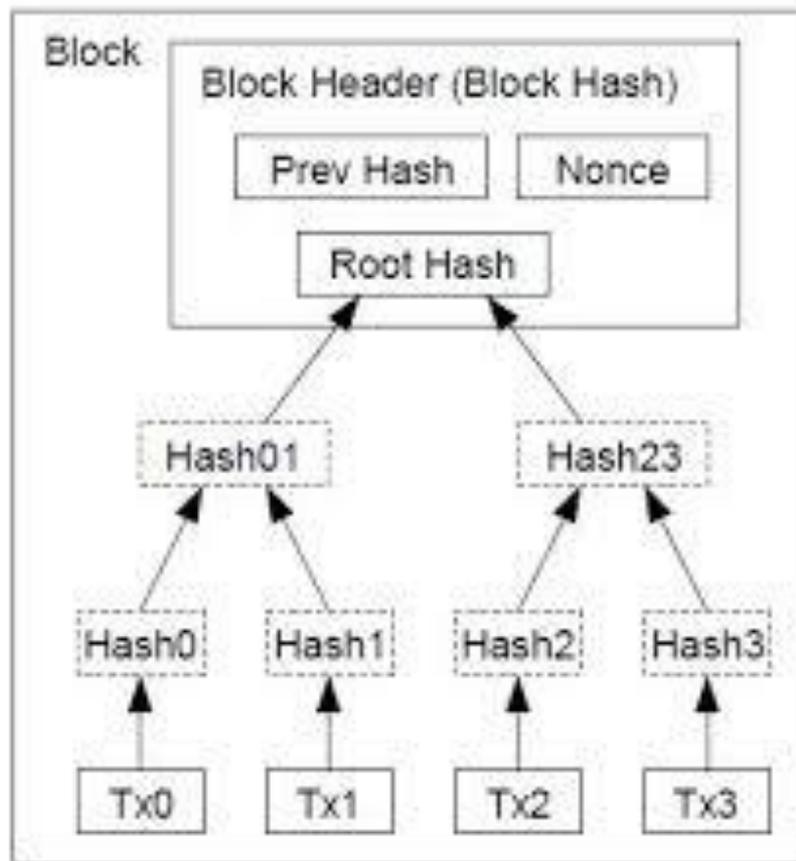
Proportion of hash-power:

Number of confirms:

```
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)=0.00106695
```

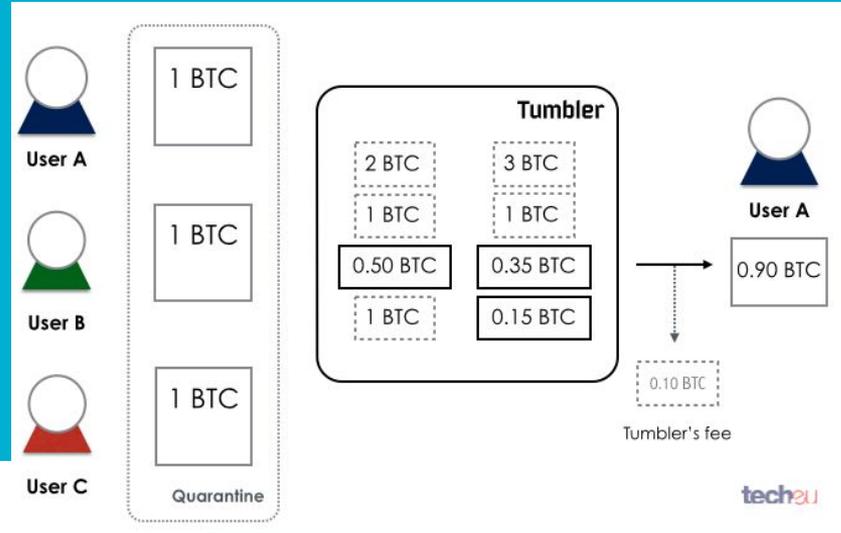
Difficulty



Wallets



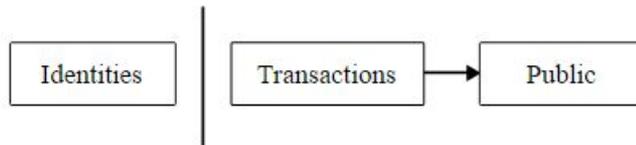
Privacy



Traditional Privacy Model

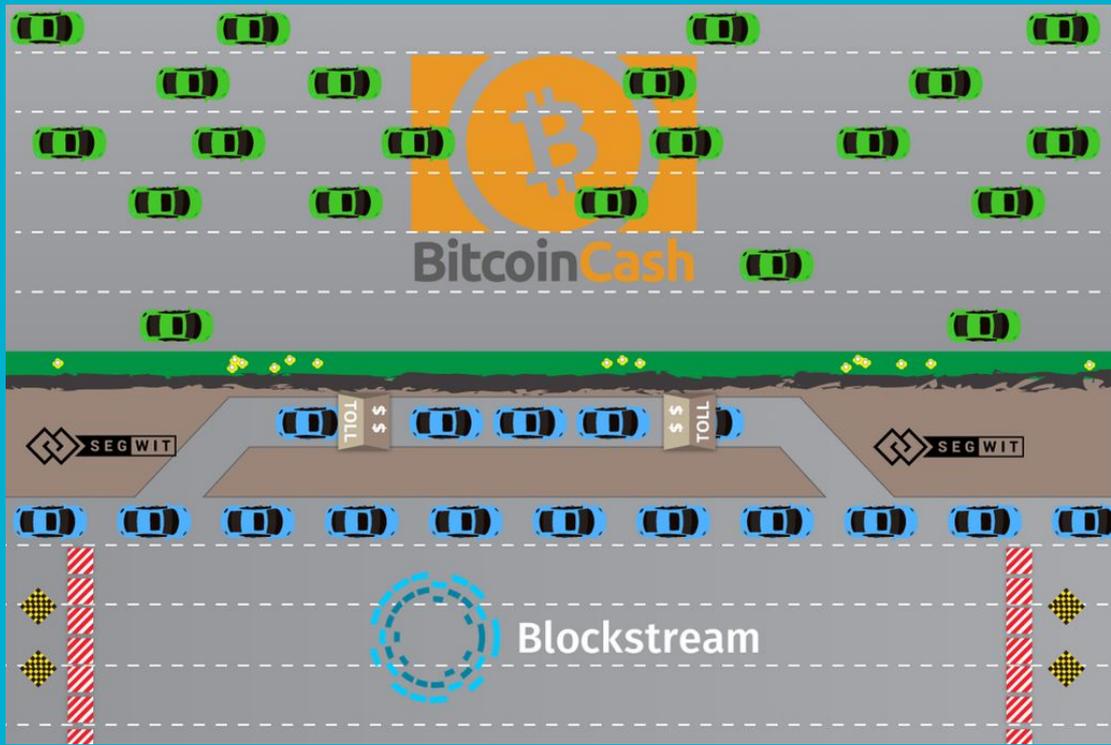


New Privacy Model



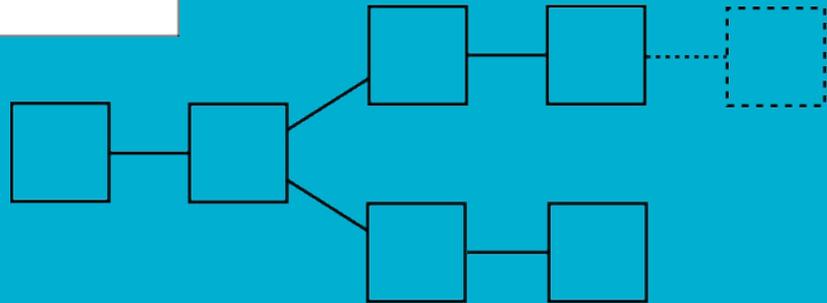
Block Size, SegWit, Lightning Network

[\(More drama and details here!\)](#)



Blockchain 2.0

Proof of Stake



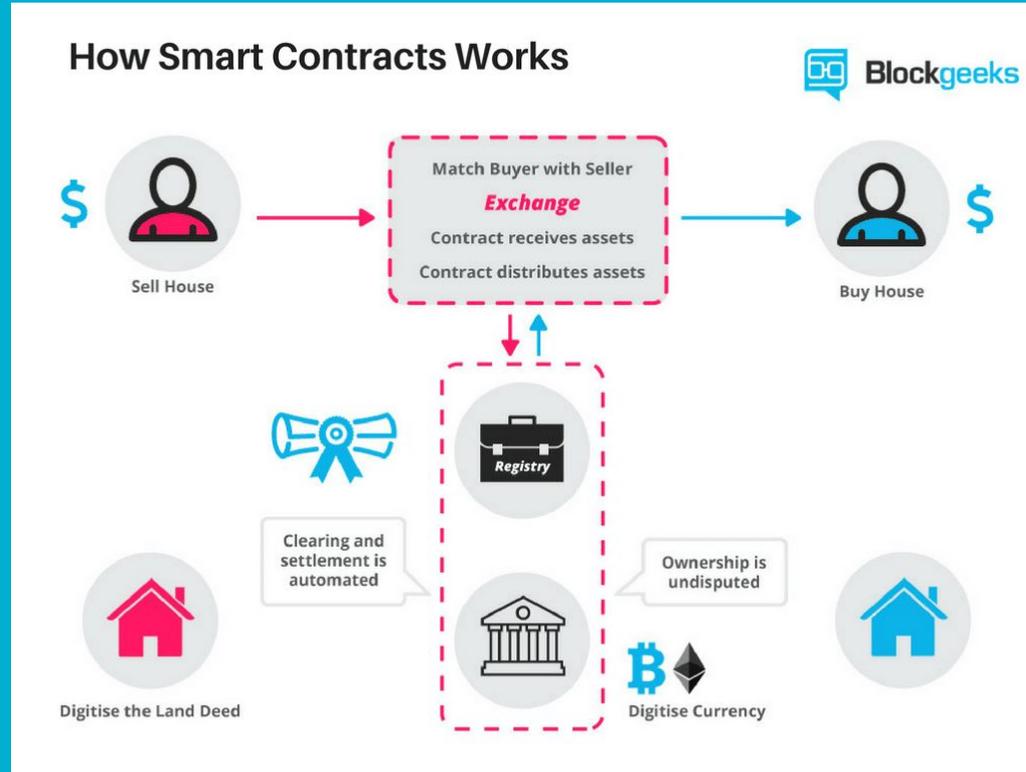
You are trying
to create a
block here

If you create the block,
you will receive a reward
R on this fork

But you receive no
revenue on this fork

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 

 Alle Contt
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 Alle Contt, illustrated by Lia Kantowitz
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 Kantowitz
Jan 16 2018, 1:25pm



Cryptocurrencies Are the New Black



Questions?

Slides are at

https://elgar.laudiacay.net/blockchain_talk.pdf