PDXWIT

augur

An introduction to bitcoin, blockchain, and cryptocurrency

Overview

- About myself
- Why you should care
- Terminology
- Blockchain Story Hour
- Signed Transactions
- Demo

About Me (Scott Bigelow)

- **Received first crypto token in 2013 when a friend sent me Dogecoin**
- Got into Bitcoin in 2014
- Ethereum early this year
- Joined Ethereum project Augur in October 2017

very currency wow much coin how money so crypto plz mine v rich
wow

About Me (Scott Bigelow)

- Received first crypto token in 2013 when a friend sent me Dogecoin
- **Got into Bitcoin in 2014**
- Ethereum early this year
- Joined Ethereum project Augur in October 2017

About Me (Scott Bigelow)

- Received first crypto token in 2013 when a friend sent me Dogecoin
- Got into Bitcoin in 2014
- **Ethereum early this year**
- Joined Ethereum project Augur in October 2017

ethereum

About Me (Scott Bigelow)

- Received first crypto token in 2013 when a friend sent me Dogecoin
- Got into Bitcoin in 2014
- Ethereum early this year
- **Joined Ethereum project Augur in October 2017**

Bitcoin is a distributed system which implements a *blockchain*-based *cryptocurrency*

Bitcoin is a distributed system which implements a *blockchain*-based *cryptocurrency*

Bitcoin is [unfortunately] ALSO the name of the tokens used on the *Bitcoin* network

Bitcoin is a distributed system which implements a *blockchain*-based *cryptocurrency*

Bitcoin is [unfortunately] ALSO the name of the tokens used on the *Bitcoin* network

(The token is sometimes referred to as **BTC**)

Ethereum is a distributed system which implements a *blockchain*-based *cryptocurrency*

ethereum

Ethereum is a distributed system which implements a *blockchain*-based *cryptocurrency*

Ether is the name of the tokens used on the *Ethereum* network

ethereum

Ethereum is a distributed system which implements a *blockchain*-based *cryptocurrency*

Ether is the name of the tokens used on the *Ethereum* network

(The token is sometimes referred to as **ETH**)

ethereum

Blockchain Story Hour

1.) No one person in the this room should dominate the story

1.) No one person in the this room should dominate the story

2.) Selected words should resist change and removal.

Teacher Strategy

Teacher Strategy

~~1.) No one person in the this room should dominate the story~~

Teacher Strategy

~~1.) No one person in the this room should dominate the story~~

~~2.) Selected words should resist change and removal.~~

Recess Strategy

Once

Recess Strategy

Upon

There

Their

Once

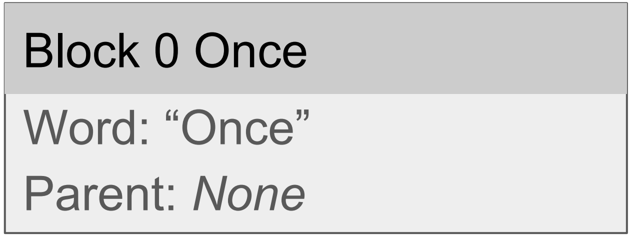
My

Again

Oncey McOnceFace

A

Blockchain Strategy

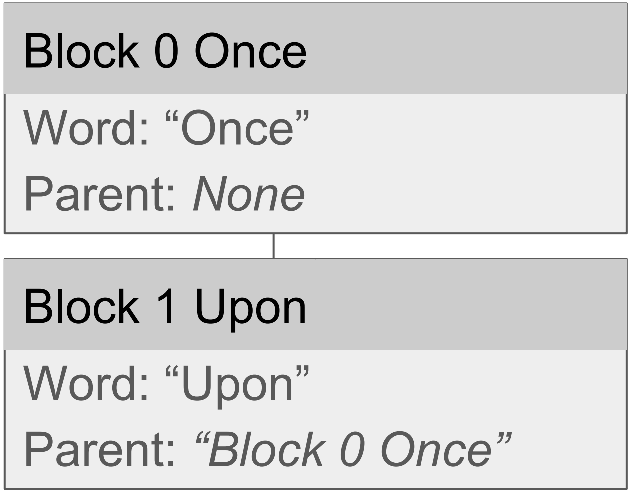


Block 0 Once

Word: “Once”

Parent: *None*

Blockchain Strategy



Block 0 Once

Word: “Once”

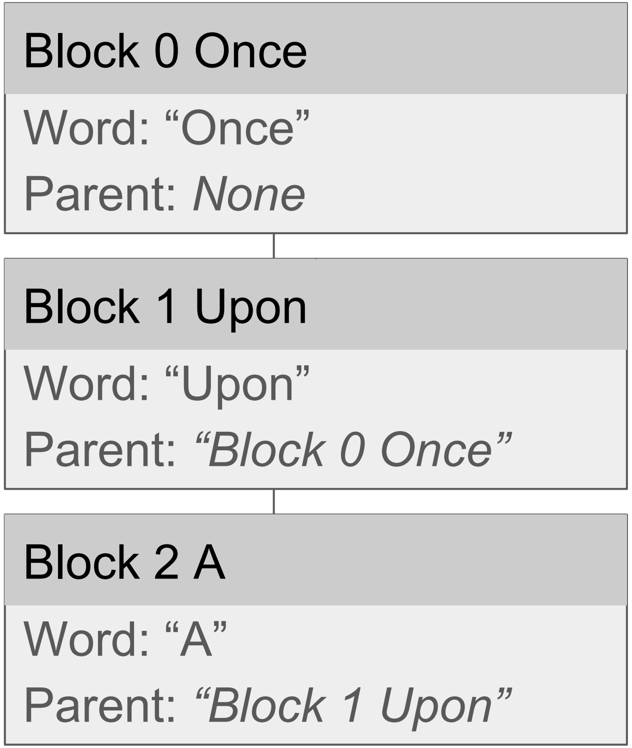
Parent: *None*

Block 1 Upon

Word: “Upon”

Parent: *“Block 0 Once”*

Blockchain Strategy



Block 0 Once

Word: “Once”

Parent: *None*

Block 1 Upon

Word: “Upon”

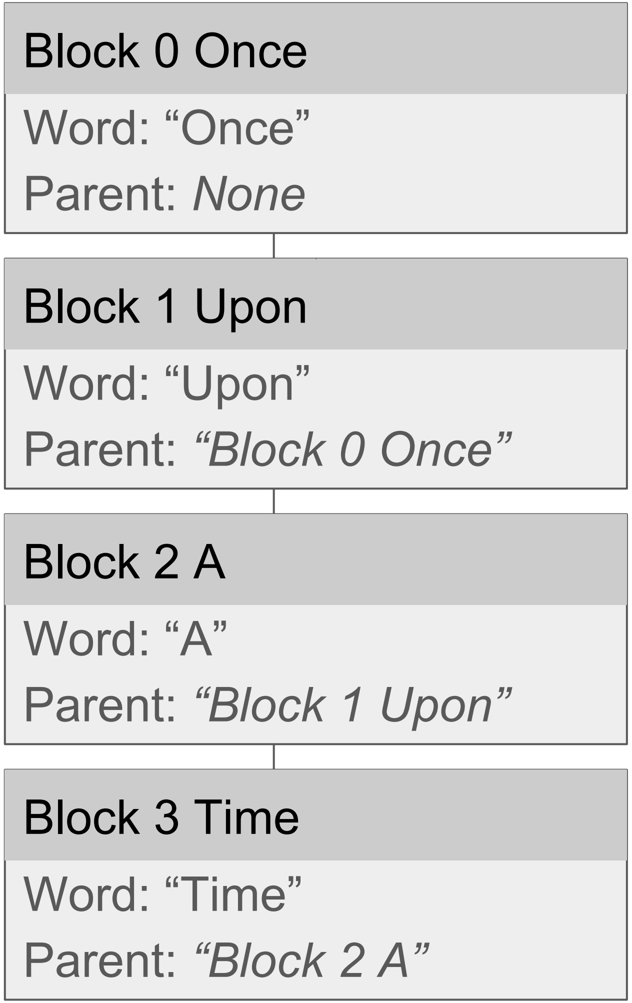
Parent: *“Block 0 Once”*

Block 2 A

Word: “A”

Parent: *“Block 1 Upon”*

Blockchain Strategy



Block 0 Once

Word: “Once”

Parent: *None*

Block 1 Upon

Word: “Upon”

Parent: *“Block 0 Once”*

Block 2 A

Word: “A”

Parent: *“Block 1 Upon”*

Block 3 Time

Word: “Time”

Parent: *“Block 2 A”*

Recess Strategy

Upon

Their

There

Once

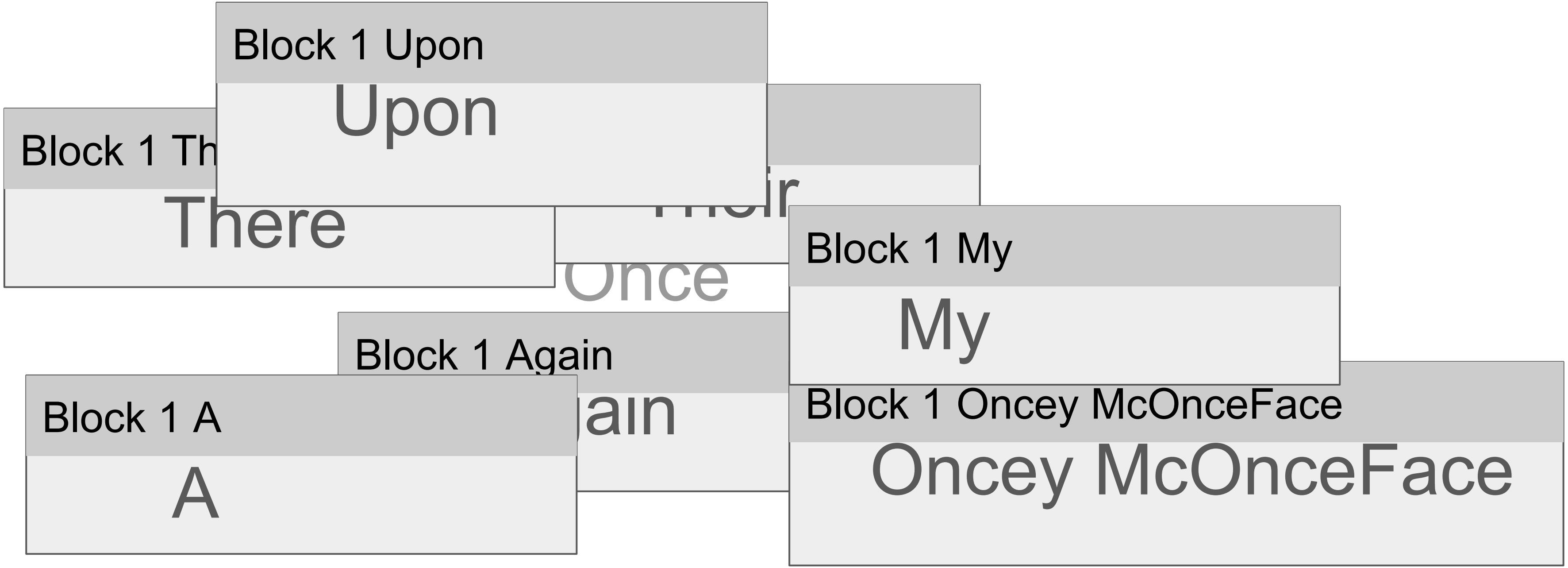
My

Again

Oncey McOnceFace

A

Recess Strategy



Block 1 Upon

Upon

Block 1 Th

There

Their

Once

Block 1 My

My

Block 1 Again

gain

Block 1 A

A

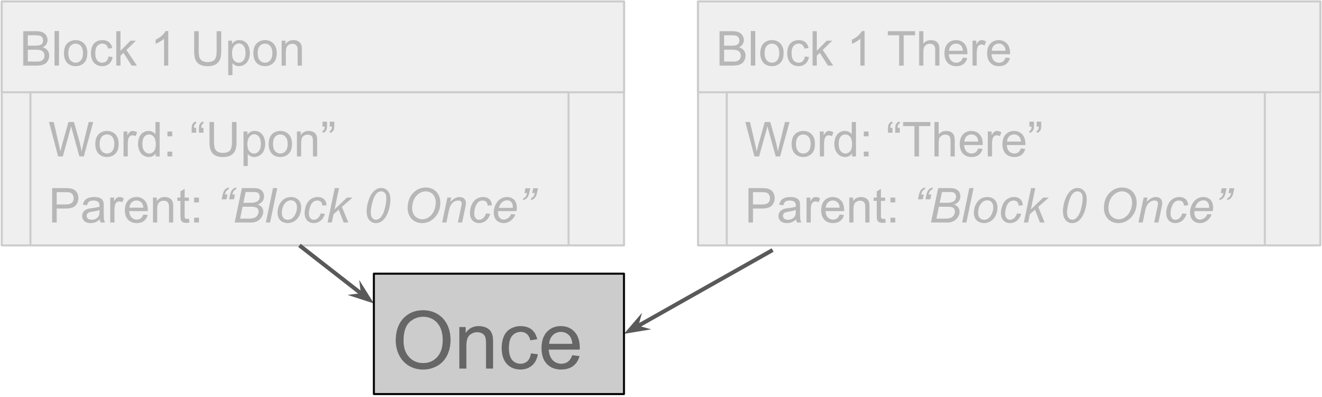
Block 1 Oncey McOnceFace

Oncey McOnceFace

Blockchain Strategy

Once

Blockchain Strategy



Block 1 Upon

Word: “Upon”

Parent: *“Block 0 Once”*

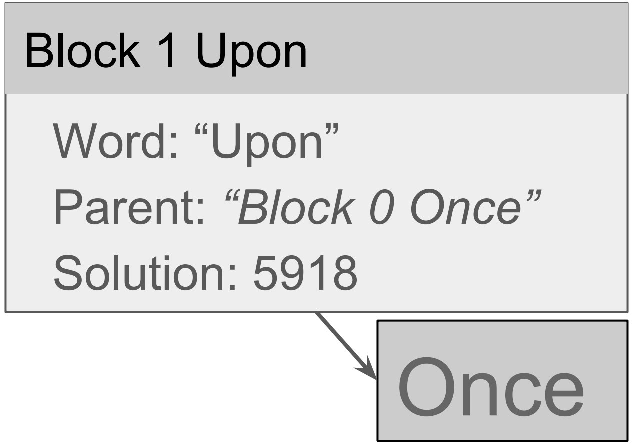
Block 1 There

Word: “There”

Parent: *“Block 0 Once”*

Once

Blockchain Strategy



Block 1 Upon

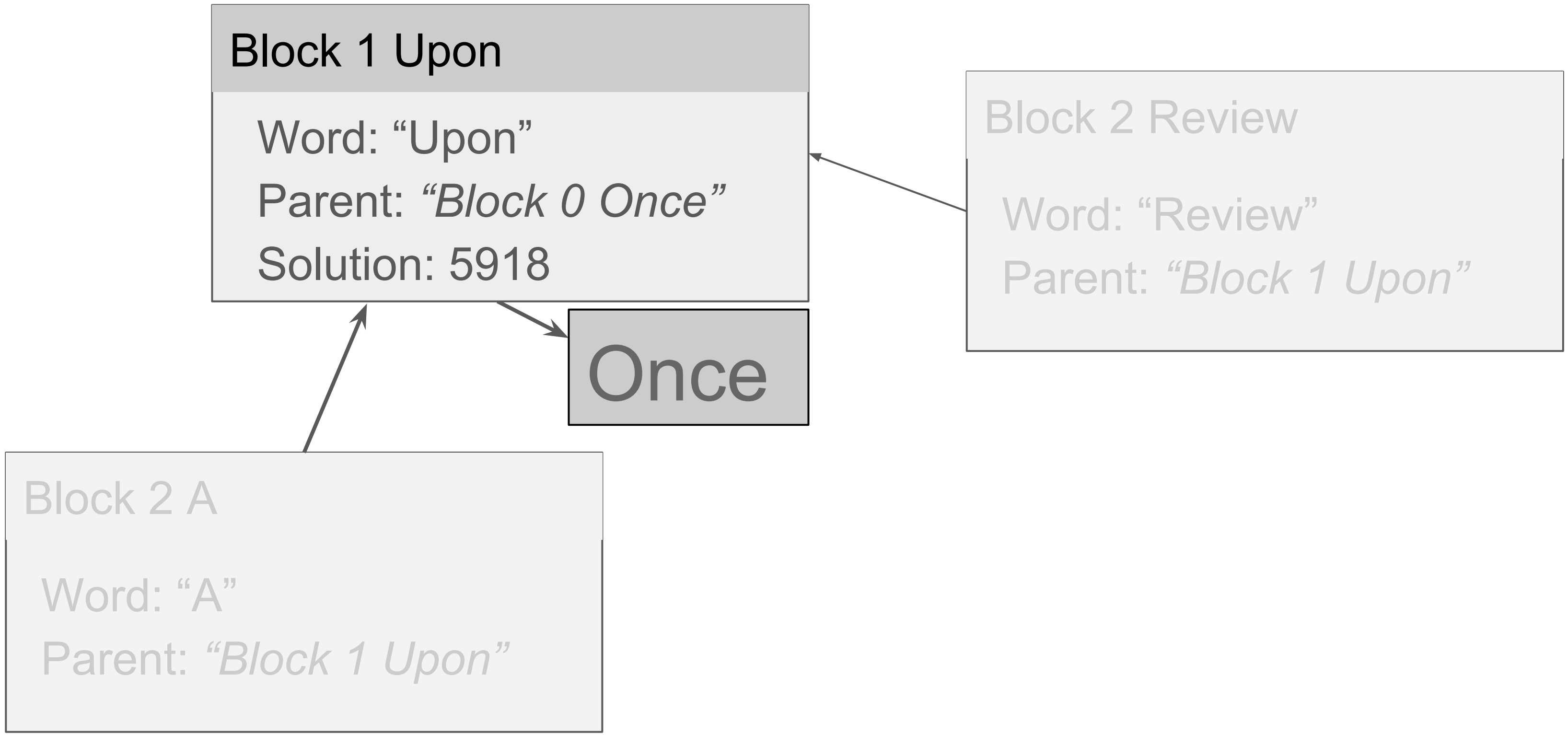
Word: “Upon”

Parent: *“Block 0 Once”*

Solution: 5918

Once

Blockchain Strategy



Block 1 Upon

Word: “Upon”

Parent: *“Block 0 Once”*

Solution: 5918

Once

Block 2 Review

Word: “Review”

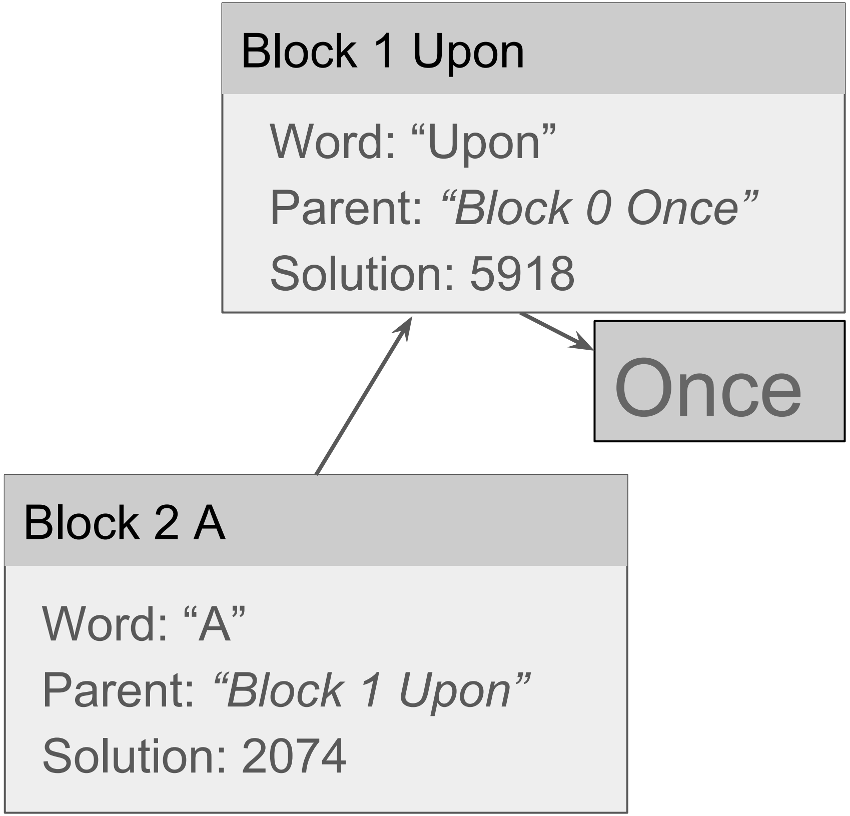
Parent: *“Block 1 Upon”*

Block 2 A

Word: “A”

Parent: *“Block 1 Upon”*

Blockchain Strategy



Block 1 Upon

Word: “Upon”

Parent: *“Block 0 Once”*

Solution: 5918

Once

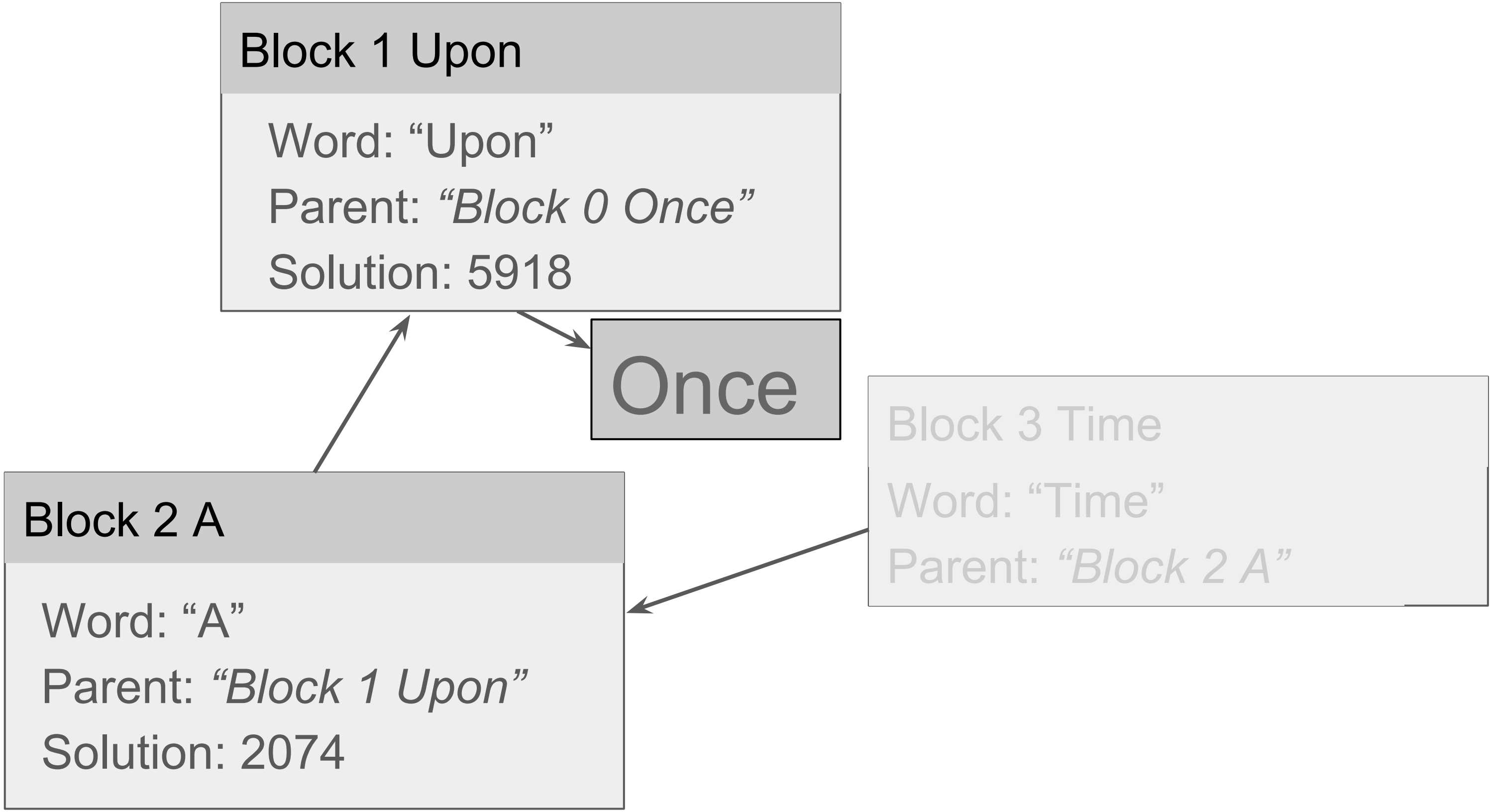
Block 2 A

Word: “A”

Parent: *“Block 1 Upon”*

Solution: 2074

Blockchain Strategy



Block 1 Upon

Word: “Upon”

Parent: *“Block 0 Once”*

Solution: 5918

Once

Block 2 A

Word: “A”

Parent: *“Block 1 Upon”*

Solution: 2074

Block 3 Time

Word: “Time”

Parent: *“Block 2 A”*

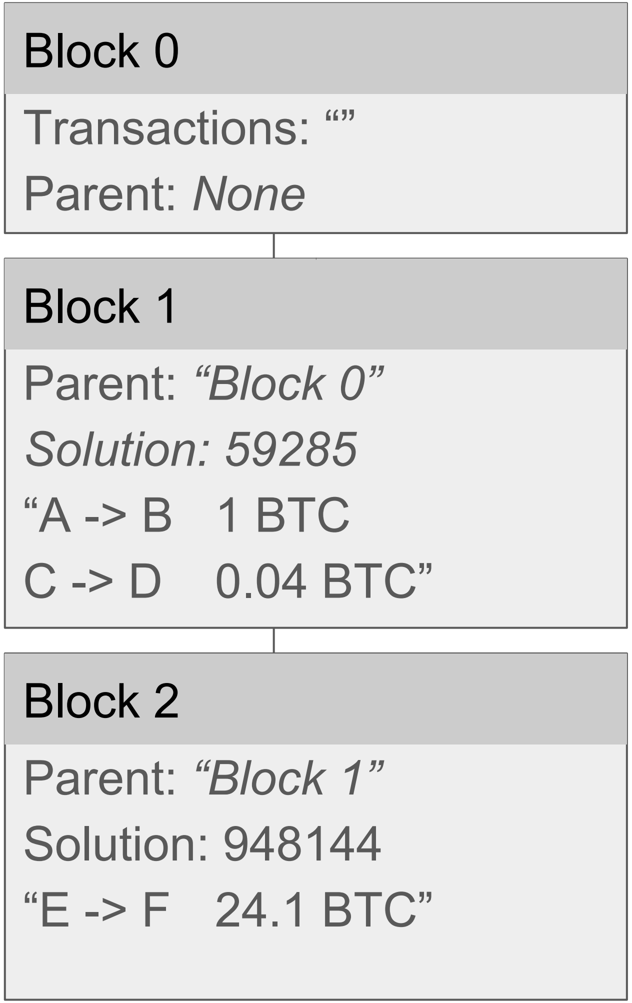
Blockchain Strategy

1.) No one person in the this room should dominate the story

Blockchain Strategy

1.) No one person in the this room should dominate the story

2.) Selected words should resist change and removal.



Block 0

Transactions: “”

Parent: *None*

Block 1

Parent: *“Block 0”*

Solution: 59285

“A -> B   1 BTC

C -> D   0.04 BTC”

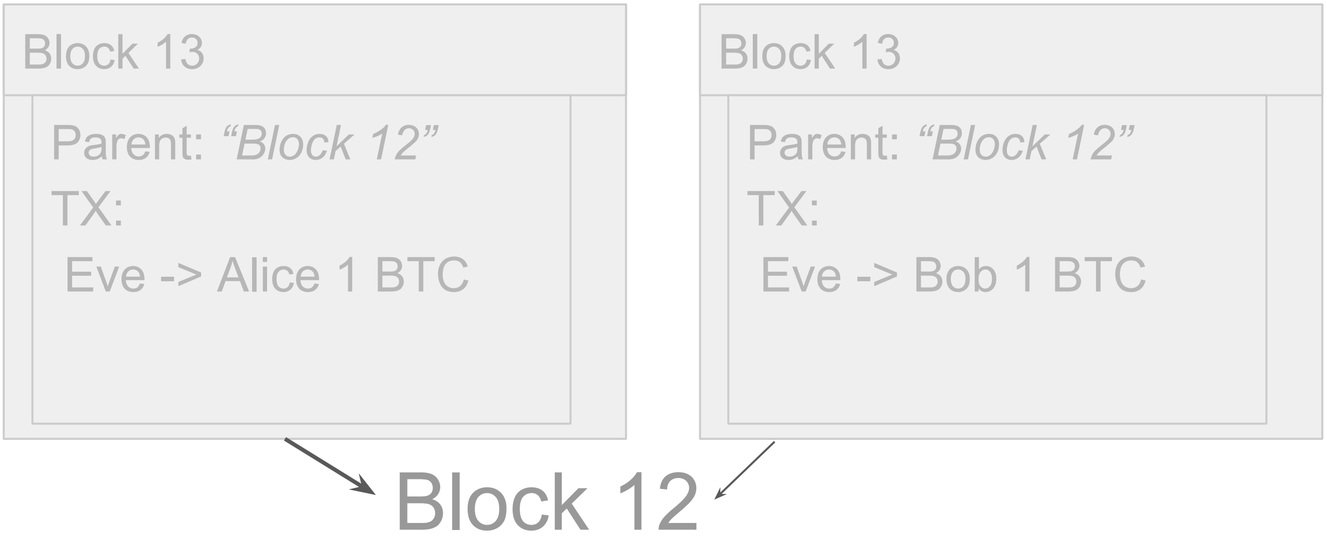
Block 2

Parent: *“Block 1”*

Solution: 948144

“E -> F   24.1 BTC”

Double Spend



Block 13

Parent: *“Block 12”*

TX:

Eve -> Alice 1 BTC

Block 13

Parent: *“Block 12”*

TX:

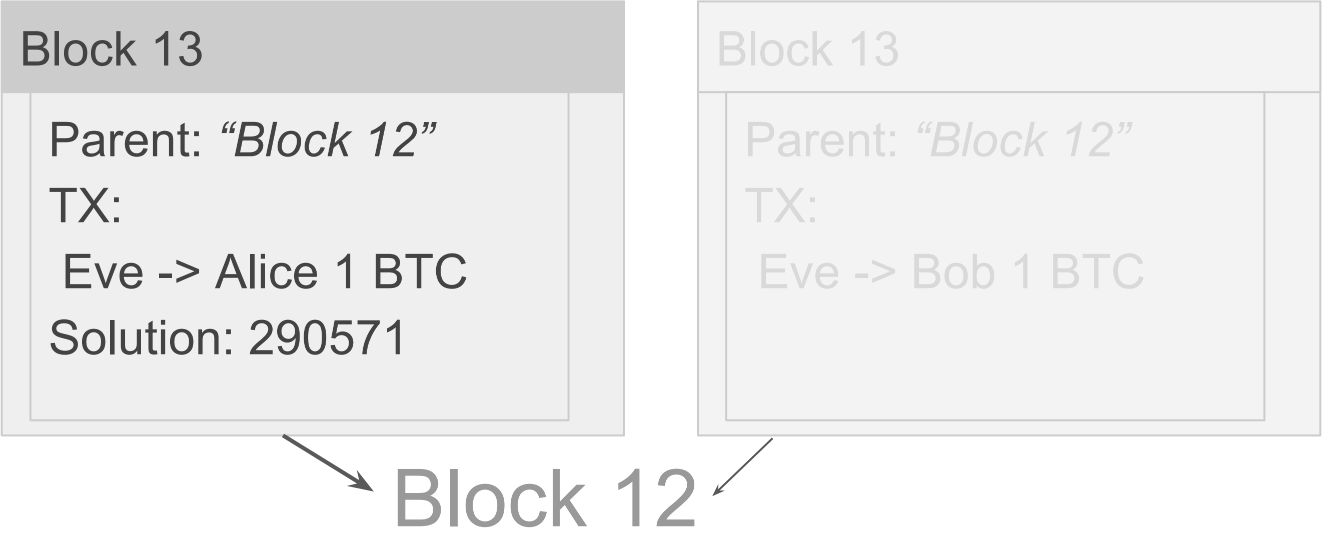
Eve -> Bob 1 BTC

Block 12

Balances:

- Eve: 1 BTC
- Alice: 0 BTC
- Bob: 0 BTC

Double Spend



Block 13

Parent: *“Block 12”*

TX:

Eve -> Alice 1 BTC

Solution: 290571

Block 13

Parent: *“Block 12”*

TX:

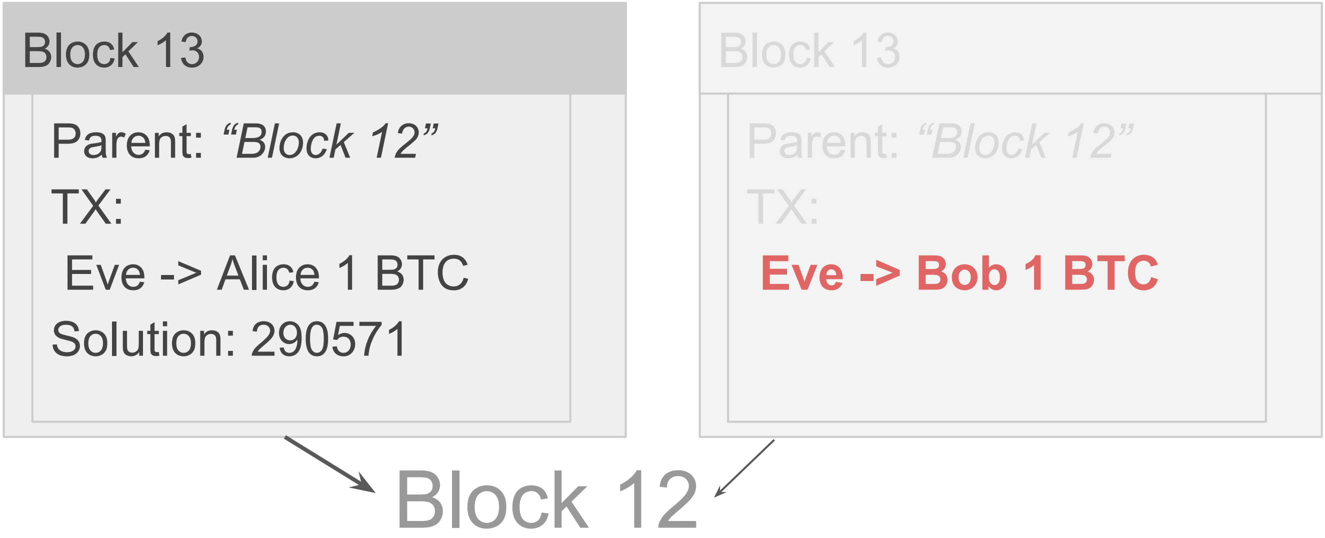
Eve -> Bob 1 BTC

Block 12

Balances:

Eve:	0 BTC
Alice:	1 BTC
Bob:	0 BTC

Double Spend



Block 13

Parent: *"Block 12"*

TX:

Eve -> Alice 1 BTC

Solution: 290571

Block 13

Parent: *"Block 12"*

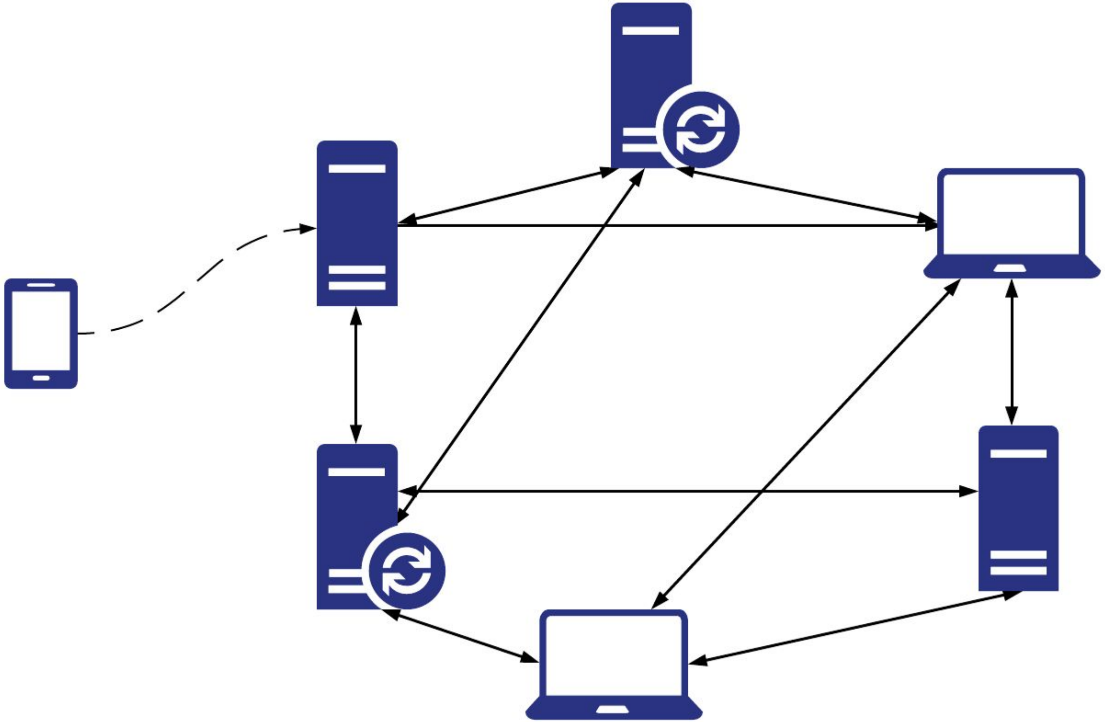
TX:

Eve -> Bob 1 BTC

Block 12

Balances:

- **Eve: 0 BTC**
- Alice: 1 BTC
- Bob: 0 BTC

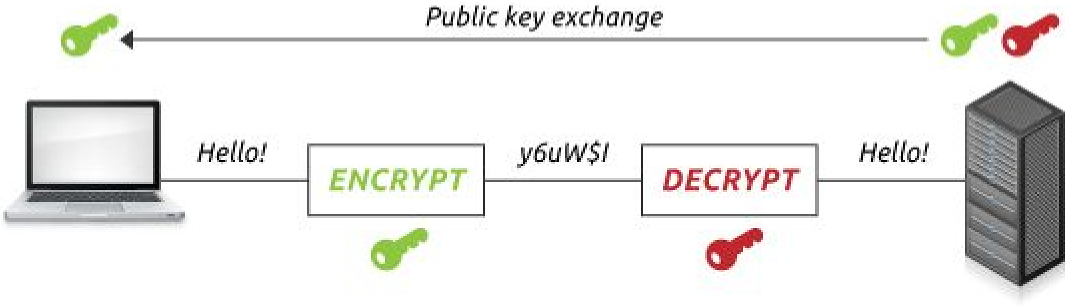


- Demo - https://anders.com/blockchain/
- Bitcoin Explorer - https://blockexplorer.com
- Ethereum Explorer - https://etherscan.io/

Signed Transactions

Signed Transactions

Crypto[graphy] currency



Crypto[graphy] currency

Publi key e ge
ello!
EN
DECRYPT

NO ENCRYPTION

Digital signatures

- Scheme for demonstrating the authenticity of digital messages or documents.
- A valid digital signature gives a recipient reason to believe that
    - the message was created by a known sender (authentication)
    - that the sender cannot deny having sent the message (non-repudiation)
    - and that the message was not altered in transit (integrity).

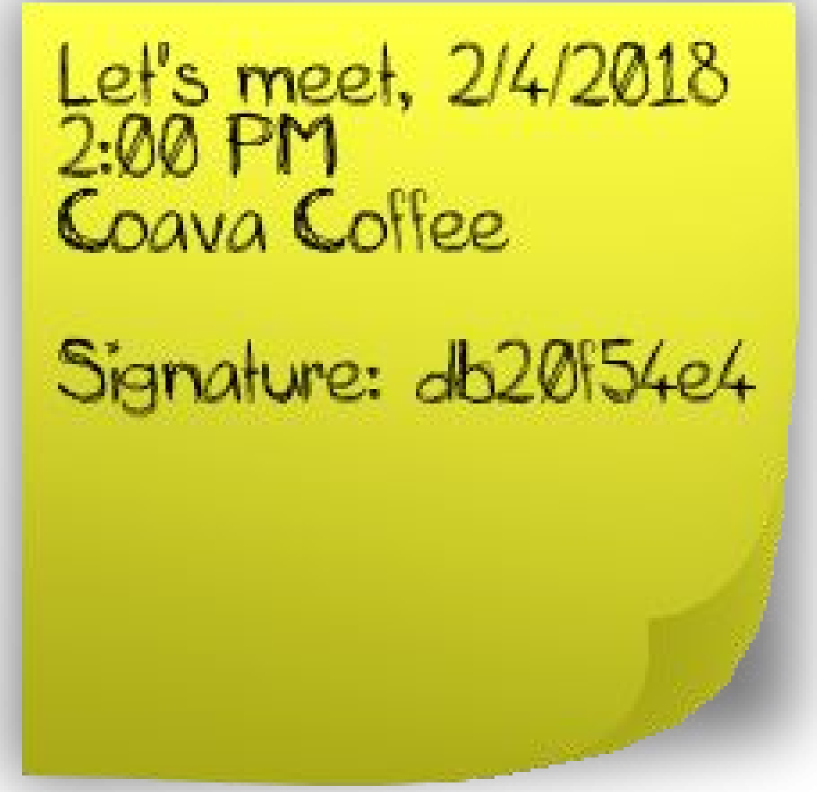
Source: https://en.wikipedia.org/wiki/Digital_signature

Signed Transactions

Scott's Public Key

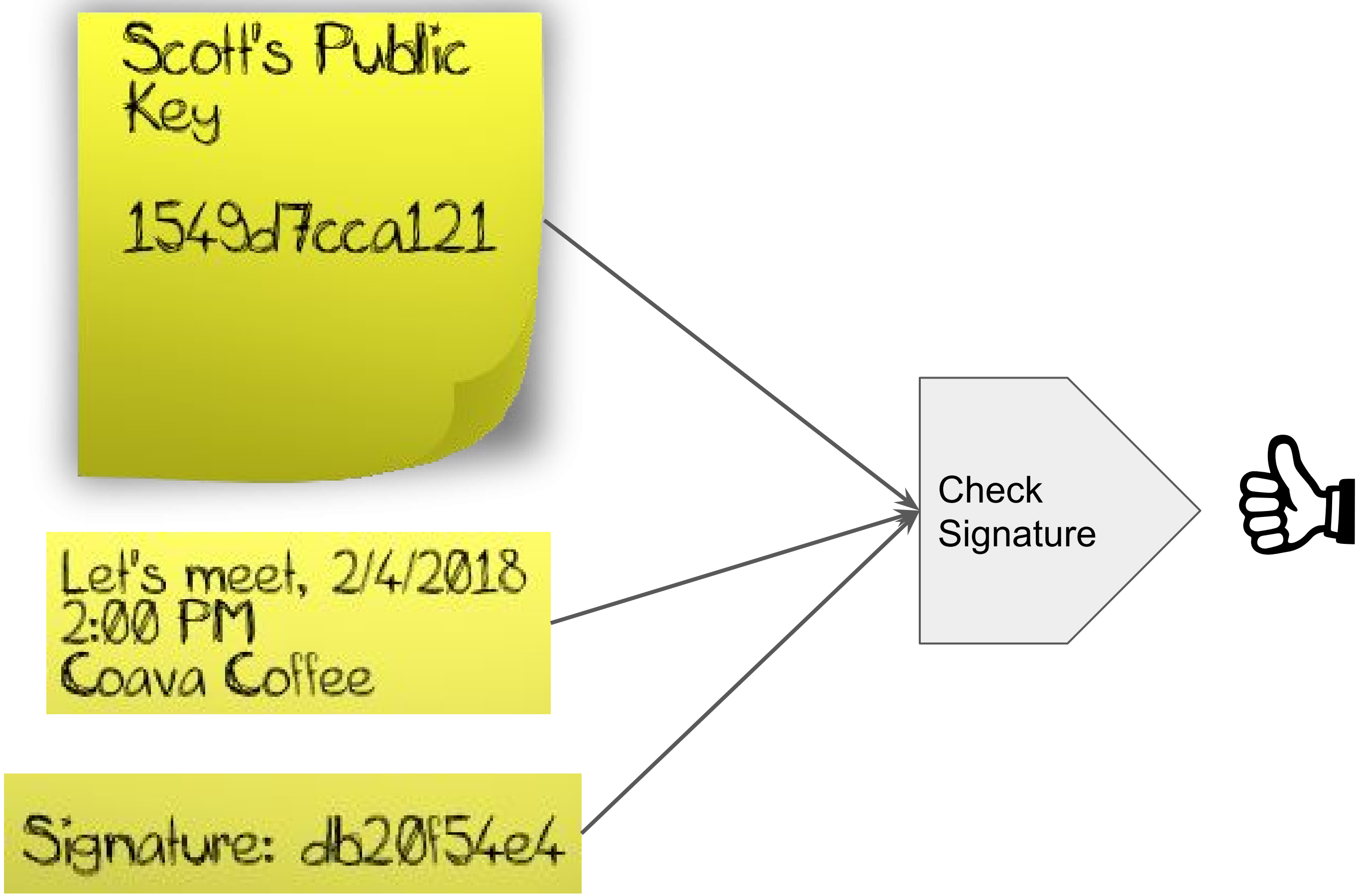
1549d7cca121

Signed Transactions



Let's meet, 2/4/2018
2:00 PM
Coava Coffee

Signature: db20f54e4



Scott's Public Key

1549d7cca121

Let's meet, 2/4/2018
2:00 PM
Coava Coffee

Signature: db20f54e4

Check
Signature

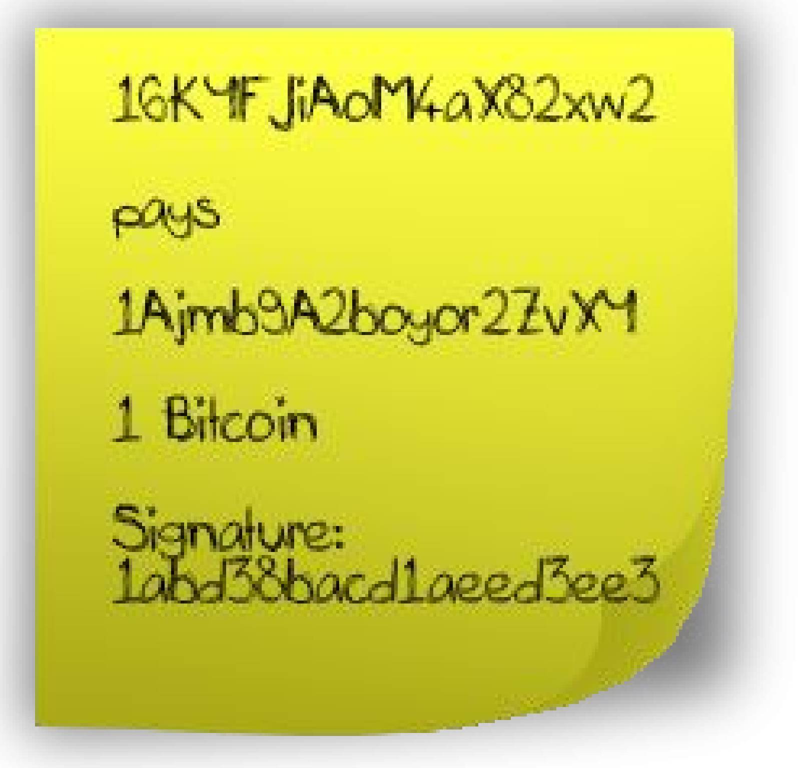
👍

Signed Transactions

Scott pays Alice
1 Bitcoin

Signature:
1abd38bacd1aeed3ee3

Signed Transactions



16K4FJiAoM4aX82xw2

pays

1Ajmb9A2boyor2ZvX4

1 Bitcoin

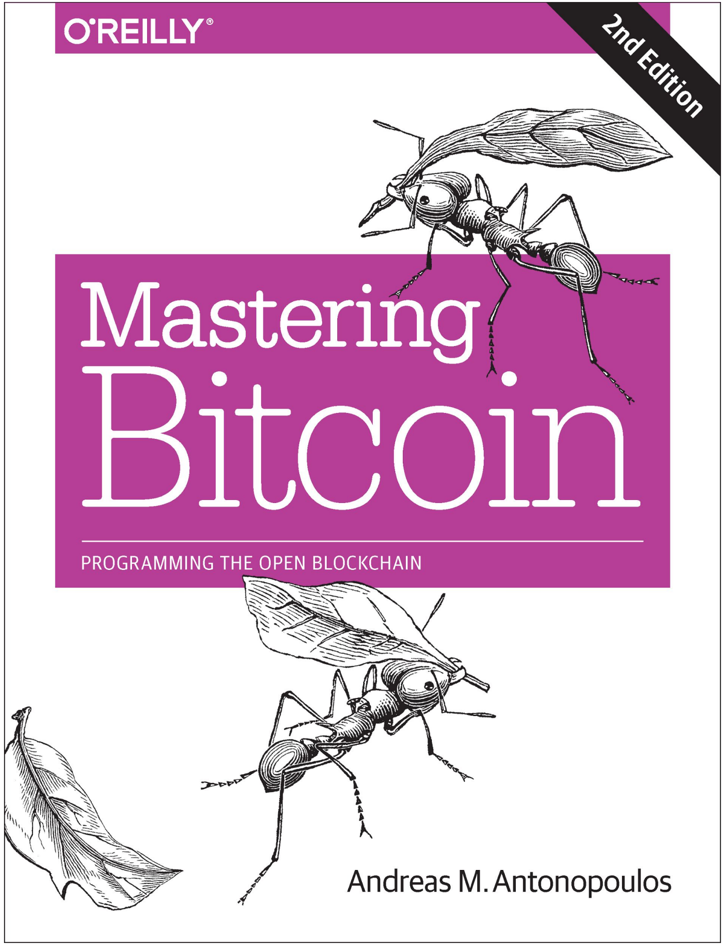
Signature:
1abd38bacd1aeed3ee3

Digital Signature Functions

createSignature(message, privateKey) => signature

checkSignature(message, signature, publicKey) = 👍 / 👎

- Demo - https://anders.com/blockchain/
- Bitcoin Explorer - https://blockexplorer.com
- Ethereum Explorer - https://etherscan.io/



O'REILLY

2nd Edition

Mastering Bitcoin

PROGRAMMING THE OPEN BLOCKCHAIN

Andreas M. Antonopoulos

https://github.com/bitcoinbook/bitcoinbook - FREE