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
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
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 is a distributed system which implements a blockchain-based cryptocurrency

Ether is the name of the tokens used on the Ethereum network
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)
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
Once
Again
Their
My
A
Oncey McOnceFace
<table>
<thead>
<tr>
<th>Block 0 Once</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word: &quot;Once&quot;</td>
</tr>
<tr>
<td>Parent: None</td>
</tr>
</tbody>
</table>
Blockchain Strategy

<table>
<thead>
<tr>
<th>Block 0 Once</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word: “Once”</td>
</tr>
<tr>
<td>Parent: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block 1 Upon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word: “Upon”</td>
</tr>
<tr>
<td>Parent: “Block 0 Once”</td>
</tr>
</tbody>
</table>
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

Once

There

Upon

Their

Once

Again

My

Oncey McOnceFace

A
Recess Strategy

Once Upon Their Block 1

There Oncey McOnceFace

Oncey McOnceFace

Upon My Block 1

My Block 1 Again

A Block 1

A Block 1
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 A
- Word: “A”
- Parent: “Block 1 Upon”

Block 2 Review
- Word: “Review”
- 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
Once

Block 1 Upon
Word: “Upon”
Parent: “Block 0 Once”
Solution: 5918

Block 2 A
Word: “A”
Parent: “Block 1 Upon”
Solution: 2074

Once

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

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

Balances:
- Eve: 0 BTC
- Alice: 1 BTC
- Bob: 0 BTC
Double Spend

<table>
<thead>
<tr>
<th>Block 13</th>
<th>Block 13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent: “Block 12”</td>
<td>Parent: “Block 12”</td>
</tr>
<tr>
<td>TX:</td>
<td>TX:</td>
</tr>
<tr>
<td>Eve -&gt; Alice 1 BTC</td>
<td>Eve -&gt; Bob 1 BTC</td>
</tr>
<tr>
<td>Solution: 290571</td>
<td></td>
</tr>
</tbody>
</table>

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
Crypto[graphy] currency
Crypto[graphy] currency

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).

Scott's Public Key

1549d7cca121
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
Scott pays Alice
1 Bitcoin

Signature:
1abd38baced1aeed3ee3
Signed Transactions

16K4FjiAoM4ax82xw2
pays
1Ajmb9A2boyor2ZvX9
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/