



An introduction to bitcoin,  
the blockchain, and cryptocurrency



# Overview

- About myself
- What is Bitcoin, Cryptocurrency?
- Breaking it down into layers
- Explore the blockchain
- Send some ether

# 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



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**



# Goals

- Holding Token
  - Blockchain resists change
  - Mining
- 
- Cryptography
  - Layers

*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



*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

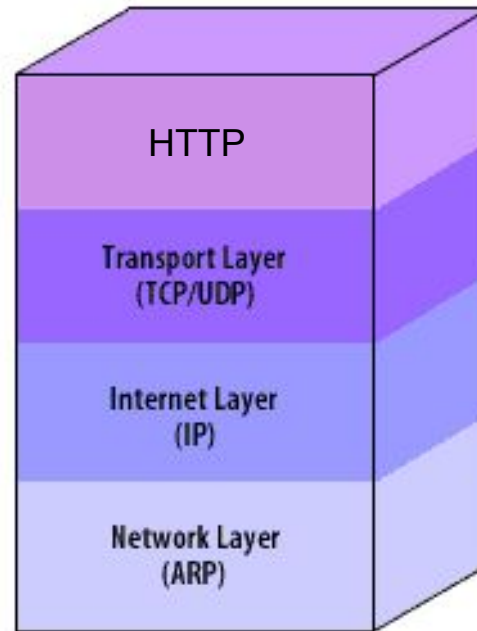


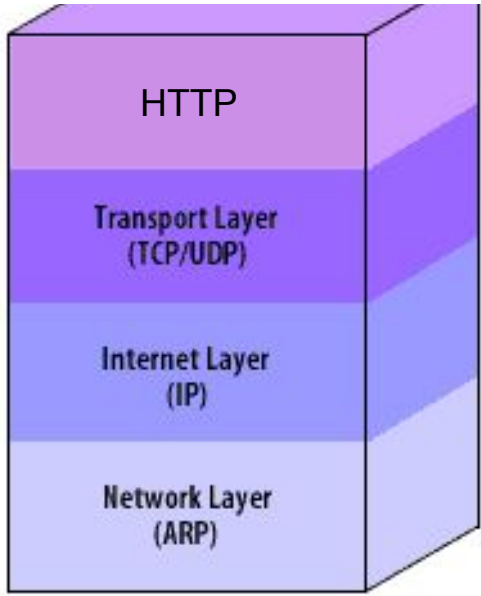
ethereum

# Cryptocurrency

Digital asset designed to work as a medium of exchange using cryptography to secure the transaction

## TCP/IP Protocol Layers





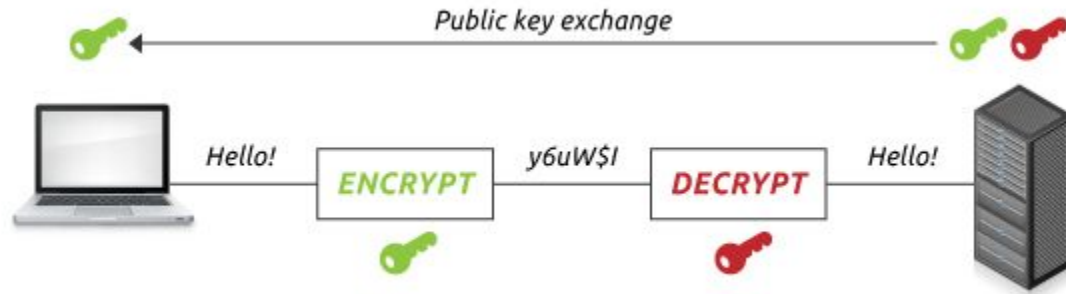
Signed Transactions

Blocks

Blockchain

Mining

# Crypto[graphy] currency





# Crypto[graphy] currency



# 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

# just love  
blueberries

Sig: db01c4a4

Scott pays Alice  
1 Bitcoin

Signature:  
1abd38bacd1aeed3ee3

16K4FJiA0M4aX82xw2

pays

1Ajmb9A2boyor2ZvX4

1 Bitcoin

Signature:

1abd38bacd1aeed3ee3

# Digital Signature Functions

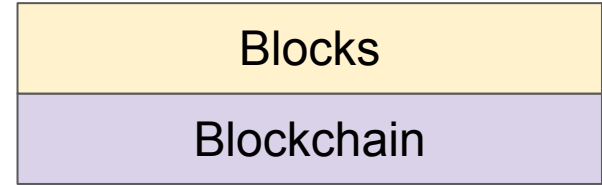
`createSignature(message, privateKey) => signature`

`checkSignature(message, signature, publicKey) =`  / 

Where do we put them?



# Blockchain



continuously growing list of records, called blocks, which are linked and secured using cryptography

Blocks

Blockchain

- 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

