Blockchain

Some slides from Joseph Bonneau, Eric Wustrow
Some technical content from “The Economics of Bitcoin, or Bitcoin in the Presence of Adversaries”

Slides by Andrew DeOrio

Blockchain

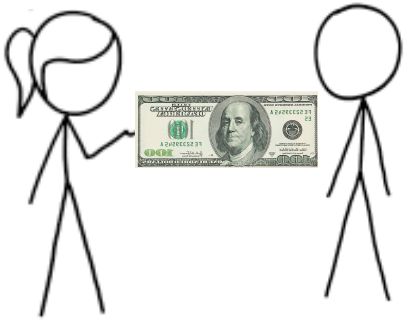
- *Blockchain* is a distributed store of information with no central authority
- Many uses for a blockchain
- Bitcoin cryptocurrency was the first

How to buy something in USD

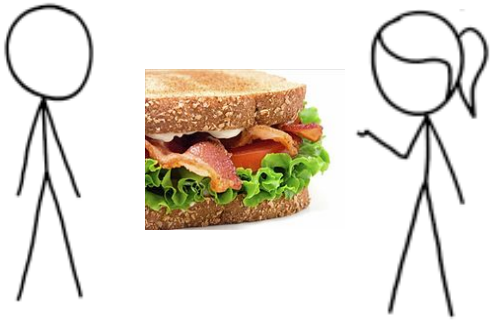
1. Alice goes to the bank and gets cash

2. Bank decreases the balance in Alice's account. Basically a single, big spreadsheet.

3. Alice gives cash to Bob



4. Bob gives sandwich (or whatever) to Alice



5. Bob goes to bank, deposits cash

6. Bank increases the balance in Bobs's account.

Stick characters from xkcd.com

How to buy something in USD

1. Alice gives card to Bob

2. Credit card company decreases the balance in Alice's account.

3. Credit card company increases the balance in Bob's account.

Stick characters from xkcd.com

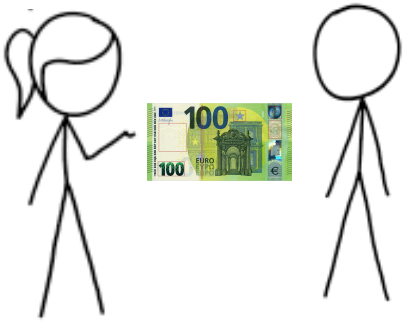
How to buy something in EUR

1. Bank goes to a currency exchange. Sells USD, buys EUR.

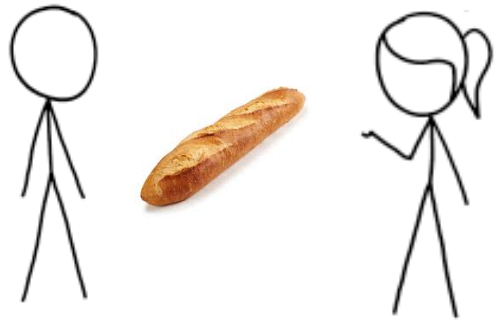
2. Alice goes to the bank and gets EUR cash.

3. Bank decreases the balance in Alice's account. Basically a single, big spreadsheet.

4. Alice gives cash to Bob



5. Bob gives baguette to Alice

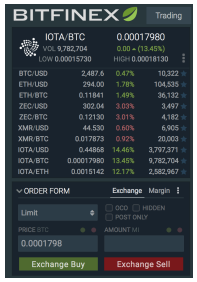


etc.

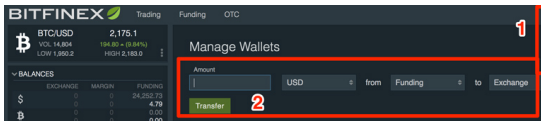
Stick characters from xkcd.com

How to buy something in BTC

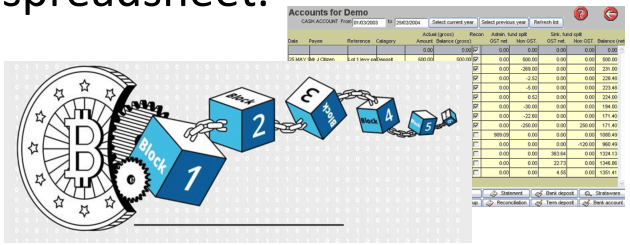
1. Alice goes to a bitcoin exchange. Sells USD, buys BTC.



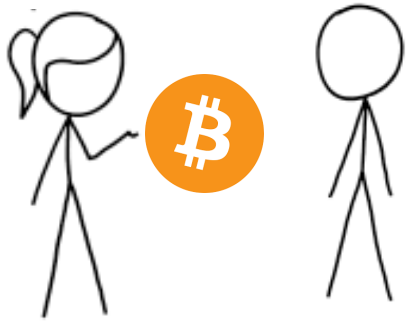
2. Bitcoin exchange puts digital currency in Alice's digital wallet.



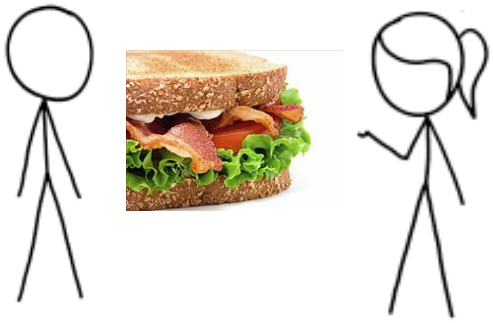
3. Blockchain increases the balance in Alice's wallet. Basically a *distributed* spreadsheet.



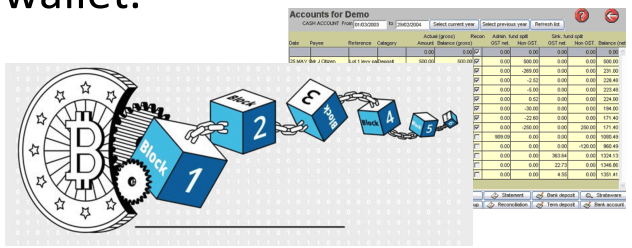
4. Alice gives BTC to Bob



5. Bob gives sandwich to Alice



6. Blockchain decreases the balance in Alice's wallet and increases the balance in Bob's wallet.

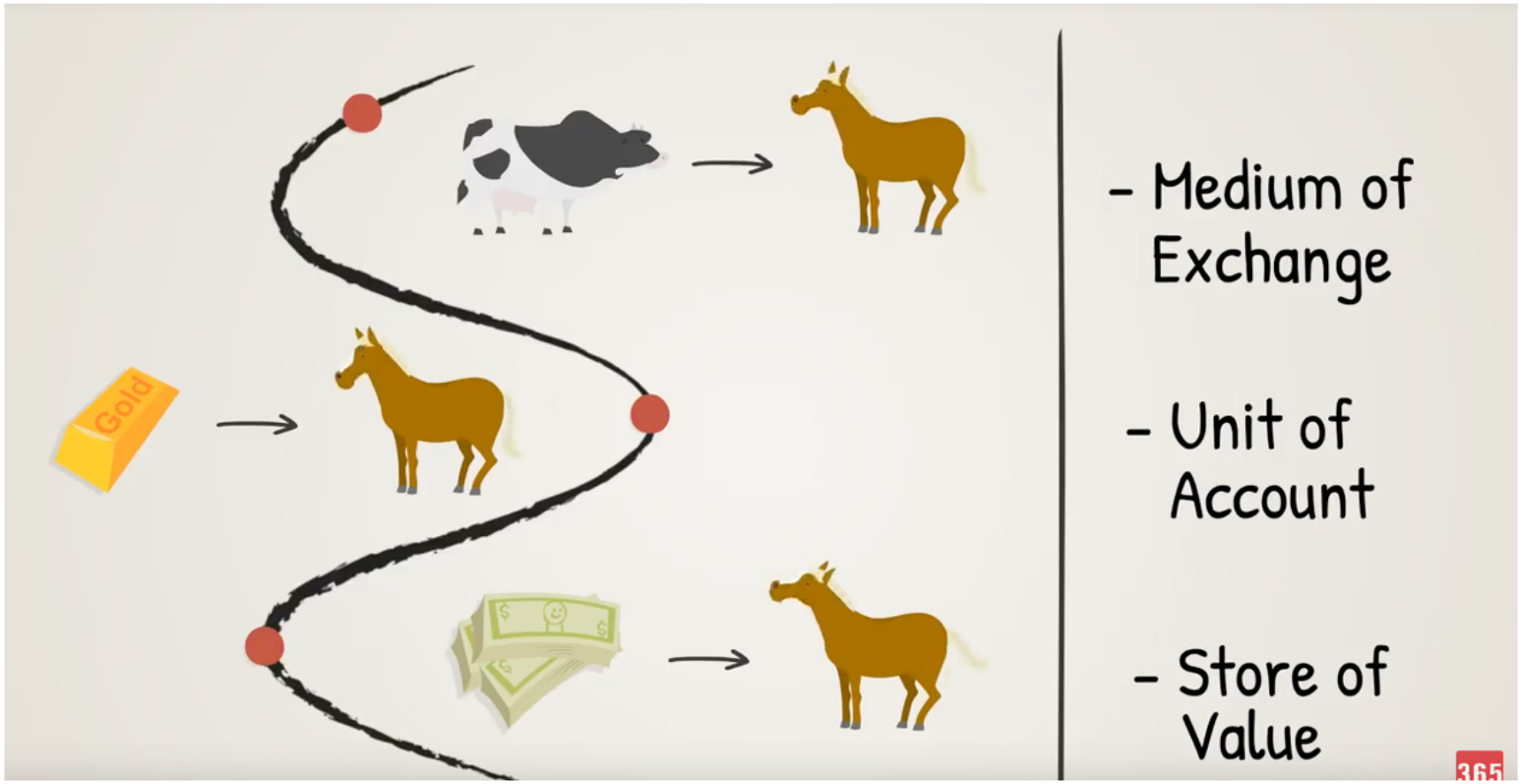


Stick characters from xkcd.com

Agenda

- **Background: currency crash course**
- Bitcoin
- Blockchain
- Mining
- Altcoins
- Summary

Brief history of money



https://www.youtube.com/watch?v=kU6NaDs-7ww&t=5

Stop about half way, before examples of countries

Traditional currency

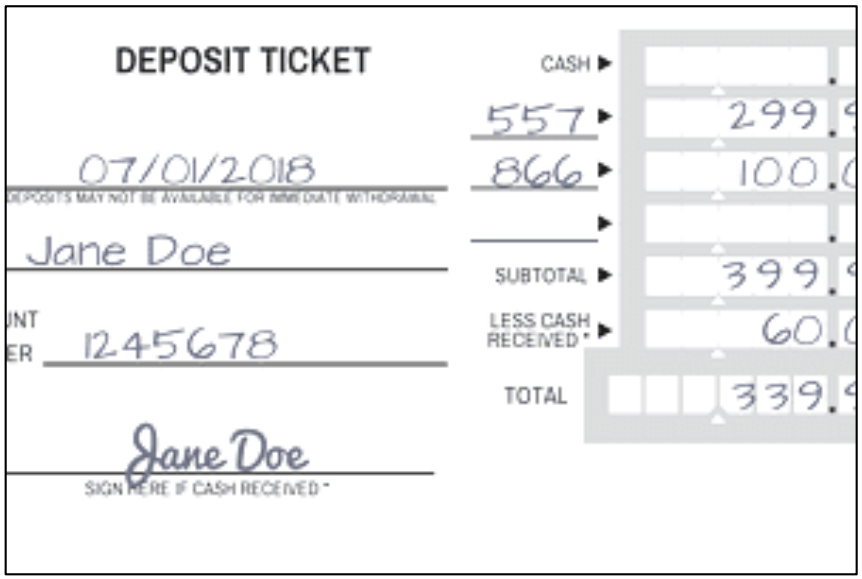
- What is money?
- *Currency* is a medium of exchange
- A convenient way to buy and sell stuff
  - Easier than bartering "I'll fix your laptop if you give me one dozen eggs."
  - Easier than carting around Gold bullion

Fiat currency

- *Fiat money* is a currency without intrinsic value
- Often created by government regulation
- It's valuable because two parties agree it has value

Digital currency

- *Digital currency* is currency available in digital form
- Example: Bank deposit
  - After deposit, the money exists only as a number on the bank's balance sheet
  - You can spend it by transferring it, e.g., to pay a credit card bill



Central bank

- In the U.S., the central bank is the Federal Reserve
  - "Fed" for short
- Decides how much money exists, e.g., when to print money
- Bank used by banks
  - Lends money to banks
- Another digital currency example: central bank reserve
  - Money exists as a number on the central bank's balance sheet

Central bank

- A central bank is centrally controlled
- Example: the U.S. controls how much U.S. Dollars are worth AKA how many there are
- If the Fed wants more dollars, the Fed can print more
  - Print more dollars. Don't even need to print them. Just increase the number on the balance sheet.
  - *Quantitative easing*

Agenda

- Background: currency crash course
- **Bitcoin**
- Blockchain
- Mining
- Altcoins
- Summary

Bitcoin

- Bitcoin is a decentralized digital currency
- First cryptocurrency
- First to solve the digital currency “double spending” problem
- Mix of cryptography, distributed systems, and game theory

Bitcoin

Bitcoin is also ...

- A get-rich-quick scheme
- A fiat currency without a government behind it
- A handy resource for criminals
- The future of money… maybe?

Satoshi Nakamoto

- Bitcoin was invented in 2008 by an unknown person or persons using the Satoshi Nakamoto
- *Bitcoin: A Peer-to-Peer Electronic Cash System* posted to a cryptography mailing list
- 2009 opensource bitcoin code released
- Nakamoto mines the Genesis Block
- 2010 Nakamoto disappears after mining about 1,000,000 BTC

Gov't backed currency vs. Bitcoin

Government backed

- Analog and digital
- Fiat currency
- Centralized
  - Controlled by a central bank
  - Represented by a single bank ledger

Bitcoin

- Digital
- Fiat currency
- Decentralized
  - Controlled by a distributed algorithm
  - Represented by shared ledger

Bitcoin basics

- A Bitcoin is an information object that represents value
- It's represented as a chain of digital signatures over the transactions that the Bitcoin participated in
- Owner of a Bitcoin is a Bitcoin address, which is a public key (AKA *Bitcoin Wallet*)
  - The human owner is whoever has the corresponding private key
- The owner of a Bitcoin creates a transaction by signing a statement that describes transfers ownership from one Bitcoin address to another

Spending Bitcoin

- Alice pays Bob
- Alice broadcasts the transaction to all Bitcoin nodes
- All nodes must agree on a sequence of transactions
- Sequence is *Blockchain*
- Process of agreement is *Bitcoin mining*

signed by Alice

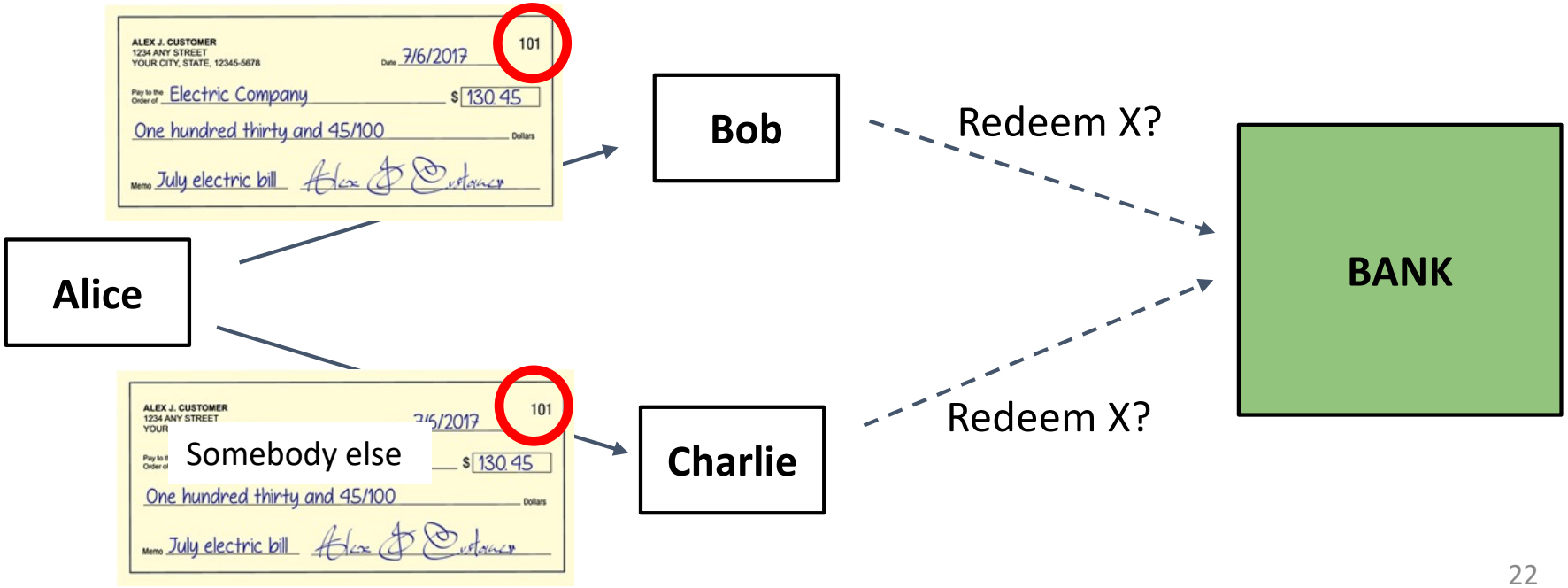
Pay to pk_{Bob} : H( )

Agenda

- Background: currency crash course
- Bitcoin
- **Blockchain**
- Mining
- Altcoins
- Summary

Double spending

- In US, ACH system prevents double spending

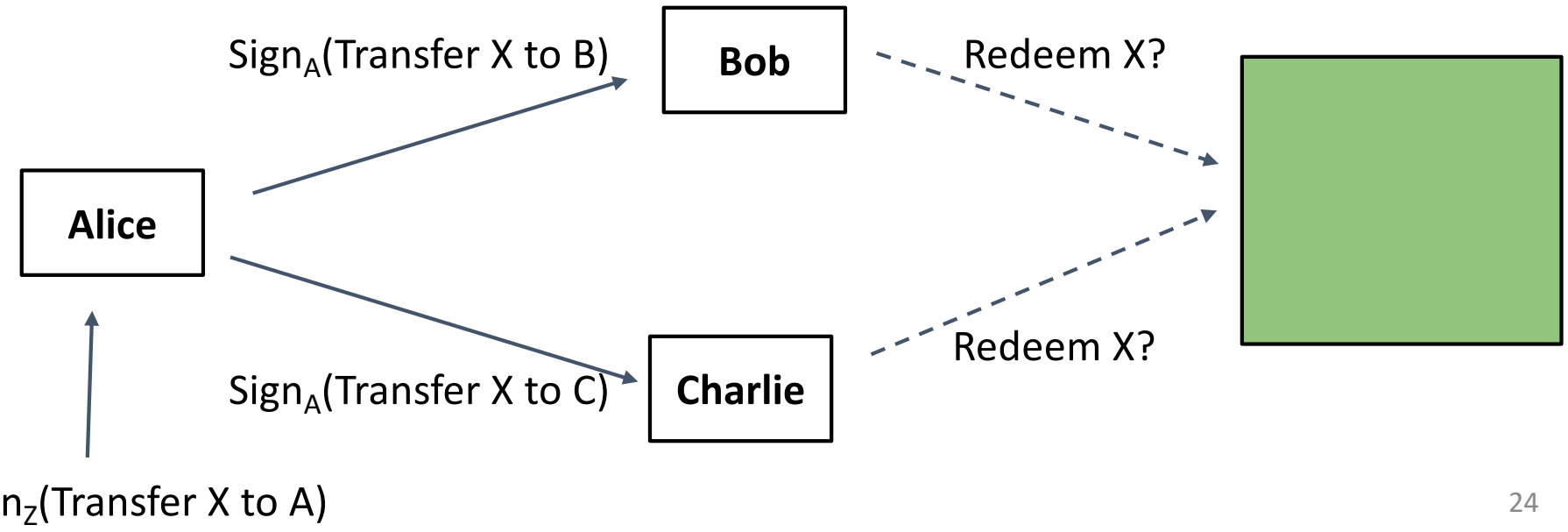


Double spending

- With traditional banking, avoid double spending by checking the account's balance
  - Centralized balance sheet
- ACH system for transferring money
  - Verify identity of the sender and recipient bank
  - Verify account amounts
  - Federal Reserve runs network

Double spending

- If you receive a Bitcoin, you can cryptographically verify the signatures
- But how can you verify that no double-spending took place?



Distributed ledger

- Distributed alternative to bank's centralized balance sheet
- Bitcoin participants engage in peer-to-peer protocol that shares transaction data
- They collectively build a log of every Bitcoin transaction, ever
- The log is built from *blocks*

Distributed ledger

- Blockchain is essentially a distributed database with a shared protocol for multiple writers who don't trust each other or a central authority.

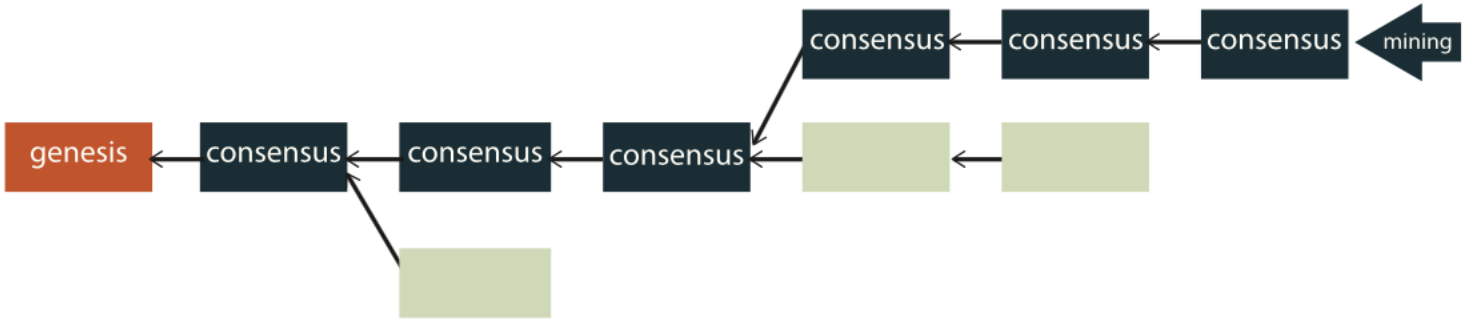
- Blockchain useful when
  - Database is shared with multiple writers
  - Users don't trust each other
  - Users don't trust a central authority

Blocks

- Each block has:
  - A sequence id
  - A timestamp
  - A nonce
  - Cryptographic hash of the previous block
  - Various metadata fields
  - Some actual transactions!

Blockchain

- Blocks connected in a *blockchain*
- There's always a backward hash link; eventually you can traverse it all the way back to the "genesis block"
- The set of blocks form a tree, with the genesis block at the root; possibly multiple branches



The blockchain in action

- Suppose Alice wants to give Bitcoins to Bob
- Alice creates and signs a transaction object that transfers the Bitcoin from herself to Bob
- She sends it to all peers in a peer-to-peer network
- The peers rebroadcast it, so soon, everyone knows about the transaction
- Any participant who also mines on the blockchain can now attempt to create a block that contains all the transactions known (including Alice's transfer)
- If this works, then the Alice-> Bob transfer is added to the global shared log of transactions

Agenda

- Background: currency crash course
- Bitcoin
- Blockchain
- **Mining**
- Altcoins
- Summary

Motivating Bitcoin miners

- Who runs the distributed ledger?
- *Bitcoin miners* are paid to operate the blockchain
  - Run servers
- Block creator is allowed to insert some **reward** Bitcoin transactions
- This is how miners earn Bitcoins, and how Bitcoins are created

Blockchain

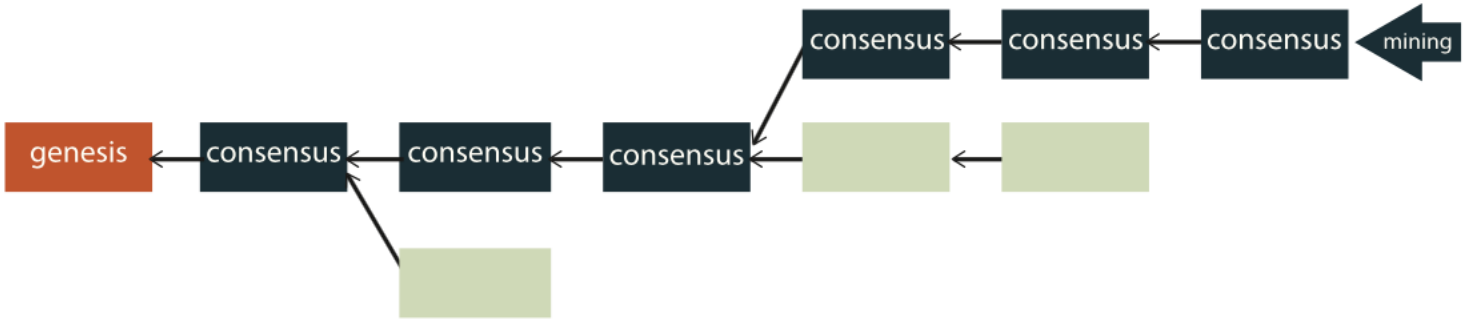
- Bitcoin design decisions focus on building and maintaining a blockchain that is agreed-upon
- Why only reward blocks added to the consensus branch?
- Encourages miners to focus on achieving consensus

Bitcoin consensus

- Transactions are broadcast to all nodes
- In each round a random node signs a block of new transactions, including the hash of the previous block
- Other nodes accept the block if all transactions are valid
- Invalid blocks are ignored, next node repeats this block
- Longest chain is considered canonical
- Leads to a valid canonical chain with “honest majority”

Mining the blockchain

- Anyone can become a **miner**, and mine new blocks to add to the blockchain
- Why does a new block have to be mined?
  - Remember the nonce?
  - The block is only valid if the the hash of the block is under a target value

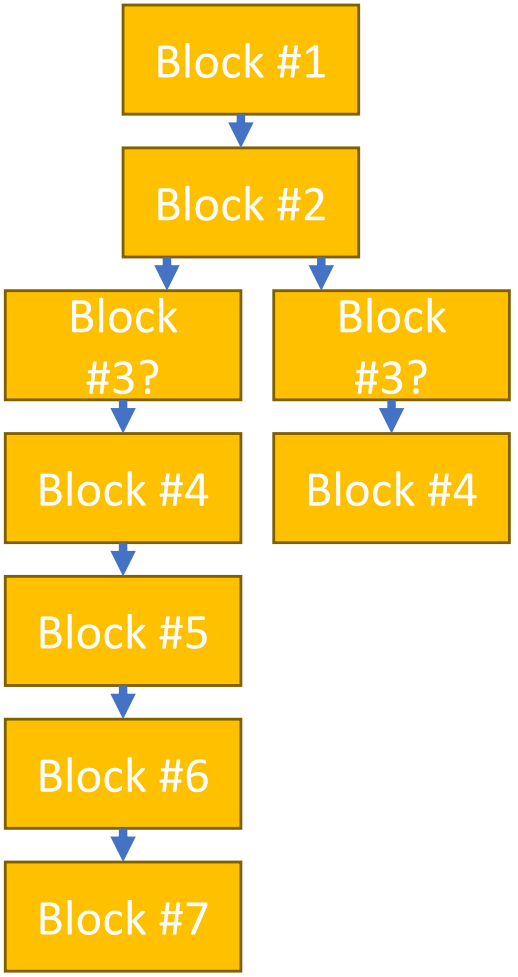


Proof-of-work

- Formulating a block is a **proof-of-work** puzzle: hard to compute, easy to validate
- A solution is evidence you have done some amount of work
- The target value can be adjusted to make a block harder or easier to mine; tuned for 10 mins

Blockchain forks

- What if two miners find the next block at the same time?
- The branch with more computational power will grow more quickly
- Bitcoin says that only the longest chain should be treated as valid
- Eventually, one chain wins!
  - Or a fork is maintained and a new cryptocurrency is born
  - A fork means different versions of the transaction history and potentially different versions of ownership

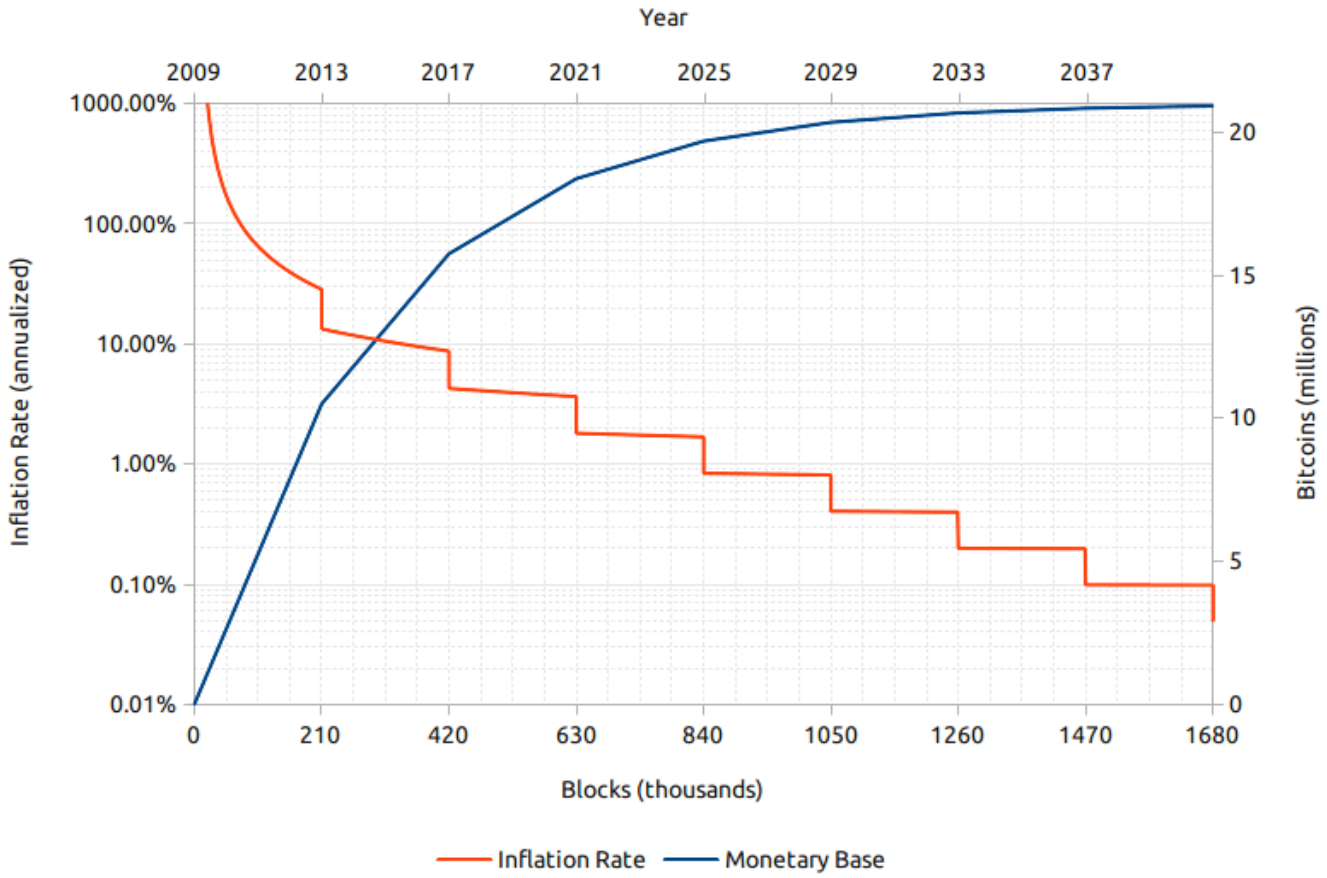


Blockchain

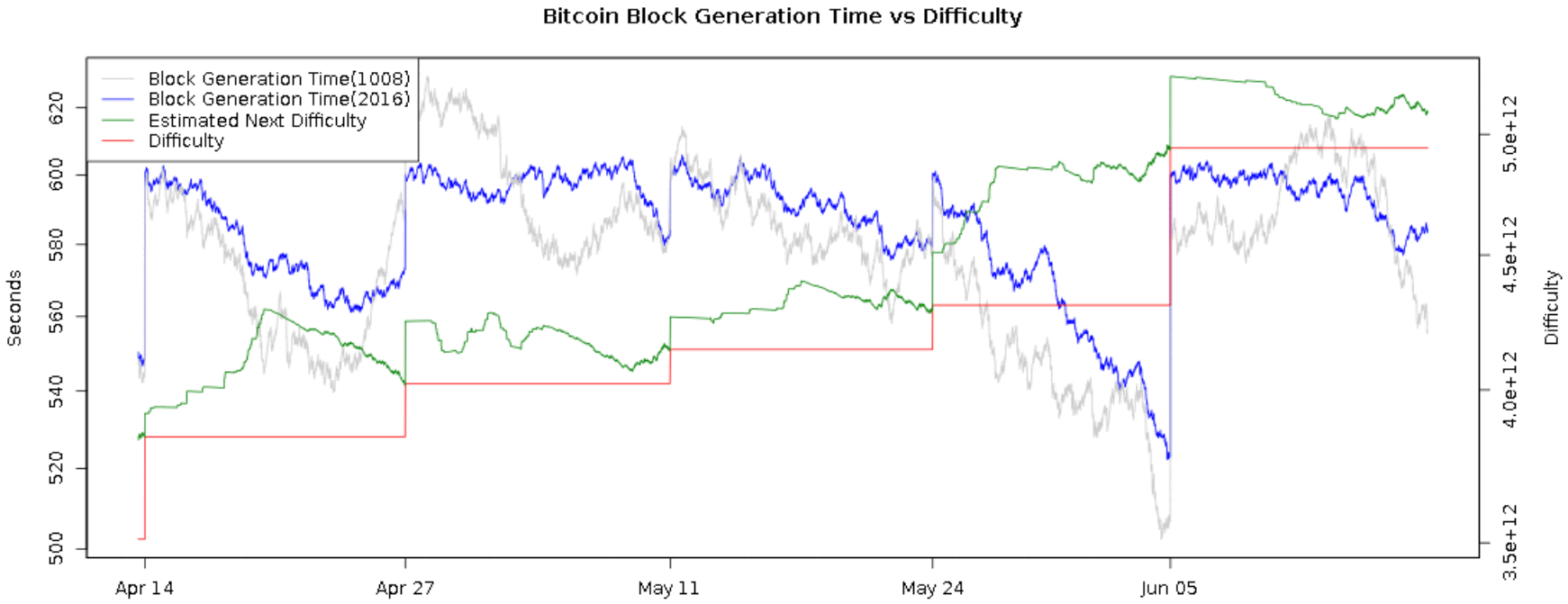
- Why give miners such strong incentives to formulate blocks?
  - Bring more hashing power online
    - Reduces anyone's ability to forge an alternate history blockchain
  - You can start to ignore transactions if you control 51% of the hashing power

Bitcoin reward function

- Block reward halves every ~4 years



Block creation difficulty adjustment



Energy consumption

- Current estimates: ~70 TWh / yr
- Enough to power ~7 million households
- Hardware is changing
  - Mining equipment: anything from normal CPU -> dedicated ASIC datacenter
- Power generation is changing
  - Coal, natural gas, wind, solar, hydroelectric

Source: https://digiconomist.net/bitcoin-energy-consumption

Bitcoin mining hardware

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card

The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

THE LEOPARD

DETAILS :

- **2,5 TH/s**
- Dimensions: 15“ x 13.3“ x 13.7“ (38cm x 34cm x 35cm)
- 28nm ASIC technology
- Silent Cooling
- In-built WiFi Connection (without Antenna)
- Less than 750 watt (0.3 per GH)
- 1 Year Guarantee
- $ 5.800

COMES WITH :

1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

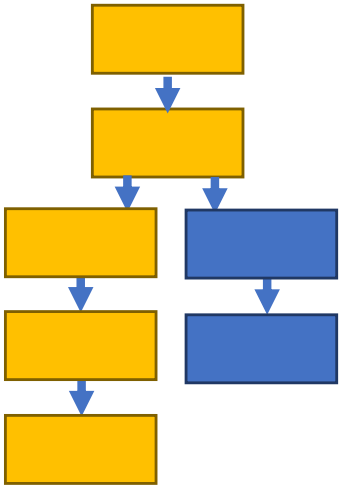
SHIPPING :

- Worldwide, Express
- Included in the price
- Available: 100 Units: Shipping April (Week 3)

Energy consumption

- Why make the task so hard? Why proof-of-work?
- It caps the rate at which new Bitcoins can be added
- In other words, prevents runaway inflation

Hard forks



- *Hard fork* one cryptocurrency becomes two
  - Shared partial history
  - Holders of original asset now have both assets
  - Often, sum of both asset prices exceeds original price
- Requires all nodes to upgrade protocol software
- Example: correct security risk

Agenda

- Background: currency crash course
- Bitcoin
- Blockchain
- Mining
- **Altcoins**
- Summary

Altcoins

- *Altcoins* are alternative cryptocurrencies, launched after Bitcoin
- Different blockchains offering different features
- Political and social motivations

Altcoins

Cryptocurrencies ▾ | Watchlist | USD ▾ | ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$115,958,700,822	$6,779.05	17,105,450	$3,899,810,000	0.40%	0.45%	6.05%
2	Ethereum	ETH	$53,749,221,582	$536.41	100,201,565	$1,603,770,000	0.38%	0.09%	12.04%
3	Ripple	XRP	$21,143,682,612	$0.538757	39,245,304,677 *	$257,288,000	0.25%	-1.56%	0.88%
4	Bitcoin Cash	BCH	$15,311,968,314	$890.51	17,194,625	$431,488,000	0.38%	-0.83%	5.34%
5	EOS	EOS	$9,314,308,977	$10.39	896,149,492 *	$852,903,000	-0.27%	-2.37%	2.89%
6	Litecoin	LTC	$5,582,662,691	$97.83	57,066,628	$260,778,000	0.15%	-0.87%	3.70%
7	Stellar	XLM	$4,319,794,720	$0.232133	18,609,136,658 *	$43,012,900	0.38%	-1.50%	3.87%
8	Cardano	ADA	$4,200,107,646	$0.161997	25,927,070,538 *	$83,806,800	0.37%	-1.89%	-0.10%
9	IOTA	MIOTA	$3,231,620,884	$1.16	2,779,530,283 *	$63,015,400	0.38%	-0.71%	-4.19%
10	TRON	TRX	$3,230,835,907	$0.049140	65,748,111,645 *	$399,997,000	1.31%	1.05%	18.40%
11	Tether	USDT	$2,610,633,914	$1.00	2,607,140,346 *	$2,216,500,000	-0.06%	-0.09%	-0.18%
12	NEO	NEO	$2,541,123,000	$39.09	65,000,000 *	$74,580,700	0.36%	-1.68%	1.01%
13	Dash	DASH	$2,160,268,318	$265.24	8,144,641	$93,661,600	0.13%	1.38%	6.32%
14	Monero	XMR	$1,982,013,017	$122.72	16,150,824	$33,497,200	0.49%	-2.73%	0.78%
15	Binance Coin	BNB	$1,828,332,771	$16.03	114,041,290 *	$65,433,400	-0.22%	-3.74%	10.02%
16	NEM	XEM	$1,752,723,000	$0.194747	8,999,999,999 *	$13,929,200	0.48%	-1.48%	1.54%
17	Ethereum Classic	ETC	$1,723,159,622	$16.82	102,443,410	$342,631,000	2.40%	8.91%	22.06%

Cryptocurrency exchange

- A cryptocurrency exchange allows customers to
  - Trade different cryptocurrencies
  - Exchange cryptocurrency for conventional currency

- Examples: Poloniex, Bitfinex

Different blockchain features

- One reason to create a different cryptocurrency: different blockchain with different features
- Alternative proof of work
- Faster block times / larger block sizes
- Alternative transaction types
  - Computable “smart contract” transactions
  - Anonymous / Private transactions

Political and social motivation

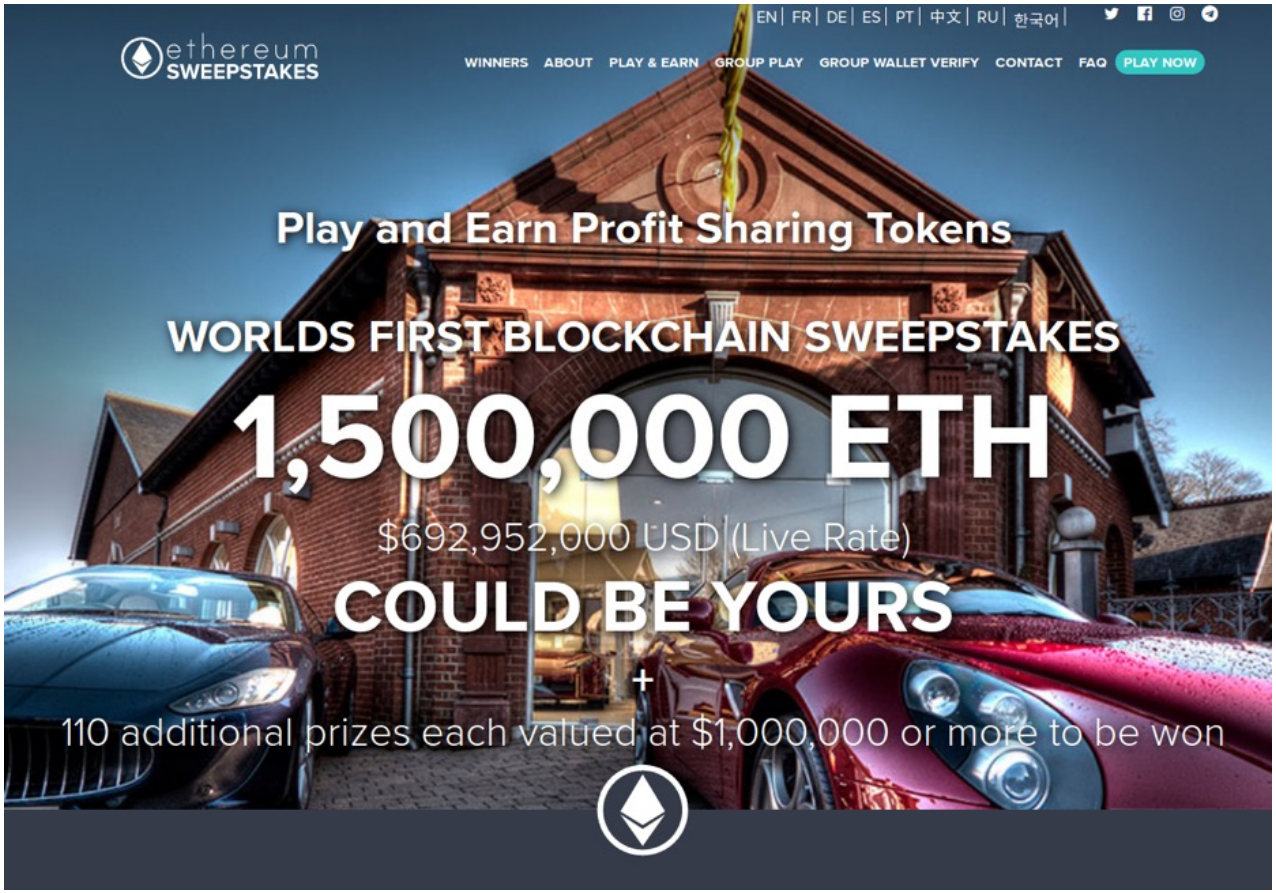
- Another reason to create a different cryptocurrency: political and social motivations
- Forks of existing cryptocurrencies
- Big disagreements over small block vs. large block

Ethereum

- Decentralized virtual machine
  - “Smart contracts”
- Transactions can:
  - Move money (ETH)
  - Create new contracts (virtual machines)
  - Update state in existing contracts
- Contracts can:
  - Send money (ETH)
  - Interact with other contracts

Ethereum lotteries

- Example smart contract: automated lottery



Ethereum lotteries

- Contracts that create a **decentralized lottery**
- Players pay cryptocurrency directly to contract
- Fraction of winners receive payout
  - Often lottery contract creator also receives a “fee”
- Technical questions:
  - How are winners selected?
  - Are winners paid directly from contract or indirectly from owner?

Example Ethereum smart contract: DAO

- DAO: Decentralized Autonomous Organization
- Allow investors to directly vote on projects to be funded collectively
  - Send ETH to contract in exchange for DAO tokens
  - Projects are proposed
  - DAO token holders vote on which projects to fund
  - Projects receive collective funding (ETH)
- Collected over 11 million ETH (~$150 million USD)
  - Attacker discovered bug in smart contract
  - Stole 3.6 million ETH (~$50 million USD)

DAO fallout

- Disagreement over what to do
- Option 1: Revert changes, return money to investors (requires a “hard fork”)
  - Needs collective consensus from miners and other participants
  - Attacker does not get to keep money, DAO victims made whole
- Option 2: Code is law, investors should suffer the consequences of a bug
  - Attacker keeps stolen money
  - Everyone learns a valuable (and expensive!) lesson

DAO fallout

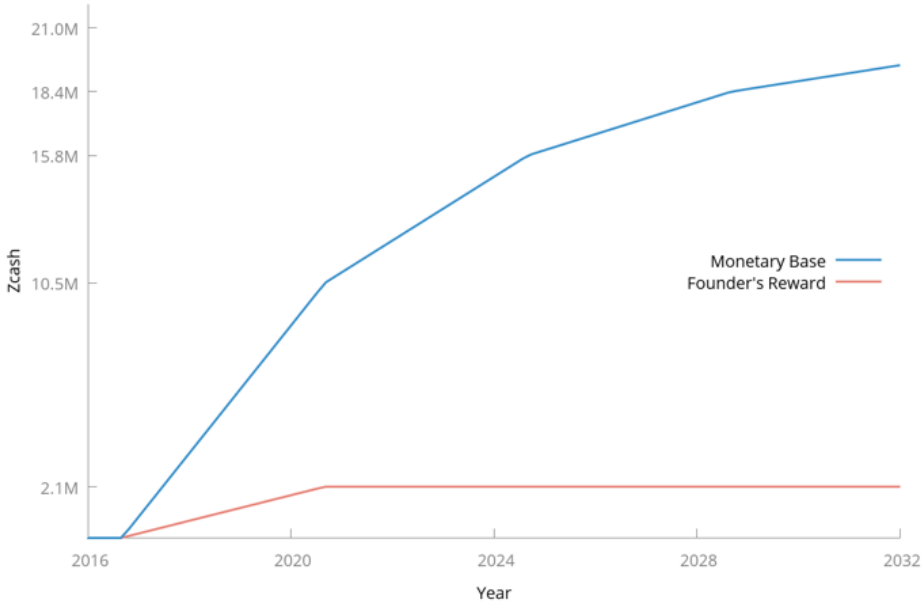
- And then there were two:
- Ethereum (ETH) reverted the change and hard forked the cryptocurrency
- Ethereum Classic (ETC) continued on the existing chain
  - Attacker keeps ETC

Initial Coin Offering (ICO)

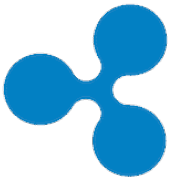
- Crowdfunding via token sales:
  - Project launches token sale (usually through an Ethereum contract)
  - Investors pay ETH in exchange for tokens
  - Project uses ETH to fund development
  - Tokens are then used for:
    - Dividend payments
    - Investment returns
    - Exclusive access, etc

Premined cryptocurrencies

- Creators (and friends) privately mine new currency prior to release
- Publicly announce blockchain with first blocks already mined
- Alternative approach: Build “Founders reward” into protocol (ala Zcash)



Ripple



- “Web of trust” consensus
- Allows settlement of any currency/assets
- Also has a “native” digital asset: XRP
- XRP distribution: developers start with all the money (100 billion XRP)
  - Still retain a large fraction
- Recently sued for alleged sale of unregistered security (XRP)

Agenda

- Background: currency crash course
- Bitcoin
- Blockchain
- Mining
- Altcoins
- **Summary**

Reasons for cryptocurrencies

- Distrust in centralized banks or governments
- Predictable policy
  - Code and protocols instead of malleable laws
- Removing financial gatekeepers

Reasons against cryptocurrencies

- Should we trust anonymous people on the Internet?
- What about bugs in code?
- Does replacing financial gatekeepers with code mean that things will never change?
- Large power consumption causes environmental concerns

Blockchain summary

- A distributed database with a shared protocol for multiple writers who don’t trust each other or a central authority
- Blockchain useful when
  - Database is shared with multiple writers
  - Users don’t trust each other
  - Users don’t trust a central authority
- Cryptocurrency is just one way to use a blockchain