Overview of Cryptocurrencies

by John & Harrison

Pitt Crypto

Pizza Sponsor

- https://lucylabs.io/
- Cryptocurrency Merchant Bank

1 Bitcoin (2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

"In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions." – **Nakamoto, 2008**

Whitepaper: https://bitcoin.org/bitcoin.pdf
Source: https://github.com/bitcoin/bitcoin

Bitcoin main ideas

- Transactions without a 3rd party
- Replacing **trust** with **cryptographic proof**
- Blockchain + proof-of-work (PoW)

Bitcoin vs. Blockchain

- Blockchain is a technology used to create an **append-only database** across a network of **untrusted nodes**

- Bitcoin *uses* blockchain technology to create an **append-only database** of **transactions**
  - Transaction changes ownership of bitcoins

Price history

2 Bitcoin Derivatives

Litecoin

- Larger total supply (84 million LTC vs 21 million BTC)
- Faster block time (2.5 minutes vs 10 minutes)
- “ASIC-proof” hashing algorithm (Scrypt vs. sha256)

Source: https://github.com/litecoin-project/litecoin

Namecoin

- Decentralized DNS with Bitcoin
- Never really took off

Source: https://github.com/namecoin/namecoin-core

Web: https://namecoin.org/

Primecoin

- Replace proof-of-work with a method that looks for prime numbers
- Cunningham chains and bi-twin chains

Paper: http://primecoin.io/bin/primecoin-paper.pdf

Web: http://primecoin.io/

Dogecoin


NOT ALWAYS SUCH INTERESTING,
BUT WHEN AM
WOW

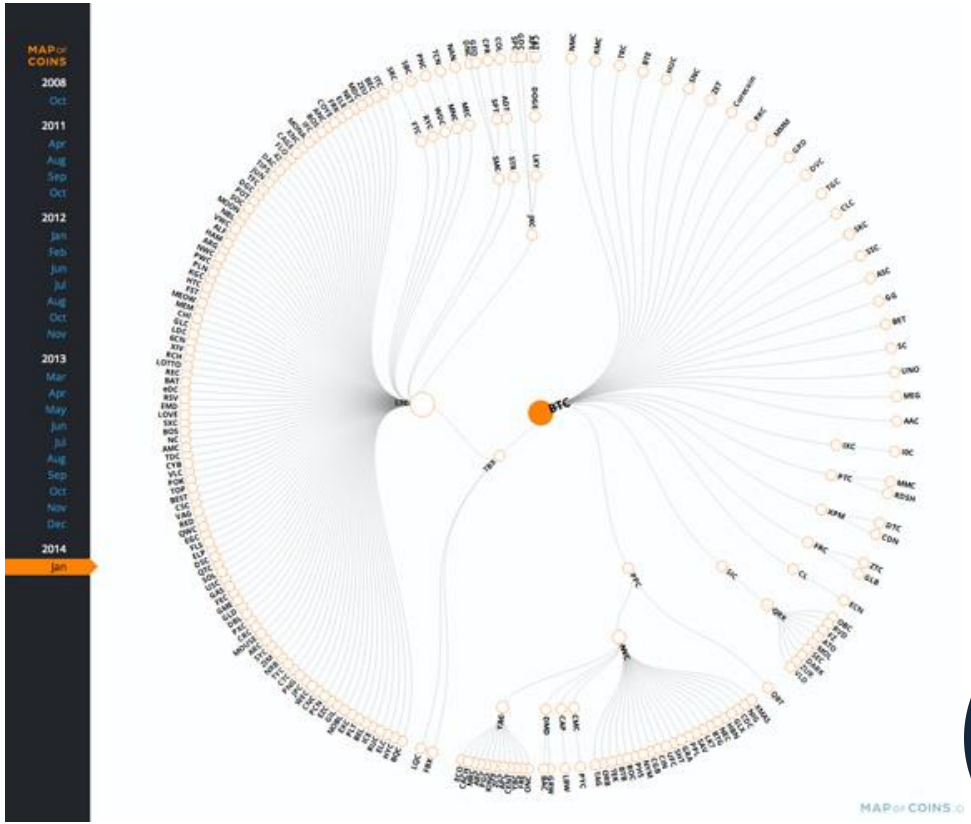

wow
such doge
much meme
very internets
so currency
many popular

Dogecoin Fundraising

Many more derivatives

http://mapofcoins.com/

see a visualization of coin hierarchy



3 Buying/Selling/Using/Investing

Cryptocurrency is not a Safe Investment!

- Reasons you should NOT invest
  - “Bitcoin is a cash machine”
  - “Bitcoin generates coins out of thin air = FREE MONEY $$$”
  - “If I invest in Bitcoin, I will get a Lambo”
- You must think of “investing” in cryptocurrencies as gambling
- Bitcoin, and most other cryptocurrencies, are backed by nothing and are given a value based upon only what other people think it should be worth
- The real value in all these cryptocurrencies is the technology (blockchain, smart contracts, etc.) to which we will discuss much more of in this club

How to Obtain a Bitcoin

1. Have a friend send you bitcoin
2. Mine your own bitcoin (or join a mining pool)
3. Meet up with someone at localbitcoins.com
4. Go to a bitcoin ATM
5. Register at an exchange and buy bitcoin through them

Requirements to Obtain a Bitcoin

- You must have a wallet with an address (public key) and the wallet or you must know what the secret key is
- You must have someone willing to send you bitcoin
- The transaction then must be broadcasted to the bitcoin network, where it will stored in the mempool until a miner puts it into a block

Getting a Bitcoin through an Exchange

- To start exchanging USD to Bitcoin, you need an exchange that accepts USD for Bitcoin
- 2 Most popular US exchanges for buying Bitcoin: Coinbase and Gemini
- To be able to register on these exchanges, you will need at a minimum a valid US I.D.
- Once you have bitcoin, it becomes easy to exchange it for other cryptocurrencies
- The most popular altcoin exchange is Binance

How to Track a Cryptocurrency's Value

- Most popular website is https://coinmarketcap.com/
  - Price of each coin is a volume weighted average of all prices reported at each market
- Other Websites to track Cryptos
  - https://coincodex.com/
  - https://coinranking.com/
  - https://www.cryptocompare.com/
- Market Cap of each coin is a way of ranking the relative size of each cryptocurrency
  - Formula: Market Cap = Price X Circulating Supply
  - Example: Bitcoin's current price is $6,513.55 and its circulating supply is 17,265,975 BTC. What is its current market cap?
    - Market Cap = ($6,513.55)(17,265,975) = $112,462,733,935

Other Cryptocurrency Value Trackers

- Volume: Based on the average weighted price of the coin, how much is being traded (usually within a 24h timespan) on exchanges
- The higher the volume, the more stable the price of the coin will likely be
- The lower the volume, the more volatile the coin price will be
  - When trading, make sure to keep track of not just the price; the volume matters to
- Can you compare 2 coins based on price alone? Why or why not?
  - You can't because price is usually dependent on circulating supply. One coin may have a slightly lower price but a much higher supply, thus having more market cap
  - Market Cap and volume are the 2 best methods for comparing prices of coins

Reading the Charts

- Check all axes
  - Blue line represents Market Cap in this picture
  - Green line represents USD value per coin
- Check the timespan of the chart
- Make sure to check if the graph is Logarithmic or Linear
- “Past performance is not indicative of future results”
  - Cryptos are all new tech will few real world applications currently
  - Much more volatile than stocks

Bitconnect

- #1 Cryptocurrency Ponzi scheme to date
- It is a service where it takes your BTC, converts it to BCC, and it then pays you interest on their “trading robot”
- Interest is paid in BCC
- They claim interest rate of return is 1% per day
- The dev team behind Bitconnect pre-mined 4.8 million coins
- Proof-of-stake is used to reward people who held onto coins longer and to people with more coin

Many Cryptocurrencies are Scams

4 Smart Contract Platforms

Introduction to Ethereum

- 2nd most popular cryptocurrency (by market cap)
- Platform to develop **smart contracts**
- Designed by Vitalik Buterin

What the heck is a smart contract?

What the heck is a smart contract?

```
contract Mortal {
    /* Define variable owner of the type address */
    address owner;

    /* This function is executed at initialization and sets the owner of the contract */
    function Mortal() { owner = msg.sender; }

    /* Function to recover the funds on the contract */
    function kill() { if (msg.sender == owner) selfdestruct(owner); }
}

contract Greeter is Mortal {
    /* Define variable greeting of the type string */
    string greeting;

    /* This runs when the contract is executed */
    function Greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* Main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
```

Dumb Bytecode

Stored on the Ethereum blockchain

Users can interact (call functions) through transactions

EVM is turing complete

Benefits of Smart Contracts

- Immutable Code
  - once sent to the Ethereum blockchain the code cannot be edited (but the data can)
- Security
  - Smart contract is encrypted and distributed to many nodes in blockchain
- Speed
  - Can cut out the middleman, most processes will now be automated
    - Note: processing speed of code is very slow; the process, however, with no middleman can be significantly faster
- No 3rd Party Required!
  - Smart contracts are decentralized and do not require a lot of trust for an agreement to execute

If Smart Contracts Don't Require a 3rd Party and Are Fast, then are they Perfect?

- Smart contracts are far from perfect
- Most use cases require relying on information from an external event
- Smart contracts, to pull external data, have to have nodes that reach an identical state due to consensus rules
- Problem is the external data source can change its response between requests of different nodes - no longer consensus
  - Can be fixed with an Oracle that pushes data to the blockchain instead of a smart contract pulling data
- Great article that addresses Ethereum smart contract misconceptions
  - https://www.coindesk.com/three-smart-contract-misconceptions/

Oracles

- A 3rd party that pushes data to the blockchain
- Helps ensure all nodes receive the same data
- Oracles will be discussed more in depth in a later meeting
- Good source to learn about oracles : https://blog.oraclize.it/understanding-oracles-99055c9c9f7b

More Smart Contract Negatives

- Human Error
  - If humans mess up the code in smart contracts, it cannot be changed once sent to the Ethereum blockchain
- Uncertain Legal Status
  - Smart contracts are not currently regulated by any government. Smart contracts may have to change
- Costs Real Money to Implement
  - Every smart contract sent to the Ethereum blockchain is paid with real money
  - Continuously making new Smart Contracts are expensive
  - Updating data to the Ethereum blockchain costs real money in the form of Gas too,
  - Must make sure to be as efficient with Gas as possible

Case Study of Coding Error: The DAO

- Stands for Decentralized Autonomous Organization
- Entity that operated on smart contracts
- All financial transactions and Rules were encoded on Blockchain
- One of the biggest crowdfunds ever
  - Raised 12.7 M Ethereum (One point worth over $250 million)
- Platform allowed people to pitch project ideas to the DAO community and anyone with DAO tokens code vote on projects, and would receive money if the project made a profit

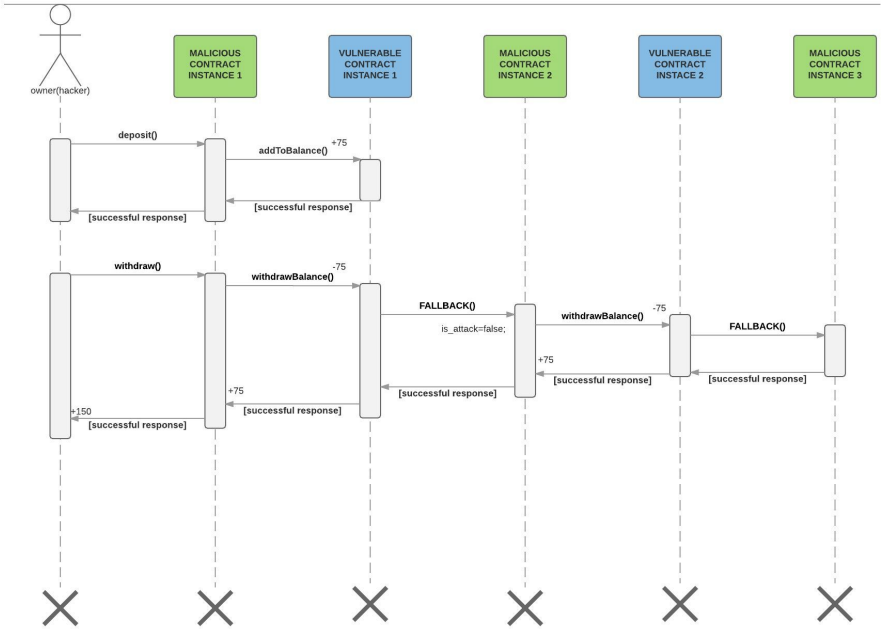
DAO's Massive Coding Error

- On June 17, 2016, a hacker found a loophole in the coding of the smart contract that allowed him to take funds from the DAO
  - 3.6 Million ETH were stolen from the attack
- The EVM executes instructions *synchronously*, one after another, unlike JavaScript
- The hacker was able to "ask" the smart contract to give the Ether back multiple times before the smart contract could update its balance.
  - ***Note: Very simplified Explanation, will get into more detail another time***

Why is it a problem to allow someone to request for their money back before updating a person's balance?

DAO Exploit

- Important lesson: make sure to understand EVM when making smart contracts
  - Solidity make look like JavaScript, but it is different!
- Test for vulnerabilities on an Ethereum Testnet



Real Life Use Cases of Smart Contracts

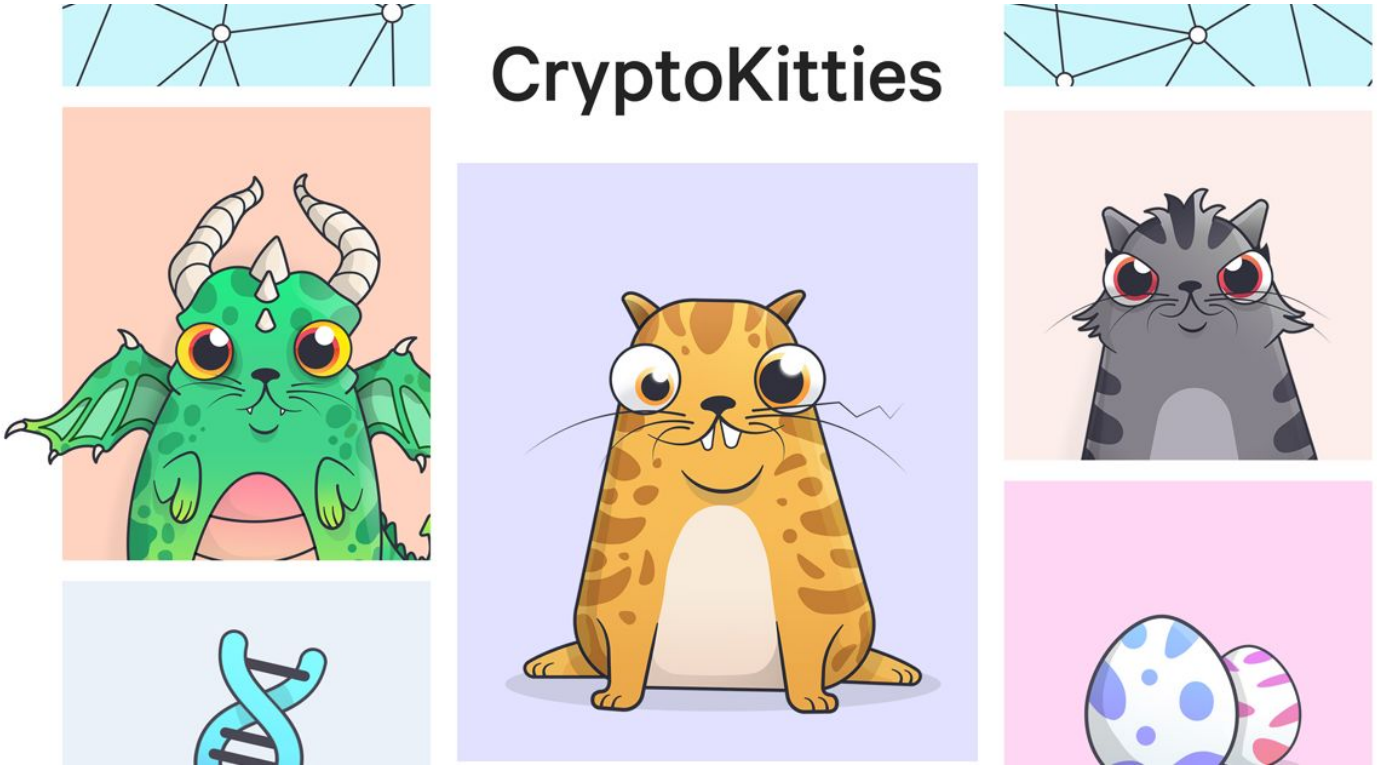
- Elections
  - Voting data can be put into blockchain
  - Data is encrypted and (somewhat) anonymous
- Supply Chain Logistics
  - Supply chain has many links that need a confirmation from the previous in order to work
  - Waiting for confirmations to further send information down to another link is highly time inefficient
  - Smart contracts allow the progress of each link to be uploaded to the blockchain and confirmed
  - This ensures transparency, prevents fraud, and is quicker
  - Also endless uses with IoT

Smart Contract Applications

Can you guys think of any other potential examples of applying smart contracts to the real world?

Remember: they are immutable, can securely store data, provide anonymity, and cut out the middle man

Blockchain Game: CryptoKitties



You can make other coins (ERC20 Tokens)

https://etherscan.io/tokens

Etherscan
The Ethereum Block Explorer

LOGIN | Search by Address / Txhash / Block / Token / Ens | GO

HOME | BLOCKCHAIN | TOKENS | RESOURCES | MORE

Token Tracker

Home / Tokens

Sponsored: **Investoland;** A Global Decentralized Investment Network. Don't get left out. Join the pre-sale.

Ethereum Tokens Market Capitalization
A total of 118973 Token Contracts found

Search for Token Name or Address | Find

First | Prev | Page 1 of 14 | Next | Last

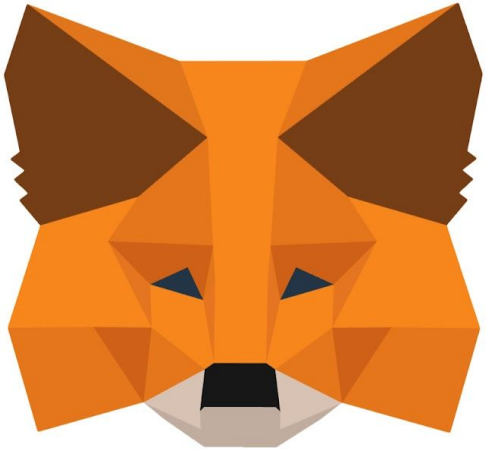
	Token	Price	%Change	Volume (24h)	MarketCap
1	BNB (BNB) Binance aims to build a world-class crypto exchange, powering the future of crypto finance.	$9.5233 0.00147056 Btc 0.046494 Eth	4.05%	$22,717,068	$909,596,610
2	VeChain (VEN) VeChain aims to connect blockchain technology to the real world by providing a comprehensive governance structure, a robust economic model as well as advanced IoT integration.	$0.0140 0.00000216 Btc 0.000068 Eth	1.67%	$28,083,742	$775,965,687
3	OmiseGO (OMG) OmiseGO (OMG) is a public Ethereum-based financial technology for use in mainstream digital wallets	$3.4362 0.0005306 Btc 0.016776 Eth	6.09%	$40,040,521	$481,906,596
4	ZRX (ZRX) The Protocol for Trading Tokens	$0.5347 0.00008256 Btc 0.002610 Eth	5.98%	$12,259,811	$288,475,626
5	Zilliqa (ZIL) Zilliqa is a high-throughput public blockchain platform - designed to scale to thousands of transactions per second.	$0.0340 0.00000525 Btc 0.000166 Eth	4.87%	$9,520,014	$264,738,803

Actual Ponzi Schemes

- https://powh.io/
- Proof of weak hands coin
- Ponzi scheme is programmed into the smart contract

Metamask

- Metamask is an ethereum wallet that can store ETH and ERC20 tokens
- Is more than a wallet; it is a bridge that allows you to run Ethereum dApps without running a full Ethereum node
- Is crucial to using the Ethereum blockchain on a browser
- Go get metamask extension at https://metamask.io/



Sources

https://medium.com/@anesthesteve/bitconnect-explained-c68dd2daef2f

https://www.youtube.com/watch?time_continue=1&v=xK3yuxrmCac

https://bitcoin.org/bitcoin.pdf

https://github.com/ethereum/wiki/wiki/White-Paper

https://metamask.io/

https://cointelegraph.com/explained/smart-contracts-explained

http://www.ethdocs.org

https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470

https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Sources

https://coinmarketcap.com/faq

https://www.coindesk.com/three-smart-contract-misconceptions/

https://blog.oraclize.it/understanding-oracles-99055c9c9f7b