Block Chain

Not Just for Cryptocurrency

About Me

- Michael Vieau
- Full time penetration tester at Sikich LLP
- Adjunct professor at MSOE
- Maintainer of the MiniPwner project
- Co-creator of The Mayhem Lab
- Hardware hacking
- Body hacking enthusiast

SIKICH®

Agenda

- Introduction to Blockchain
- How it works (technically)
- Examples using Blockchain
- Attacks against Blockchains
- Demo
- Can Blockchain Help?

Introduction to Blockchain

What you know

- Who here has head of Blockchain?
- What have you heard about Blockchain?

Definitions

Per Wikipedia

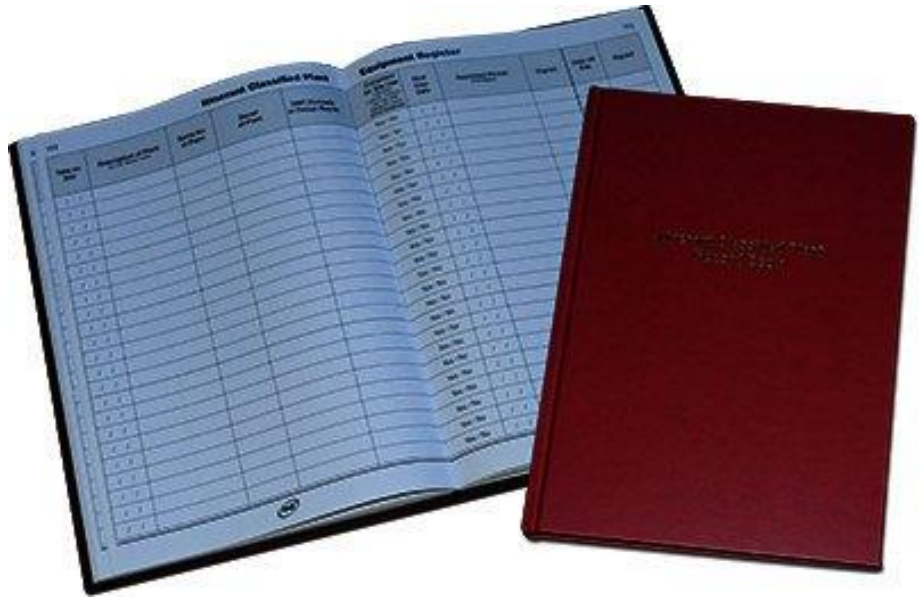
- A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree root hash)

Per IBM

- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

How to think about Blockchain

- A very fancy record book to keep track of transactions throughout a process which is immutable to change due to cryptography.



Public vs. Private

Public blockchain

- Any user can join, read and write to a public blockchain
- An example would be Bitcoin

Private blockchain

- Functions the same as a public blockchain but with access controls to restrict who can use it
- An example would be Hyperledger

Characteristics of a Blockchain network

- Each host (node) on the network stores a copy of the Blockchain
- No one node can tamper with the Blockchain
- 51% or more of the nodes must come together and decide that a transaction is valid
- Self policing of transactions

What can it be used for?

- Cryptocurrency
- Manufacturing
- Healthcare
- Smart Contracts
- Any process needing to track a sequence of events

Why use a Blockchain?

- Reduces the time between transactions
- It can be expensive to use a credit card for large transactions
- A large percentage of people do not have access to a bank account
- Can help reduce fraud
- Can increase transparency into the transaction process

What Blockchain isn't

- It is not a magical cure for a broken process
- Blockchain is not a replacement for a database. A Blockchain is used to store data related to transactions, not the data its self.

How Blockchain Works

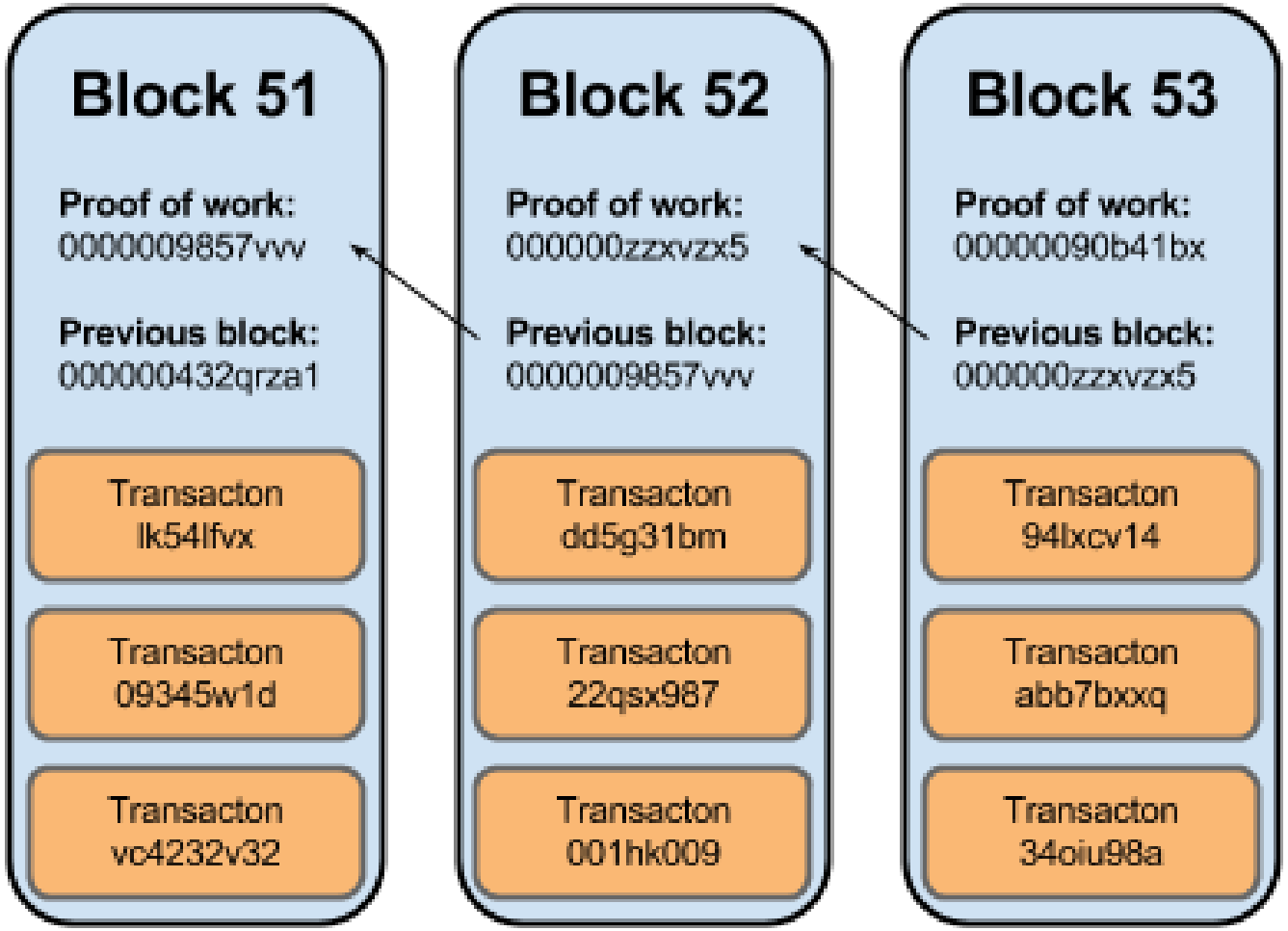
From a technical point of view

Overview

- Since blockchain technology can be used for many different purposes, the section will talk about how the most common parts of a blockchain.

The chain of blocks

- Each block in a chain contains transaction information related to the process. In the example of Bitcoin, it should show the moving of money between wallets.



Let's start at the beginning

- You need a genesis block
- The genesis block is unique as it is the only block that is not linked to a previous block.
- The code to generate the genesis block is often hardcoded within the application using the blockchain

What's in a block

- Block header
  - Hash of the previous block
  - Timestamp
  - Size (normally in Kilobytes)
  - Nonce
  - Hash of the data contained within the block
- Transaction
  - Each transaction stored within that block
  - Could be a single or many transactions

Hashing

- Hashing is using a cryptographic algorithm to generate string (the hash) of a predefined length based on the input
- MD5hash of the word “password” is **5f4dcc3b5aa765d61d8327deb882cf99**
- You will received the same output each time the same input is ‘hashed’
- By changing one valid in the input string the hash will change
- MD5 hash of the word “Password” is **dc647eb65e6711e155375218212b3964**

Hashing

- There are multiple different types of hashing algorithms that can be used
- Each algorithm has pros and cons
- The major risk is collisions

Hashing

Nounce

- In cryptography, a nonce is an arbitrary number that can be used just once in a cryptographic communication.
- It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.
- They can also be useful as initialization vectors and in cryptographic hash functions.
- In blockchain, a nounce can be adjusted by the miner in order to produce the proof of work (PoW)

Proof of Work (PoW)

- A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements.
- The most widely used proof-of-work scheme is based on SHA-256 and was introduced as a part of Bitcoin.

Mining

- The goal of mining is to calculate a hash of a block of transactions that cannot be easily forged
- The main incentive for mining is that users who choose to use a computer for mining are rewarded for doing so. In the case of bitcoin, it is *n* bitcoins per hash.
- The miner is trying to find the proof-of-work

Transactions

- Transactions are not encrypted
- It is possible to browse and view every transaction ever collected into a block
- You would need a hex editor to view the transaction data
- There are web sites (Blockchain browser) were transactions are displayed in human readable format

https://www.blockchain.com/btc/unconfirmed-transactions

54da994b6e1918717ebc40fd8fe56fafb5f409a2ae272a725907b824a729c7a8 **2019-02-17 17:55:02**

32ynVPgqbZ47cqUuEnoFjgU1oQrV9DJ1fG → 3Pdbbz22rHhsAbJ28fv2bfLnt6JZ2WfY8e 0.0072 BTC
32ynVPgqbZ47cqUuEnoFjgU1oQrV9DJ1fG 0.0211881 BTC

10 Confirmations -0.0072721 BTC

72098f303543e24910b756d26700fae5f4642a03012f566346435f0e4e2f0b12 **2019-02-17 10:57:13**

32ynVPgqbZ47cqUuEnoFjgU1oQrV9DJ1fG → 1PcsE4c5dHheMa2H5YAqaGvFgwmKEmzp8v 0.001467 BTC
32ynVPgqbZ47cqUuEnoFjgU1oQrV9DJ1fG 0.0284602 BTC

60 Confirmations -0.0015398 BTC

Examples

Blockchain in industry

How can I use a Blockchain?

- In this section we will look at three examples of real world blockchains

Blockchain in Business

- Most blockchains used in business are private. This means you need to be granted permission to access the blockchain
- Blockchain for business uses Practical Byzantine Fault Tolerance (PBFT) to handle disputes between nodes on the network

Financial

- In America we have a solid financial infrastructure
- There are third world countries that do not
- Cryptocurrency can be used to facilitate transactions without requiring the government to build out a financial infrastructure

Healthcare

- Health records controlled entirely by the individual and a more robust patient matching and identification system that improves patient safety while eliminating administrative pain points
- All the records that are stored within the blockchain, isn't saved inside one centralized storage unit, making no single source in charge of the data
- Interoperability between different systems is one of the largest issues win healthcare
- There is currently no universally recognized patient identifier

Healthcare

- Illinois is partnering with Hashed Health to work on a system that will **track provider credentials**
- In the short team the goal is to show how distributed ledger technology can help reduce the complexity of interstate licensing
- Long team goal is to have a way in which state licensure boards can efficiently manage credentialing at a national scale
- Accurately tracking providers as they move through their careers can improve patient safety, reduce frustration for consumers, allow employers to assess potential workers more completely, and possibly even prevent employee fraud or abuse

HASHED HEALTH

Healthcare

- Collaboration between payers and providers is a fundamental requirement for value-based care
- Departments within a healthcare system have hurdles sharing information on services performed in a secure and timely manner
- Each department has their own data repositories
- The goal is to create a new exchange method

Smart Contracts

- A smart contract is an agreement that holds a set of rules that will be executed after a given event
- They can be used to eliminate the delays inherent in contracts by building the contract into the transaction
- The goal of a smart contract is to establish conditions in which transactions can be processed based on an event
- Example would be rebooking a flight after a six hour delay

Smart Contracts

- Smart contracts are account holding objects on the Ethereum blockchain
- A contract contains code functions and interacts with other contracts, make decisions, and stores data
- A user on the Ethereum network defines a contract (the contract creator)
- A contract is executed within the Ethereum network

- Ethereum has a Go implementation called **Geth** and a C++ implementation call **Eth**

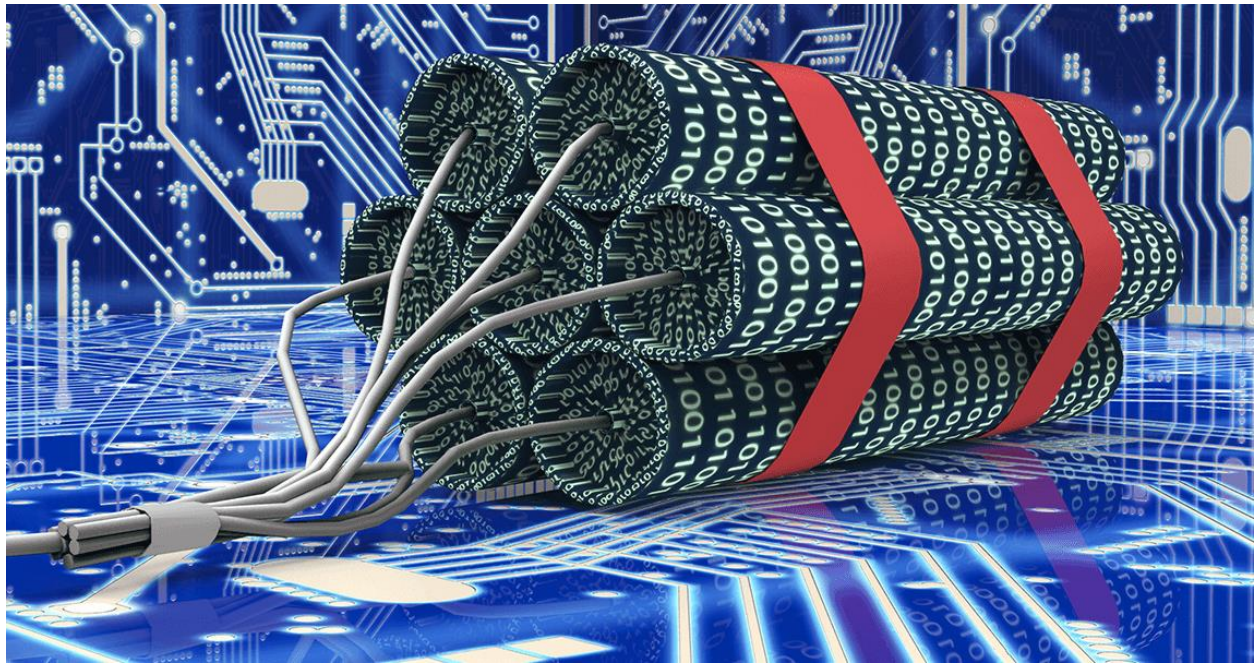
Supply Chain

- Blockchain can help provide traceability across the supply chain
- Import terminals could receive bills of lading quicker, the terminal could plan for the incoming cargo
- The blockchain could be configured to only share appropriate data, such as expected arrival time and weight of the containers
- A blockchain could also be used to share logistic information and make better use of warehouse space and use of trucking fleets

Supply Chain

- Researched the options he wanted on his new car
- Ordered the car from a dealer
- A month later the order was still not placed with the factory
- Several months later the car was delivered to the dealership, it was missing options
- A new order was placed with the factory
- Several more months later the car delivered to the dealership

- How could have a Blockchain helped streamline the process?



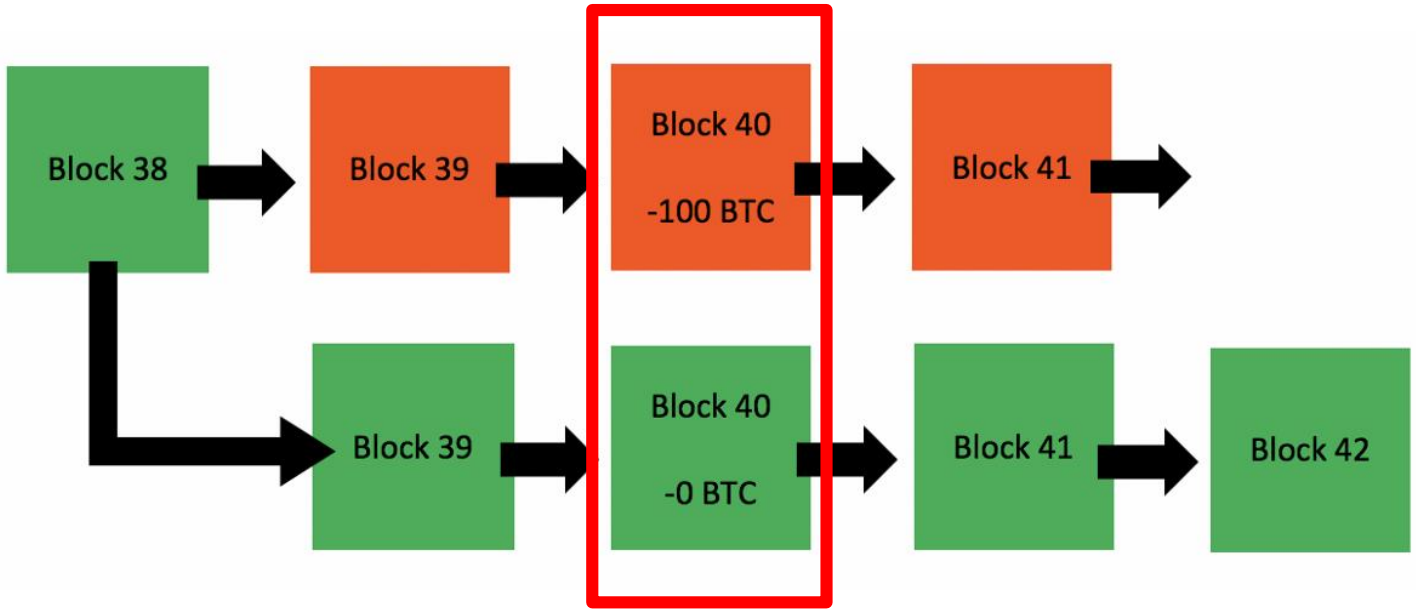
Attacks Against Blockchains

Attack Overview

- There are many different types of attacks that can occur against a blockchain
- Some attacks are more likely to happen then others
- Here are a few attacks that I found more interesting and likely to occur against a modern blockchain implementation

51% Attack

- The most common type of attack is known as a 51% attack
- In the 51% attack, the attacker(s) control 51% of the nodes on the blockchain network and can change the outcome
- The altered blockchain is accepted by all nodes due to its length
- In June 2018 Monacoin, bitcoin gold, zencash, verge and litecoin cash were hit with a 51% attack
- A 51% attack allows the attacker to double send their funds



51% Attack Cost Table

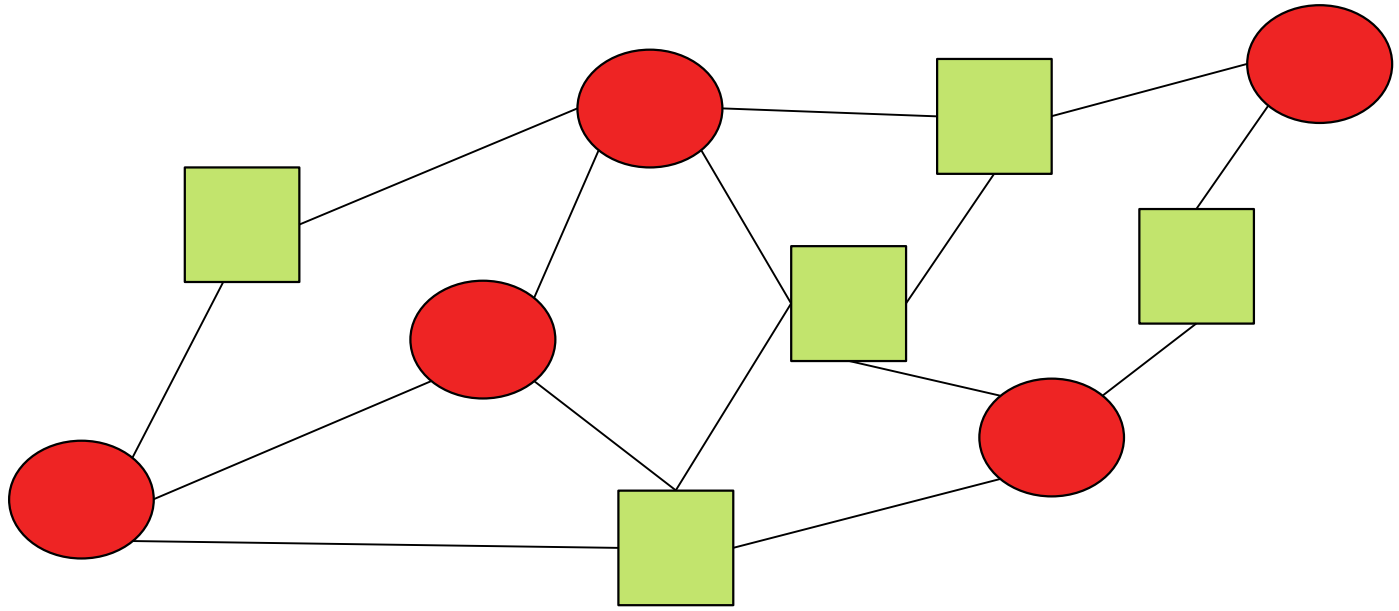
Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$129.59 B	SHA-256	36,414 PH/s	*$660,068*	1%
Ethereum	ETH	$58.69 B	Ethash	201 TH/s	*$381,917*	3%
Bitcoin Cash	BCH	$17.31 B	SHA-256	3,678 PH/s	*$66,679*	14%
Litecoin	LTC	$6.83 B	Scrypt	299 TH/s	*$70,156*	7%
Monero	XMR	$2.51 B	CryptoNightV7	448 MH/s	*$21,947*	11%
Dash	DASH	$2.51 B	X11	1 PH/s	*$12,754*	43%
Ethereum Classic	ETC	$1.58 B	Ethash	8 TH/s	*$14,634*	79%
Bytecoin	BCN	$1.28 B	CryptoNight	426 MH/s	$969	111%
Zcash	ZEC	$970.07 M	Equihash	476 MH/s	*$59,942*	16%
Bitcoin Gold	BTG	$762.88 M	Equihash	34 MH/s	$4,308	224%
Bitcoin Private	BTCP	$493.31 M	Equihash	7 MH/s	$895	1,081%
Dogecoin	DOGE	$394.05 M	Scrypt	245 TH/s	*$57,411*	8%
MonaCoin	MONA	$197.50 M	Lyra2REv2	2 TH/s	$3,104	411%

51% Attack Prevention

- Limit the percent of hashing power any one party or group can perform on your blockchain
- Use a well defined protocol
- Setup your protocol to take several minutes to compute the PoW

Sybil Attack

- An attack in which the attacker(s) create multiple notes on the blockchain network
- If the attacker(s) control a large enough number of notes on the network they can prevent legitimate users from using the blockchain
- Named after Sybil Dorset due to her split personality condition

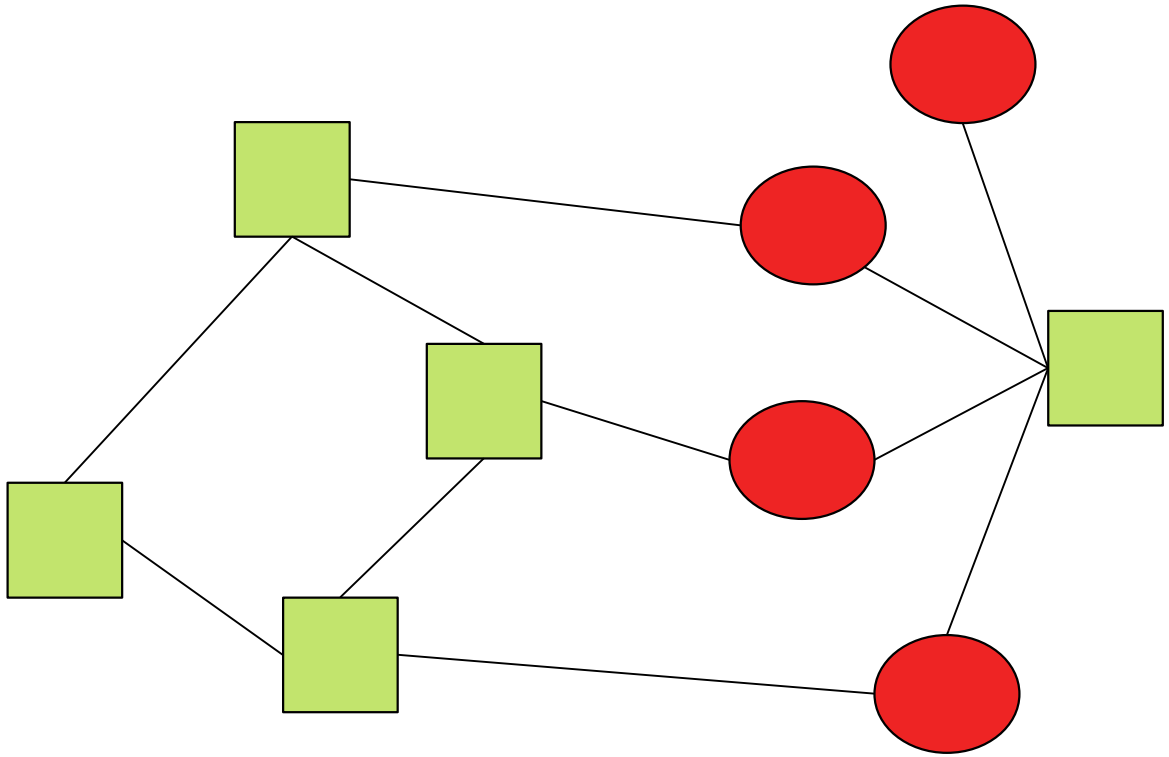


Sybil Attack Prevention

- Limit the number of nodes a person can control
- Implement a fee for creating new nodes on the blockchain
- Use a chain of trust to validate users when a new node is added to the network
- Give a higher reputational value to users that have been part of the blockchain longer

Denial of Service (DoS)

- Multiple notes flood traffic to a single node to prevent that node from taking part in the Blockchain



Denial of Service (DoS) Prevention

- It is almost impossible to prevent a DoS attack 100% of the time
- Increase the transaction fee for each block that is submitted to the blockchain
- Change network parameters such as the size of the blocks containing transactions (if the blocks are smaller it would cost the attacker more to submit enough blocks to perform a DoS attack)

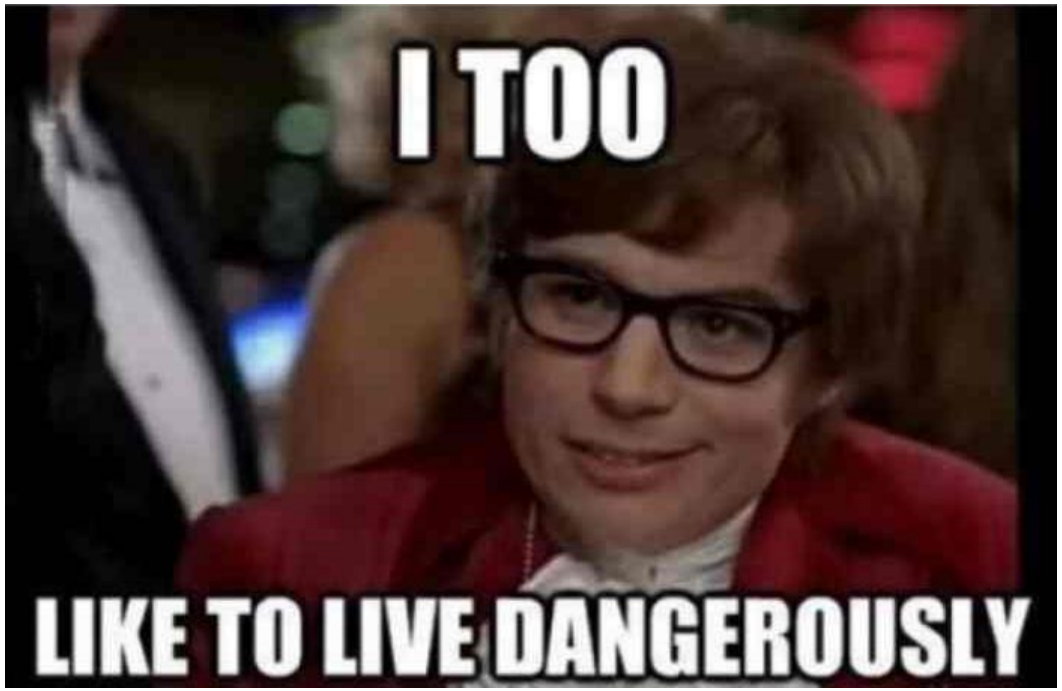
Software Bugs

- All software has bugs, blockchain is no different
- Bugs can be introduced during development
- Code can be implemented incorrectly

Software Bugs Prevention

- Have an independent third party perform code review
- Test, test and test your code before implementation

Live Demo Time



Can Blockchain Help?

Things to Consider

- Do you need to manage complex contracts?
- Do you have a need to track transactions that involve multiple parties?
- Do you have a need to improve transparency between parties?
- Is your current system complex and costly?
- Is your current system full of errors or prone to errors?
- Is your current process vulnerable to fraud?

Determine the Goal

- Will using a blockchain provide more value to your business over using a more mature technology?
- What do you want to accomplish by using a blockchain?
  - Reduce costs
  - Reduce fraud
  - Speed up transactions

What's Needed

- A service provider to assist in deployment?
- Internal resources (human or technology)
- Will you be hosting the blockchain yourself?
- What parties will you be sharing the blockchain with?

First Step

- The first deployment should be for testing and tuning
- Consider re-deploying a ‘clean’ version of the blockchain after testing
- Monitor the application and adjust as necessary

Ending Thoughts

Take-a-ways

- A blockchain is not a cure all technology
- Evaluate your process to see if a blockchain can help, don't just assume it will
- Select the platform that is best for you (public or private)
- Using a Blockchain maybe a way to reduce cost

Resources

IBM Blockchain for Dummies

- https://www.ibm.com/blockchain/what-is-blockchain

Anders Brownworth (Demo site)

- https://anders.com/blockchain

Thank you

Michael Vieau

Vieau@msoe.edu

Michael.Vieau@Sikich.com

https://michaelvieau.com

Twitter: @michael_vieau