



# A BRIEF HISTORY CREATING OUR OWN CRYPTO USING BLOCKCHAIN

ALEJANDRO ZAMORA

CS 131 WEDNESDAY 5:40PM – 10:00PM

PROFESSOR YUEN YUEN

SPRING 2021

# WHAT IS BITCOIN?

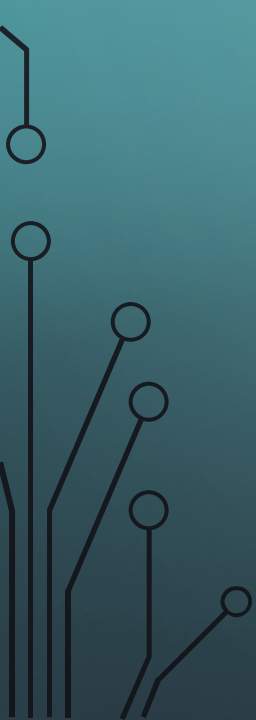


- A cryptocurrency developed by an individual or group of people known as Satoshi Nakamoto
- Started development in 2008 and was released in 2009 when it was released via open-source software
- It is decentralized digital currency capable of being shared via peer-to-peer network
- Transactions are verified by network nodes through cryptography and recorded in a ledger called a Blockchain.

# HOW TO WE OBTAIN THE COIN OF BIT?

- Bitcoin is a reward granted via a process known as “Mining”
- Mining is the process of record-keeping using computer processing power
- An individual, known as a miner, will keep the blockchain consistent, complete and unalterable by grouping new transactions into a block
- These blocks are then verified by recipient nodes using SHA-256 cryptographic hash of the previous block



# BLOCKCHAIN

- Gets its name from the series of blocks that make up a blockchain series
  - When a block containing SHA-256 hashes is verified, the previous block's hash is used
  - Once the hash is verified, a new block is formed creating a chain
  - To be accepted, every hash has includes a proof-of-work that requires miners to find a number called a nonce
  - Once found, the hash is proven and is added to the chain
- 
- 
- 



# WHY BITCOIN?

- In 2017, University of Cambridge published research indicating that there are 2.9 to 5.8 million users with crypto wallets, most of them using bitcoin
- Some use it as a means of investing money, others because they believe in anarchy and decentralization
- Others use it for its convenience and ease of use

# ISSUES WITH BITCOIN

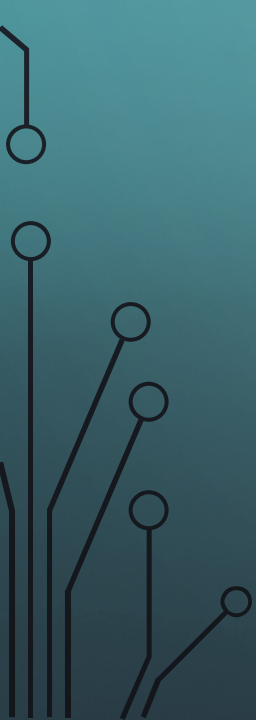

- Used in illegal transactions on the dark web or elsewhere
- Can be used to launder money and is subject to price and market manipulation
- There are a finite number of coins that can be mined, set at 21 million and 18 of those are already in circulation
- The use of a private and public key present potential avenues of theft
- Energy usage by miners gives it one giant carbon footprint

# ENERGY CONSUMPTION

- Mining consumes excessive amounts of energy due to all the processing power required to mine the coin
- As of 2015, an estimated combined consumption clocked in at 155.7 megawatts of power
- By 2017, it had risen to a number between one and four gigawatts of power or about 6% of all energy consumed globally
- In 2021, it was clocking in at 17 Terawatt-hours of consumption, which if classified as a country, would rank in the top 30 energy consumers



# SAVING POWER, FOR THE SAKE OF CRYPTO

- Bitcoin is not the only cryptocurrency out there, but it is the most popular and thus scrutinized the most
  - Miners are already exploring ways to consume power by tapping into renewable resources like hydroelectric power or mining out of cold regions like Iceland
  - They also work with companies with renewable energy surpluses like Hydro Quebec
- 
- 



# SAVING POWER, FOR THE SAKE OF CRYPTO

- It is time to move away from coal because of its effect on the environment and mining operations
- A coal mine explosion that occurred in April of 2021 in Xinjian coincided with a 35% drop in hashing power which caused the price of each coin to drop
- Mining accounts for a total of 22.9 metric tons of CO<sub>2</sub> emissions which is comparable to the emissions total of Kansas City

# A PROPOSED SOLUTION

- Further establishing mining centers in areas where the climate and local resources can be used is a great start
- Mining in arctic regions provides cool air perfect for keeping machines cold
- Using solar energy in high sun areas like the desert provides a steady source of renewable energy
- Establishing mining centers near hydroelectric dams also provides clean renewable energy
- Windy locations can also be used when setting up a wind farm to harvest clean energy

# A QUICK SOLUTION

- One of the quick ways to reduce mining's environmental impact is to move away from a proof-of-work model
- A proof-of-stake model is widely regarded as a worthy replacement to POW model
- POS is a validation is the authority to validate entries on the blockchain
- This method involved giving a person the privilege to mine based on how many coins they have



# PROOF OF STAKE AND PROOF OF AUTHORITY

- This model requires miners to place their coins in escrow so as to use them as a token of validity
- If the person fraudulently alters the blockchain, they lose all their coin as well as the ability to mine
- The Proof-of-Authority model limits the amount of people who can validate blockchain transactions
- The Energy Web Foundation is designing a POA method for confirming blockchain that can be the future



# ALTERNATIVE, WE MAKE OUR OWN CRYPTO

- What if instead of subscribing to an already present crypto, we create our own?
- Let's call it...BrahmaCoin!!
- Using blockchain, this coin is made up of:
  - Blocks that store data
  - Has a digital signature that connects the blocks together
  - Uses proof-of-work to validate new blocks
  - Can check for valid and unchanged data



# BRAHMACOIN

- Our newly minted crypto's goal is so we use it as a form of on-campus payment alternative to cash and credit for food, books, classes and other things
- It is implemented using Java and the latest JDK to generate and validate hash codes while adding them to our blockchain
- Using the GSON library by Google, allows us to turn an object into JSON



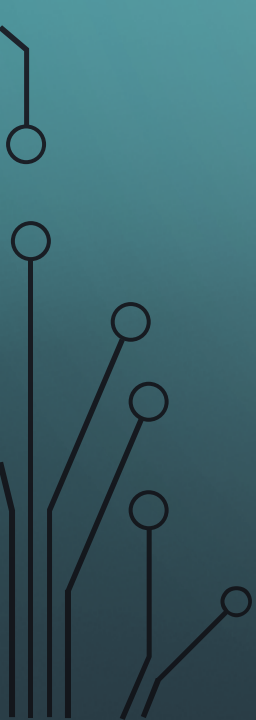


# BRAHMACOIN

- To create our crypto, we will first make a Blockchain program that when run, mines for our crypto
- By mining, we check the hashes, verify they are valid and add them to our chain
- A second program is created that sends transactions of this coin between two individuals by checking the hashes and statement balance





# BRAHMA COIN

- Although this is a simulation and is in no way a real crypto, the way it functions is as accurate as possible
  - This program teaches us the inner workings of Blockchain and how to set up our very own cryptocurrency
  - It also helps us understand hash values and their importance
- 
- 
- 



# PUBLIC AND PRIVATE KEYS (AND HOW THEY ARE DISCRETE MATHEMATICS BASED)

- A crypto wallet, like the one demonstrated, uses a public and a private key to exchange funds between users
- A public key is a user's key that allows a user to send and receive crypto transactions by decrypting that information
- A private key is used to verify and unlock or decrypt the public key transaction thus receiving funds. You never want to share your private key with anyone because that gives them access to your wallet.

# USING RSA INSTEAD OF SHA-256

- Sending crypto uses mathematical induction to decrypt a transaction
- Using the RSA Scheme, Alex sent Yuen some BrahmaCoin. His key contained two extremely large prime numbers  $p, q$
- The public key consists of a number  $n$ , which is the product of  $p, q$  and another number  $e$
- $e$  is a prime number with  $(p-1)(q-1) \nmid e$ . Euler's totient function which gives number of integers  $\leq n$  and relatively prime with  $n$
- You use  $n, e$  to encrypt messages but need to know  $p, q$  to decrypt
- Security of RSA relies on computational difficulty and prime factorization

# ENCRYPTING WITH RSA

- To send money to Yuen, Alex first represents the transaction as a sequence of numbers ,  $M$
- Alex uses Yuen's public key,  $n$ ,  $e$  to perform encryption as:
  - $C = M^e \pmod n$  [C is the cyphertext]



# ENCRYPTION EXAMPLE

- Encrypting the message “STOP” using RSA with  $n = 2537$ ,  $e = 13$
- Convert each letter to a number  $[0,25]$ :
  - $S = 18, T = 19, O = 14, P = 15$
- Group the numbers into blocks of 4 digits:
  - $M = 1819\ 1415$
- Encrypt each block as  $C = M^{13} \pmod{2537}$ 
  - First Block:  $C = 1819^{13} \pmod{2537} = 2081$
  - Second Block:  $C = 1415^{13} \pmod{2537} = 2182$
- Our Cyphertext : 2081 2182



# DECRYPTING RSA

- Decryption key  $d$  is the inverse of  $e$  modulo  $(p-1)(q-1)$ :
  - $d * e \equiv 1 \pmod{(p-1)(q-1)}$
- The inverse of  $e \pmod{(p-1)(q-1)}$  can be computed efficiently if we know  $(p-1)(q-1)$
- Since attackers do not know  $p, q$ , they cannot compute  $d$  with reasonable computing effort or time
- Using the Chinese Remainder theorem and Fermat's Little Theorem, we can see that:
  - $(M^c)^d \equiv M \pmod{n}$

# DECRYPTING RSA

- Using the Chinese Remainder theorem and Fermat's Little Theorem, we can see that:
  - $(M^c)^d \equiv M \pmod{n}$
- The Cyphertext  $C$  is just  $(M^c)^d$ ,  $C^d \pmod{n}$  allows decrypting the message
- Since Yuen can compute  $d$  using  $p, q$ , Yuen can easily decrypt the message but no one else can.

# WHY RSA ISN'T USED AND WHY IT SHOULD BE

- Crypto like Bitcoin uses an ECDSA keypairs versus RSA because of hardware limitations at the time of its creation
- This was done because RSA keys are big and need at least 2048-bit modulus compared to 256-bit ECC keys Bitcoin uses
- Smaller amounts of bits equals smaller storage space but with storage prices so low in today's market, it is possible to make the switch to RSA without feeling the effect of storage constraints
- It is possible to compress RSA signatures, but it has yet to be implemented and used enough to see if it's worth it



# SOURCES

- [Cryptography – How are RSA, AES and SHA different? | AUTRUNK \(wordpress.com\)](#)
- [bitcoin.pdf](#)
- [https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency](#)
- [https://www.theverge.com/2017/12/21/16806772/bitcoin-cryptocurrency-energy-consumption-renewables-climate-change](#)
- [https://www.theguardian.com/commentisfree/2019/jan/17/bitcoin-big-oil-environment-energy](#)



# BRAHMACOIN DOCUMENTATION

- System Specs:

- Ryzen 7 2700x
- 16gb 3200mHz RAM
- GeForce GTX 1650 4gb

- Software:

- Windows 10 Pro
- IntelliJ Ultimate
- Java 16
- Google GSON Library
- Bouncy Castle