

CMSC 304 Computer Ethics



1

Bookkeeping

- EA2 due tomorrow night
 - 3-4 pages, single spaced, Times, 1" margins
 - Rubric published
- Last class before spring break
 - When we return: Cyberstalking/cyberbullying, then midterm
- How familiar are you with cryptocurrency?
 - A lot
 - Somewhat
 - Slightly
 - Not at all

2

Cryptocurrency and blockchain

- A.K.A. Web 3.0
- Cryptocurrency: a medium of exchange that is created by individuals* and whose transactions are maintained in a decentralized ledger
 - Security of the transaction history is maintained using cryptographic work
 - A decentralized peer-to-peer system that can validate electronic transactions
 - Allows online payments to be sent directly from one party to another without going through a financial institution
- Blockchain: the distributed, decentralized ledger that records everything about a cryptocurrency – creations, transactions, NFTs, etc.

3

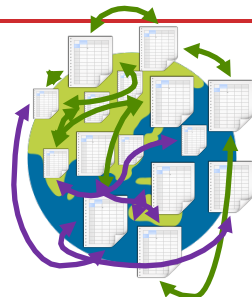
Cryptocurrency basics

- Mining:** creating new units of currency (e.g., bitcoins)
 - Usually "proof-of-work" – solving hard (useless) computational puzzles
- Transactions:** transferring currency between people
- The ledger:** a history of all created currency and all transactions
- (The) Blockchain:** how the ledger is stored
 - Every time a new puzzle is solved, a new 'block' is added
 - It stores the creation of that block and all transactions since the previous one
 - Every time a block is added, the solver receives some amount of currency, the "block reward"

4

Blockchain, a metaphor

- Picture a spreadsheet that is duplicated millions of times on the Internet and is continuously updated.
- On this spreadsheet:
 - You can add new rows
 - but
 - You can never modify a row



5

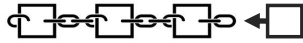
Blockchain

- A peer-to-peer immutable distributed ledger to generate computational proof of the chronological order of transactions
- Founded upon a single, agreed-upon history of the order of transactions
- Maintains all history as 'blocks'



6

What is a Block?



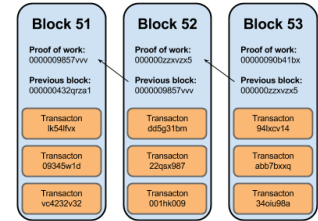
- Files where data pertaining to the network is permanently recorded
- A block records some or all of the most recent Bitcoin transactions that have not yet entered any prior blocks
- Like a page of a ledger or record book
 - Each time a block is 'completed', it gives way to the next block in the blockchain
 - A block is thus a permanent store of records which, once written, cannot be altered or removed

www.sanishin.com/documents/Bitcoin_PP_-_08-21-21/20111.pdf

7

What's in a Block?

- So a block is a record of new transactions
- Location of cryptocurrency
- Other uses: medical data; land (ownership) registries; work history; voting records; NFT registries; ...
- Once each block is completed it's added to the chain

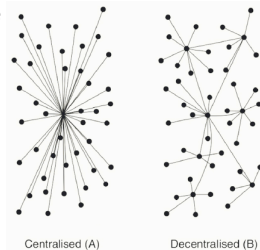


www.sanishin.com/documents/Bitcoin_PP_-_08-21-21/20111.pdf

8

Decentralization

- So far this could all happen on a single computer
- What makes it secure is that the blockchain is **decentralized**
- Everyone has copies of the blockchain
- They all communicate to ensure they agree
- Work is hard to **do** but easy to **verify**

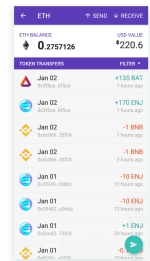


Centralised (A) Decentralised (B)

9

Wallet

- Software program where "Bitcoins" are stored
- Bitcoins aren't stored but your private keys are saved in the wallet
- Helps facilitate sending and receiving bitcoins
- Four main types
 - Desktop
 - Mobile
 - Web
 - Hardware



academicworks.cuny.edu/context/mc_oers/article/10133/type/native/figure/attachment

10

Exchanges

- Not everyone takes bitcoin
- How do you get (legal) goods and services?
 - Illegal services frequently take bitcoin directly
- An **exchange** lets you buy and sell cryptocurrency



Cryptocurrency Exchange

11

Advantages (?) of cryptocurrency

- Anonymous
- High availability
- Borderless (for now)
- No centralized source of control
- No (single) 'middleman' gating transactions
 - As in fiat currency
- No regulations
 - Of course, regulations usually exist for a reason

12

Crypto and Organized Crime

- Money laundering
- Kidnapping (literal ransom)
- Ransomware extortion
- Cryptocurrency scams
- Sale of illegal assets
 - Drugs, human trafficking, child exploitation, dark sales
- Terror funding

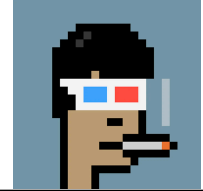


www.cnn.com/2018/05/15/news/tech/cryptocurrency-criminals/index.html

13

NFTs

- Non-fungible (that is, non-interchangeable) tokens
- Proof of ownership of some (usually digital) asset
- Essentially registers ownership in the blockchain
 - Mostly Ethereum, another cryptocurrency
 - Ethereum has a more complex concept of 'token'
- What does that ownership give you?
 - Bragging rights
 - Speculation rights



14

Wash trading

- Person A buys an NFT for \$10.
- Person A sells it to Person B for \$10,000.
- Person B sells it to Person C for \$100,000.
- Person C sells it to Person D it for \$10,000.
- A, B, and C are all the same person
- This is called 'wash trading' and it's illegal in regulated markets

twitter.com/sandwich/status/1445705667826208770?lang=en

15

Money laundering

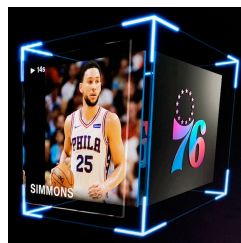
- Say you have several million in bitcoin from a ransomware attack
- Exchanges won't let you cash out because of AML laws
- Create an NFT, sell that to yourself on one of the NFT platforms
- NFT platform turns dirty tokens into clean tokens

twitter.com/sandwich/status/1445705667826208770?lang=en

16

What Value does an NFT have?

- "Like all crypto scams, the essence of the NFT grift is in recruiting new believers by convincing them a blessed database is an authoritative registrar of value"
 - Consider star registries
- NBA "Top shot"
 - What does ownership mean?



nbatopshot.com/

17

Crypto and Climate

- Cryptocurrency relies on "proof of work"
- Solving computationally hard problems → block creation
 - That work has no other value
- Total energy cost > electricity use of Sweden
- Each transaction costs \$176 in energy (worldwide averages)
- Proof-of-work currencies are **literally** designed to waste computation
- Crypto mining creates substantial electronic waste

18

Crypto and climate: solutions

- “Proof of storage” crypto: destroyed the hard drive market for about 2 years
- “Proof of stake” crypto: largely unimplemented; unlikely to replace existing systems



medium.com/zolcorp/industrial-and-climate-impact-what-it-actually-means-and-why-it-matters-7061

19

Discussion

- Green energy crypto: If you have solar banks or a wind turbine, is it okay to do crypto mining?
 - What makes it an okay idea?
 - What makes it a bad idea?
 - Do these scale to municipal-level considerations?
- Ransomware attacks: When is it okay to pay?
 - Assuming no backups
 - What are the down sides of paying ransoms?
 - When is it justifiable?
- When do the benefits of NFTs outweigh the costs?

20