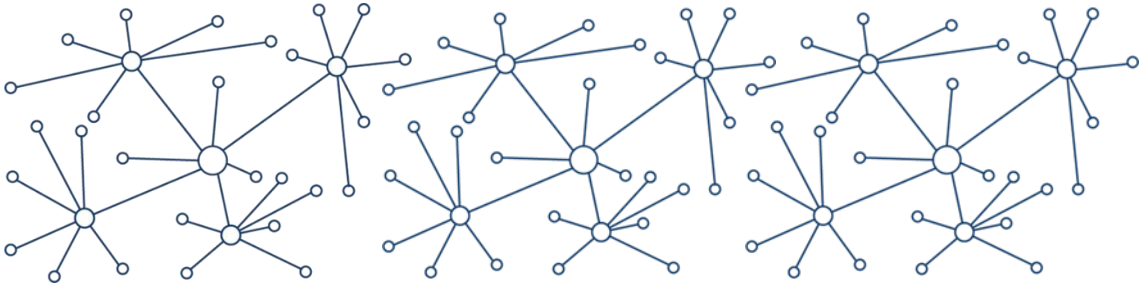


Blockchain Technology

Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#5 and 6 (16 Aug 2022)

Dr. Dhiren Patel

Blockchain - visualization

- https://andersbrownworth.com/blockchain/distributed

Blockchain Technology

- Bitcoin components (max. supply 21 M)
- Hash function SHA256
- Puzzle to solve (making x leading bits of block hash to 0)
- Difficulty adjustment (auto – approx. every 2 weeks (time it took to find the last 2,016 blocks) to keep av. time between blocks to 10 min)
- Elliptic curve crypto - Secp256k1 is the name of the elliptic curve used by Bitcoin to implement its public key cryptography (wallets)

Why Crypto price fluctuates?

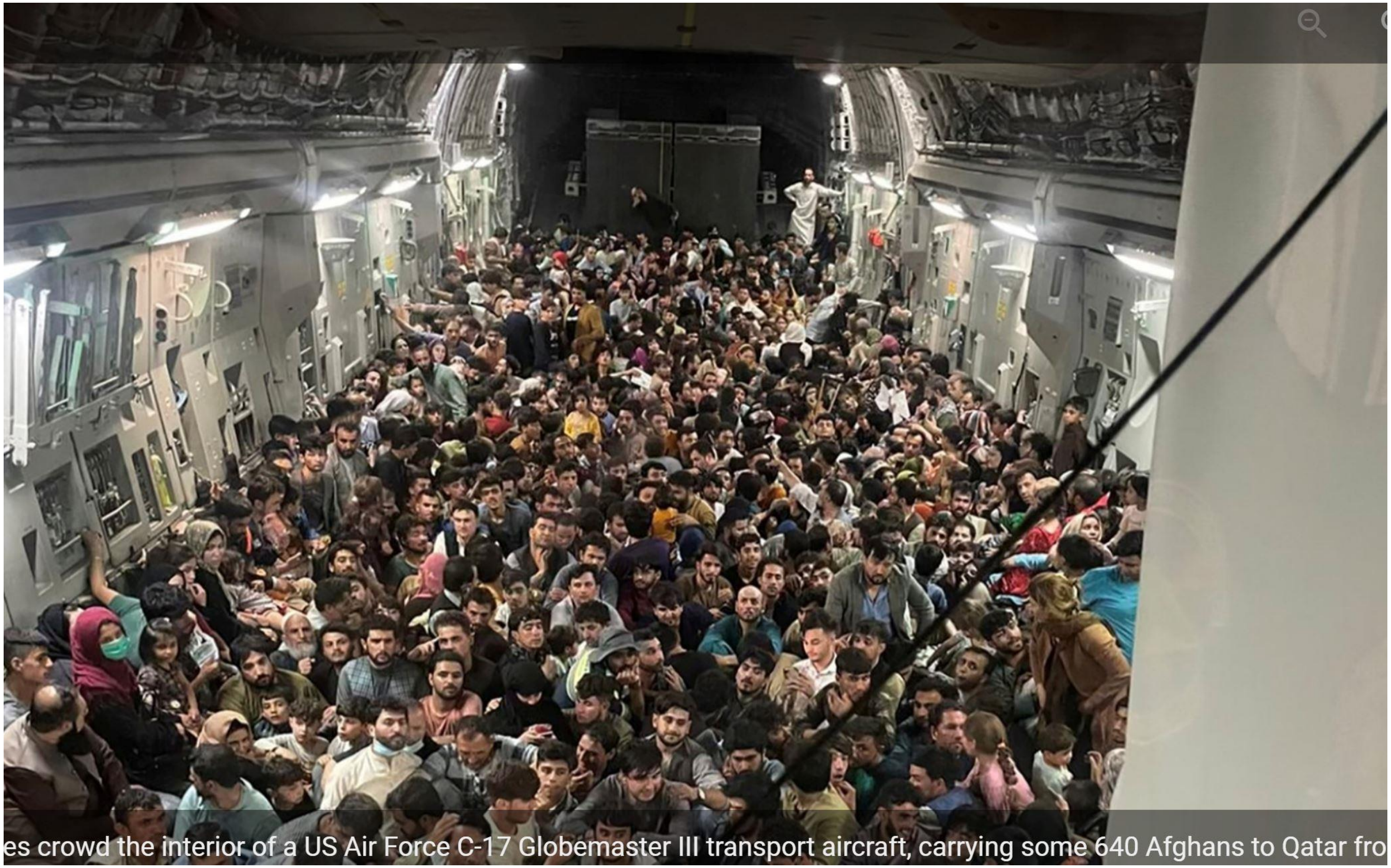
- Bitcoin halving !!!! (happened on an av. every 4 years so far – reward reduced from 50 BTC → 25 BTC → 12.5 BTC → 6.25 BTC) //last halving happened in May 11, 2020
- Miners runaway when rewards cut into half and mining bill (electricity to run computers to solve puzzle) doesn't fall!!
- El Salvador declaring BTC as a legal tender (Sept 2021)
- Wars (US force leaving Afghanistan (Aug 2021), Russian Invasion in Ukraine (Feb 2022)) ….
- Political resistance (old school) across the world ….
- Market movers (Eth2.0, DeFi, NFTs, Gaming and Metaverse, CBDC etc.)

Cryptocurrency (Wikipedia)

- It is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure transactions, control the creation of units, and verify the transfer of assets
- encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds
- It uses decentralized control as opposed to centralized currency and central banking systems
- (normal (fiat) currency example – exchange, storage, ownership, value, purchase power, trust, production, interoperability..)
- The decentralized control of each cryptocurrency works through DLT, typically a blockchain, that serves as a public financial transaction database (coinbase??)

Money Reimagined (Afghanistan context)

Money Reimagined (Afghanistan context)



es crowd the interior of a US Air Force C-17 Globemaster III transport aircraft, carrying some 640 Afghans to Qatar fro

Bitcoin could play a very important role (Aug 2021)

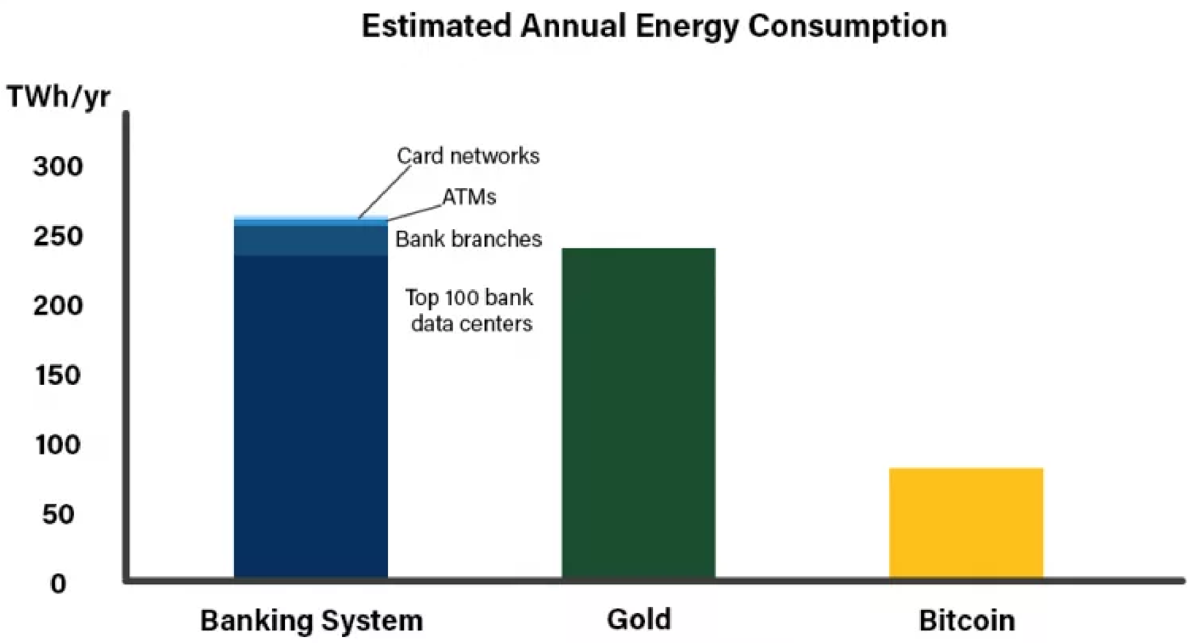
- If Afghans must embark on an arduous and dangerous escape, at least with cryptocurrency they would have a better way to transfer whatever wealth they have across borders.
- In decades past, refugees from war-torn areas would deal with this problem by sewing pieces of gold into the hems of their clothes, running the risk of having them stolen by common thieves or corrupt officials.
- Now, they can simply load up a bitcoin address that's personally accessible anywhere in the world.
- digital literacy and computer education, laying a knowledge foundation upon which bitcoin can now be deployed to bypass the failing legacy system

How Much Energy Does Bitcoin Use?

- Bitcoin uses less than half the energy the banking system consumes, according to recent data.
- Bitcoin’s energy usage depends on how many miners are operating on its network at any given time. These miners must compete against each other to win the right to add the next block to the blockchain and earn rewards. The competitive structure results in a lot of wasted energy as only one miner can add a new block every 10 minutes.
- At its present level (Aug 2021), Bitcoin consumes 81.51 terawatt hours (TWh) annually.

Banking system energy consumption

- when you take into account the sheer number of physical branches, printing facilities, ATMs, data centers, card machines and secure transport vehicles required to support the fiat currency system.



Source: Galaxy Digital (May 2021)

Old → New

- You hand banknotes to the baker or the butcher or the barber, she gives you a bread or a brisket or a buzzcut. No third party gets to second-guess or overrule your choices.
- As commerce moves online, more and more transactions are funnelled through ever-more-powerful intermediaries.
- It would be cheaper for both buyer and seller if the middleman is eliminated from the process

Censorship

- the centralized infrastructure between the buyer and seller, always comes with some sort of fee for the upkeep of the infra[structure] and for the business building and maintaining it to operate.
- the veto power of intermediaries becomes a problem when they block innocuous transactions
- Bitcoin restored censorship resistance to payments in the digital realm