

# Bitcoin and Crypto Currency Technologies

Elective CSE 662  
MTech. I CSE 2<sup>nd</sup> Sem  
(Jan 2023)

Dr. Dhiren Patel

# Bitcoin



- Bitcoin is a form of digital currency
- Bitcoin is a crypto currency
- Bitcoin has very high value (price of bitcoin these days is about \$17000 -- per bitcoin these days (Jan first week 2023); with all time high price touched around \$64000 in April 2021!!)
- Regarded as a Digital Gold; as a store of value; world's largest digital asset
- Bitcoin uses blockchain technology to support peer-to-peer transactions between users on a decentralized network

# Bitcoin price chart

16,642.70 USD

+ Follow

+16,315.70 (4,989.51%) ↑ all time

2 Jan, 6:14 am UTC · [Disclaimer](#)

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



# Bitcoin



- Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.
- **Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.**
- Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

# Money (re-imagined)

- Money is a tool. Tools are things that have purposes and utility.
- a charitable interpretation: money's purpose is to help people collaborate at scale by rewarding virtue to individuals or collectives. This is much more attractive. It's also much more practical.
- However, on this view, money is not working well.
- an example of an uncharitable interpretation: Money's purpose is to let a small number of people wield huge power over a large number of people, with little accountability. If this is the purpose of money, then it's working great.

# Fiat currency

- normal (fiat) currency example – INR, USD, GBP..
- exchange, (forex)
- storage, (Bank, Cash, Wallets)
- ownership, (User, Central bank)
- value, (??)
- purchase power, (Subjective, location based)
- trust, (Subjective)
- production, (Central Bank, Govt.)
- interoperability.. (forex rate, USD)

# Stocks

- Traded on traditional stock exchanges such as Nasdaq, London Stock Exchange, Deutsche Börse, etc.
- Can only be traded Monday to Friday. Market opening and closing times vary between stock exchanges
- Regulated financial products
- Purchasers receive share certificates to show legal proof of ownership
- Companies can produce new shares after publicly launching, though there is a finite limit
- Brokerages maintain their own record of stock trades that they execute on behalf of clients

# What is 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
- The decentralized control of each cryptocurrency works through DLT, typically a blockchain, that serves as a public financial transaction database (coinbase??)



# Fiat v/s Cryptocurrencies

- fiat currencies like the U.S. dollar or euro or INR that store all card and wire transactions on a central ledger maintained by a single authority
- Cryptocurrencies are exchangeable for fiat currency via cryptocurrency exchanges and can be used to make purchases from merchants and retailers that accept them
- (Bitcoin) Blockchain is a globally distributed ledger that can be maintained and copied by anyone on the planet and ensures total immutability and transparency

# Cryptocurrency market and Market Dominance (4 Jan 2023)

- About 22k coins (crypto currency)
- About 500 exchanges
- Market share - BTC: 39.9%, ETH: 18.4%, USDT: 8.9%, USDC: 5.5%, BNB: 4.88%, XRP: 2.14%, BUSD: 2.04%, Dogecoin: 1.18%, Cardano: 1.09%, Polygon: 0.85%, Others: 15.76%

# Old → New

- You hand banknotes to the baker or the butcher or the barber, she gives you a cake 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. //privacy breach
- 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) – most decisions are community driven rather than centralized!!

# curriculum

<b>M.Tech. I (CSE) Semester – II</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
<b>CSEXXX: BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES(CORE ELECTIVE 3 OR 4)</b>	<b>3</b>	<b>0</b>	<b>2</b>	<b>4</b>

<b>Course Objectives</b>	
1	to demonstrate a familiarity with the fundamentals of cryptocurrencies.
2	to understand different cryptographic primitives and their use in the design of cryptocurrencies.
3	to analyze different cryptocurrencies and to assess the pros and cons of different cryptocurrencies.
4	to design decentralized applications that operates using cryptocurrencies.
5	to propose and evaluate different use cases of cryptocurrencies.

# curriculum

<b>FUNDAMENTALS OF CRYPTOCURRENCIES AND CRYPTOGRAPHY</b>	<b>(8 Hours)</b>
Introduction of a Cryptocurrency, Transactions of Bitcoin, Need of Cryptocurrency, Cryptographic Hash Functions, Hash Pointers and Data Structures, Digital Signatures, Public Keys as Identities	
<b>BLOCKCHAIN TECHNOLOGY</b>	<b>(10 Hours)</b>
Centralization vs. Decentralization, Distributed Consensus, Consensus without Identity, Blockchain, Incentives and Proof of Work, Digital Signature, Tamper Proof Ledger, Distributed Consensus, Proof of Work, Mining and Currency Supply.	

# curriculum

<b>BITCOIN AND CRYPTOCURRENCY</b>	<b>(12 Hours)</b>
Bitcoin Transactions, Bitcoin Scripts, Applications of Bitcoin Scripts, Bitcoin Blocks, The Bitcoin Network, Limitations & Improvements, Cryptocurrency as an Asset Class, Risk and Return to Cryptocurrency, Review of Portfolio Theory, Asset Allocation with Cryptocurrency, Mining Cryptocurrencies, Crypto Classifications, Ethereum Overview, The DAO, Private Blockchains.	
<b>USE CASES AND THEIR APPLICATIONS</b>	<b>(12 Hours)</b>
Ways to Store and Use Bitcoins, Hot and Cold Storage, Splitting and Sharing Keys, Online Wallets and Exchanges, Payment Services, Transaction Fees, Currency Exchange Markets, Building the Blockchain, Crypto Finance, Business Use Cases, Blockchain in Gaming, Investing in Blockchain, Government and Regulation, Media and Advocacy, Creating the New Frontier of FinTech.	
<b>Practical Assignments Will Be Based on the Coverage of Above topics. (Problem Statements Will Be Changed Every Year and Will Be Notified on Website.)</b>	<b>(28 Hours)</b>
<b>(Total Contact Time: 42 Hours + 28 Hours = 70 Hours)</b>	

# Price fluctuation

16,642.70 USD

+ Follow

-2,581.30 (13.43%) ↓ past 6 months

2 Jan, 6:14 am UTC · [Disclaimer](#)

1D | 5D | 1M | **6M** | YTD | 1Y | 5Y | Max





# Price fluctuation

22,745.50 USD

+ Follow

+2,071.30 (10.02%) ↑ past 5 days

23 Jan, 8:24 am UTC · [Disclaimer](#)

1D

5D

1M

6M

YTD

1Y

5Y

Max



# Few remarks

- Digital divide (bandwidth, power, device, platform)
- NEP – New Education Policy
- Capacity building, Re-training, Up-skilling (Deep skilling)
- Personalized Education – Digital way
- As responsible citizens, all of us should fight the pandemic and other hardships, and showcase our capabilities and commitment towards economic progress with social inclusion and environment sustainability for the global good

# Blockchain

- Think of blockchain as a historical fabric underneath recording everything that happens—every digital transaction; exchange of value, goods and services; or private data—exactly as it occurs.
- Then the chain stitches that data into (encrypted??) blocks that can never be modified and scatters the pieces across a worldwide network of distributed computers or "nodes."
- A blockchain is made up of two primary components: a decentralized network facilitating and verifying transactions, and the immutable ledger that network maintains.
- **Welcome aboard in the World of Blockchain!!**

# Course objectives

- Capacity building - Learning through examples/use cases
- Understand technology foundations of Bitcoin through protocols and security primitives,
- Design and implement new ways of using blockchain for applications with cryptocurrency and beyond
- Token economics, smart contracts, attacks and advances
- Explore platforms to build applications on blockchain

# Course outcome ()

1. Understand blockchain architecture and requisite crypto foundations
2. Understand various consensus protocols and their usage for specific applications
3. Understand and Resolve security concerns in blockchain
4. Explore blockchain advances, use cases and upcoming platforms
5. Learn to write smart contracts
6. Solve problems and create solutions..

# What is a Blockchain?

## Why should we learn it?

- Blockchain facilitates peer-to-peer transfer of *digital assets* in a *decentralized network*
- It is a time-stamped series of (immutable) records of data that is managed by a cluster of nodes (computers) not owned by any single entity (?) - **a democratized system**
- A technology originally created to support *cryptocurrency* bitcoin - Founder (pseudo-named) – **Satoshi Nakamoto**
- Blockchain has the potential to improve applications in finance, healthcare, government, manufacturing, and distribution supply chain...
- There is a dire need for designers, developers, and critical thinkers, who can envision and create newer application models on Blockchain to benefit the world

# Key Information about Course

- Course name: Bitcoin and Crypto Currency Technologies
- Course type: Elective
- Course code: CSE662
- Course scheme: 3 (Lectures)-0 (Tutorial)-2 (Lab)
- Course credits: 4
- Course google classroom: exm4bbe
- Meet link: <https://meet.google.com/cjb-jwfz-qsg>
- Instructors (2023) –
  - Dr Dhiren Patel and Himanshu Patel

# Bitcoin

- Bitcoin enabled an innovative platform for peer to peer transfer of value without any central authority
- By implementing software programs for validation, verification, consensus in the blockchain
- Recording the transaction in an immutable distributed ledger
- Establishing trust among unknown peers
- BTC price on 17 March 2020 – USD 4.9 k
- BTC price mid-April 2021 – USD 64 k !!!!
- BTC price – USD 31.7 k (19 July 2021)
- BTC price – USD 16.6k (today)



# Altcoins

- best-known cryptocurrency Bitcoin – BTC (max. supply 21 M)
- And a selected number of alternative cryptocurrencies known as “Altcoins” (coins that are an alternative to Bitcoin)
- Altcoins that are built using Bitcoin’s original open-source protocol (e.g. Litecoin – LTC, max. supply 84 M)
- //The Litecoin Network aims to process a block every 2.5 minutes, rather than Bitcoin's 10 minutes. This allows Litecoin to confirm transactions much faster than Bitcoin.
- Altcoins that are not based on Bitcoin’s open-source protocol, but that have their own protocol and distributed ledger. (e.g. Ethereum – ETH max. supply – unlimited!, Ripple – XRP max. supply 100 B)
- //**Ethereum** is a decentralized, open-source blockchain with smart contract functionality

# Bitcoin invention philosophy

- Bitcoin – Satoshi Nakamoto 2008/2009
- Banking the Unbanked, De-banking All, Stable digital currency
- Crypto-currency-based payments system could be especially useful in countries with high inflation/unstable banking systems and for cross-country remittances
- control over finance that cannot be seized, frozen, or censored by Governments, Banks, Financial Institutions
- Value to Bitcoin, Total supply – 21M, Exchanges and Wallets
- Craig Wright (Aus) – claiming to be Nakamoto
- Filed 95 patents on Blockchain in the last 3 years

# Market Cap = Current Price x Circulating Supply

Market cap of BTC ~600 B USD

Circulating supply = 18,759,981 BTC

April 2021 – market cap ~ 1.2 Trillion USD

Why?

The circulating supply of a cryptocurrency can increase or decrease over time.

**BTC - Store of Value – digital gold**

Market cap of Eth ~223 B USD

**Ethereum Eth- Utility token**

Market cap of BNB ~ 52 B USD

**BNB – exchange token used for payment of fees (trading)**

Market cap of UNI ~ 10 B USD

**UNI – DeFi (lending protocol – governance token)**

**BAT – (Basic Attention Token).... digital advertisement industry**







**CHIA token - XCH (Proofs of Space and Time - Storage as a Service)....<sup>27</sup>**

# Circulating Supply










- The circulating supply of a cryptocurrency can increase or decrease over time.
- For example, the circulating supply of Bitcoin will gradually increase until the max supply of 21 million coins is reached. Such a gradual increase is related to the process of mining that generates new coins every 10 minutes, on average.
- Alternatively, coin burn events like the ones performed by Binance, cause a decrease in the circulating supply, permanently removing coins from the market.
- The max supply quantifies the maximum amount of coins that will ever exist, including the coins that will be mined or made available in the future.

# Market Cap (4 Jan 2023)







The global cryptocurrency market cap is ~\$837 Billion

Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume(24h)
1	 Bitcoin	BTC	\$320,719,103,029	\$16,659.52	19,251,406 BTC	<a href="#">\$14,067,230,080</a>
2	 Ethereum	ETH	\$148,165,674,847	\$1,210.76	122,373,866 ETH *	<a href="#">\$3,460,054,501</a>
3	 Tether	USDT	\$66,248,004,569	\$0.9998	66,263,713,431 USDT *	<a href="#">\$18,273,024,508</a>
4	 USD Coin	USDC	\$44,184,115,045	\$1.00	44,182,759,851 USDC *	<a href="#">\$1,983,025,364</a>
5	 BNB	BNB	\$39,264,125,227	\$245.46	159,964,237 BNB *	<a href="#">\$384,802,805</a>
6	 XRP	XRP	\$17,495,473,273	\$0.346	50,563,767,827 XRP *	<a href="#">\$851,693,749</a>












# 9 Jan 2023 - The global cryptocurrency market cap is ~\$848 Billion

#	Name	Price	24h Volume 	1h %	24h %	7d %	Market Cap 	Circulating Supply 
1	 Bitcoin BTC	\$17,217.03	\$13,279,822,294 771,497 BTC	▼ 0.16%	▲ 1.61%	▲ 3.37%	\$331,544,121,664	19,256,750 BTC <div><div></div></div>
2	 Ethereum ETH	\$1,309.47	\$5,360,477,668 4,097,972 ETH	▼ 0.12%	▲ 3.66%	▲ 8.87%	\$160,245,332,606	122,373,866 ETH
3	 Tether USDT	\$1.00	\$21,358,335,482 21,359,140,543 USDT	▲ 0.00%	▲ 0.01%	▲ 0.03%	\$66,273,876,397	66,272,490,385 USDT
4	 BNB BNB	\$278.57	\$702,367,691 2,523,415 BNB	▼ 0.22%	▲ 6.67%	▲ 14.12%	\$44,561,428,805	159,963,279 BNB <div><div></div></div>
5	 USD Coin USDC	\$1.00	\$2,438,706,805 2,438,830,760 USDC	▲ 0.00%	▲ 0.01%	▲ 0.00%	\$44,003,748,676	44,000,761,686 USDC
6	 XRP XRP	\$0.3508	\$787,299,183 2,238,791,517 XRP	▼ 0.34%	▲ 3.09%	▲ 5.58%	\$17,738,338,510	50,563,767,827 XRP <div><div></div></div>

# 23 Jan 2023 - The global cryptocurrency market cap is ~\$1.04 Trillion

1	 Bitcoin BTC	\$22,723.67	▼0.22%	▼0.72%	▲7.65%	\$437,884,696,786	\$23,954,307,694 1,055,446 BTC	19,269,981 BTC
2	 Ethereum ETH	\$1,635.69	▼0.11%	▲0.50%	▲4.46%	\$200,166,024,687	\$7,042,517,368 4,311,288 ETH	122,373,866 ETH
3	 Tether USDT	\$1.00	▼0.00%	▼0.00%	▼0.02%	\$66,756,014,837	\$33,400,774,698 33,394,735,355 USDT	66,744,307,804 USDT
4	 BNB BNB	\$304.01	▼0.41%	▲0.66%	▲0.30%	\$48,004,211,177	\$611,379,587 2,013,312 BNB	157,903,273 BNB
5	 USD Coin USDC	\$0.9999	▼0.00%	▲0.01%	▲0.00%	\$43,501,208,051	\$3,191,918,768 3,192,818,277 USDC	43,503,674,962 USDC
6	 XRP XRP	\$0.417	▲1.72%	▲2.99%	▲6.05%	\$21,181,249,598	\$1,045,490,202 2,530,362,297 XRP	50,796,877,639 XRP

# Crypto Exchanges

# ▲	Exchange	Score ⓘ	Trading volume(24h)	Avg. Liquidity	Weekly Visits ⓘ	# Markets	# Coins	Fiat Supported
1	 Binance 	9.9	\$7,488,504,673 ▲ 8.06%	941	15,017,449	1642	383	AED, ARS, AUD and +43 more ⓘ
2	 Coinbase Exchange 	8.2	\$980,769,099 ▲ 25.37%	781	925,724	600	237	USD, EUR, GBP
3	 Kraken 	7.7	\$495,549,629 ▲ 86.43%	737	978,767	718	219	USD, EUR, GBP and +4 more ⓘ
4	 KuCoin 	6.7	\$267,356,524 ▲ 5.61%	508	1,900,432	1399	779	USD, AED, ARS and +45 more ⓘ
5	 Bitstamp	6.5	\$140,646,523 ▲ 34.31%	554	254,173	159	71	USD, EUR, GBP
6	 Bitfinex 	6.4	\$120,057,979 ▲ 15.38%	536	225,674	406	186	USD, EUR, GBP and +1 more ⓘ



# Price fluctuation

22,745.50 USD

+ Follow

+2,071.30 (10.02%) ↑ past 5 days

23 Jan, 8:24 am UTC · [Disclaimer](#)

1D

5D

1M

6M

YTD

1Y

5Y

Max



# Bitcoin Bockchain – Block 770,227

**Hash:**000000000000000000000003f62bf7c1dbea40b23db3f9a04abf3b1ba600192ac18f

## General info

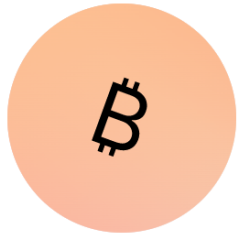
Mined on	Jan 3, 2023 8:42 PM UTC	Miner	<a href="#">Binance</a>
Transaction count	2,633	Fee per kB	0.00015968 BTC • 3 USD
Witness tx count	2,164	Fee per kWU	0.00006537 BTC • 1 USD
Input count	6,704	Output count	9,820
Input total	12,805.48 BTC • 213,592,140 USD	Output total	12,811.73 BTC • 213,696,380 USD
Fee total	0.26093689 BTC • 4,352 USD	Coindays destroyed	9,402.38
Generation	6.25 BTC • 104,248 USD	Reward	6.51093689 BTC • 108,601 USD

# Bitcoin Block773,210

Mined on January 23, 2023 01:42:41

- A total of 890.77 BTC (\$20,216,624) were sent in the block with the average transaction being 1.3662 BTC (\$31,006.74).
- Unknown earned a total reward of 6.25 BTC \$141,847.
- The reward consisted of a base reward of 6.25 BTC \$141,847 with an additional 0.0259 BTC (\$587.82) reward paid as fees of the 652 transactions which were included in the block.

# Who is this unknown? (who mined Block#773,210)




## bc1qx-cetdj

 Bech32 (P2WPKH)



Bitcoin Address

bc1qxmdufsvnuaaaer4ynz88fspdsxq2h9e9cetdj 

Bitcoin Balance

915.24148192 • \$20,824,416



ID: **711d-0dd9**   
1/23/2023, 13:42:41

From Block Reward  
To 2 Outputs

6.27585334 BTC • \$142,793  
**Fee** 0 Sats • \$0.00



ID: **d646-0486**   
1/23/2023, 13:37:42

From Block Reward  
To 2 Outputs

6.41970055 BTC • \$146,066  
**Fee** 0 Sats • \$0.00



ID: **1ece-1084**   
1/23/2023, 12:38:15

From Block Reward  
To 2 Outputs

6.34975947 BTC • \$144,475  
**Fee** 0 Sats • \$0.00



ID: **766d-9f1b**   
1/23/2023, 12:11:33

From Block Reward  
To 2 Outputs

6.27120173 BTC • \$142,688  
**Fee** 0 Sats • \$0.00

# Blockchain Explorer

- A software for visualizing blocks, transactions, and blockchain network metrics (e.g., average transaction fees, hashrates, block size, block difficulty).
- Few examples of Blockchain explorer and search engine
- <https://www.blockchain.com/>
- <https://blockchair.com>
- <https://coinmarketcap.com/>

# Bitcoin (and other cryptocurrencies)

- Traded on centralized and decentralized crypto exchanges
- Crypto markets do not close so bitcoin can be traded at any time on any day
- Bitcoin is not a regulated investment vehicle; however, most international jurisdictions recognize it as property
- Purchasers can hold their own bitcoin or delegate safe storage to third-party custodians
- There will only ever be 21 million bitcoins
- The Bitcoin blockchain publicly records all transactions and can be viewed or downloaded by anyone at any time

# Apolitical; Amoral

- Bitcoin is apolitical and amoral.
- It doesn't care who gets the funds.
- With all the foreign constraints on fiat money movements, anonymously transferred bitcoin (or another cryptocurrency) may be a convenient way to monetize opium crop/drug.
- Everyone deserves to keep their hard earned money and access to education, to technology, to digital currency. Everyone has a right to pursue their dreams
- Bitcoin and Crypto-currencies are there to help!!

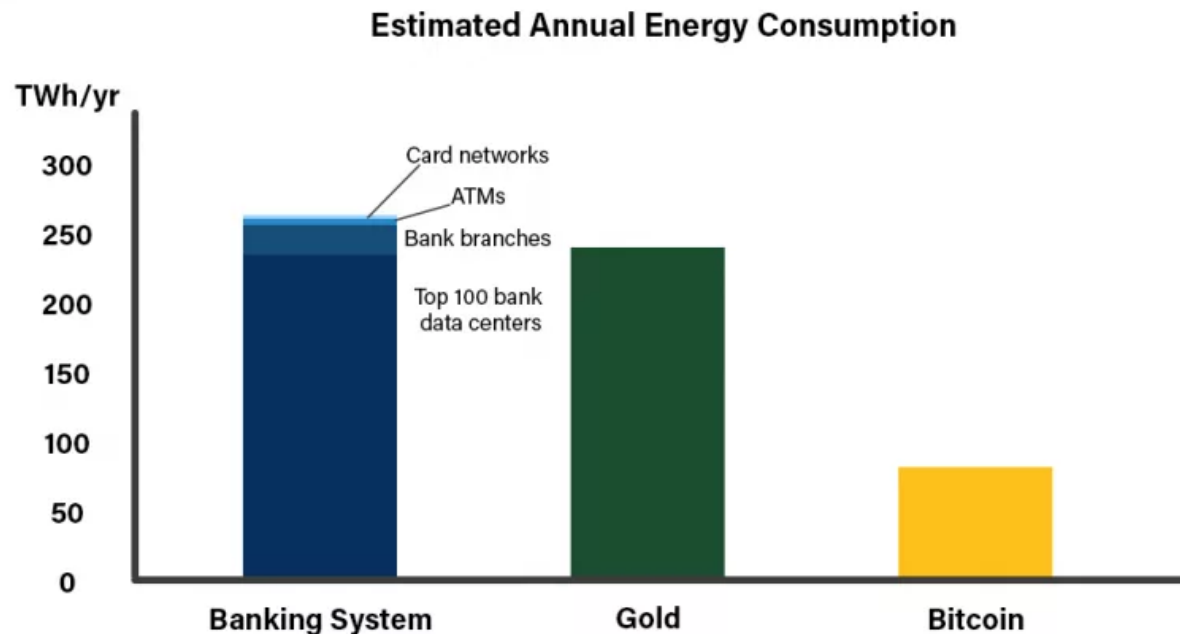
# How Much Energy Does Bitcoin Use?

- 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.



# World Needs Uncensorable Marketplaces

- As commerce moves online, transactions are increasingly subject to vetoes by middlemen who impose their values.
- why would anyone other than *a criminal* want to build a marketplace where anyone can take part and no product or service can be banned?
- Amazon and Walmart and eBay's house, eBay's rules
- **corporate censorship**
- the “illicit uses” category
- In the old world of physical stores and face-to-face business dealings, trade is almost always censorship-resistant by default

# Blockchain

- It is not owned by a single entity, hence it is *decentralized*
- The data is cryptographically stored inside (*secure*)
- The blockchain is *immutable*, so no one can tamper with the data that is inside the blockchain
- The blockchain is *transparent* so one can track the data if they want to

# Why Law enforcement would prefer criminals to use crypto?

- They could track where the funds went, identify what wallets came in contact with said funds, and if they have used a centralized exchange, they would be able to identify the individuals.

# Blockchain Technology

## (domain, keywords and symbols)

- Cryptocurrency (coins, addresses, wallets and exchanges)
- Transactions, Blocks, Hash function, Public Key Cryptography
- Remittance, Payment system(?), Stable coins,
- Mining, Consensus, Burning, Governance, Fees
- Smart contracts
- Tokenization and Virtual assets
- Supply-chain, Value-chain, Circular economy
- Scalability (Main chain, Side chain, Para chains..)

# News today (23 Jan)

- **CBDCs Could 'Revolutionize Global Financial Systems': Report by Bank of America**
- At least 114 central banks—representing 58% of all countries, which further generate 95% of global GDP—are now exploring Central Bank Digital Currencies ([CBDCs](#))
- “We view distributed ledgers and digital currencies, such as CBDCs and stablecoins, as a natural evolution of today’s monetary and payment systems.”
- **Why?** -current financial system's antiquated infrastructure and numerous inefficiencies

# BLOCKCHAIN



BITCOIN



BLOCKCHAIN



DISTRIBUTION



LEDGER



MINING



EXCHANGE



DATA ANALYTICS



CRYPTOGRAPHY



CHAIN



CONFIRMATION



TRANSACTION



MINER



MINING NETWORK



DIGITAL KEY



CLOUD MINING



SECURITY



CALCULATOR



GLOBAL NETWORKING



BITCOIN MOBILE



DIGITAL CURRENCIES



BLOCK REWARD



MINING



USER



INVESTMENT



WALLET



WHITE PAPER



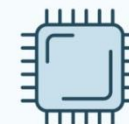
BLOCK



PORTFOLIO



MINING POOL



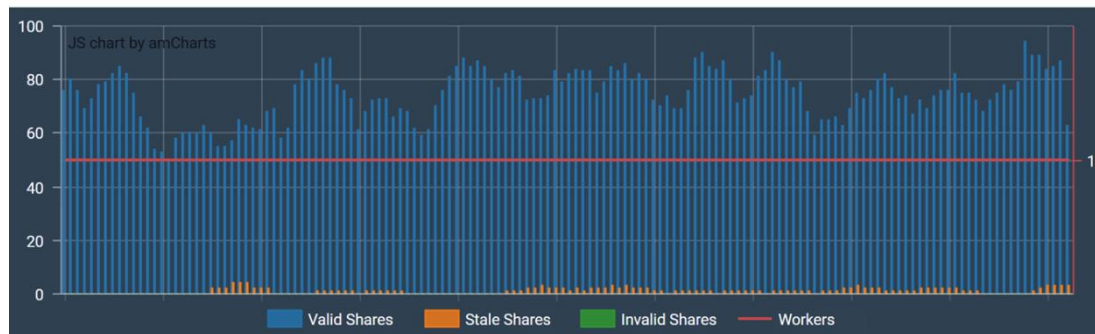
PLATFORM

gettyimages  
pop\_jop

# Minting coins: Mining experiment (May 2019) (**Don't do it!!**)



68h50m, Tesla V100 GPU – 100% (stopped on 22 May 2019 1340)



Yield ~ 0.02 ether (~5 USD)



# Concluding Remarks

- Don't waste resources in crypto-mining
- Don't get indulged into crypto-trading
- Ethics and integrity – Capacity building for the Global good
- We all have a responsibility to help advance financial inclusion, support ethical actors, and continuously uphold the integrity of the Blockchain ecosystem....

# Govt. of India stance 2019

- The draft bill proposes banning cryptocurrency-related activities in India  
(Terror funding, money laundering, black money)
- Heavy penalty and punishment of up to 10 years jail has also been proposed
- it proposes a jail term of one to 10 years for those who mine, hold, transact or deal with cryptocurrencies in any form, whether directly or indirectly through an exchange or trading
- Supreme court lifted India ban in March 2020

# Research and Education

- No person shall mine, generate, hold, buy or sell or deal in, issue, transfer, dispose of or use cryptocurrency in the territory of India
- (The draft clarifies that certain terms will not apply to any person using technology or processes underlying any cryptocurrency for the purposes of experiment or research including education provided that no cryptocurrencies are used for making or receiving payment in such activity)
- (It also clarifies that any law would not target blockchain or the use of Distributed Ledger Technology (DLT) for creating a network for delivery of any financial or other services or for creating value, without involving any use of cryptocurrency for making or receiving payment)

# Bitcoin 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.)

**Thank you  
for your attention**