



# Blockchain Technology – Introduction and Overview

Dhiren Patel, VJTI Mumbai  
Lecture(s)@FDP-BCT-2019



# Course objectives

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

# Course outcomes

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 and upcoming platforms
5. Learn to write smart contracts
6. Understand distributed application and design use-cases
7. Solve problems and create solutions..

# Why BCT/DLT?

- Records of transactions, based on certain agreed upon conditions form the basis for exchanging assets between two parties
- (the frictions in the processes, such as ascertaining the real owner of the asset, capital/asset is locked for days until the transaction is cleared, still exists as they could not be solved by technology until now).
- By maintaining an immutable, distributed ledger in a distributed network, blockchain and Distributed Ledger Technology (DLT) systems has the potential to reduce the friction in business networks and thus the operating cost for business transactions...

# Ledger

- ledger - an information store that keeps a final and definitive record of transactions
- Ledgers can be used to record transactions of almost any type: for example, the movements and transfers of physical objects.
- distributed ledger is a ledger that has its entries stored, across a series of nodes in a network, rather than in a single location
- tamper-resistant – transaction records, once entered into the ledger, cannot be altered without the alteration being clearly evident on inspection, whether the alteration is deliberate or accidental, malicious or benign
- tamper-evident - a system that has the desirable characteristic of enabling any unauthorized changes to be clearly visible

# Consensus

- Consensus in the context of DLT systems, addresses the problem of agreeing on the order of blocks
- in a potentially widely distributed system where there could be competing new blocks being added by multiple nodes across this network
- Consensus mechanisms figure out how all these independent nodes in the DLT come to an agreement about the contents and order of these blocks

# Proof of Work

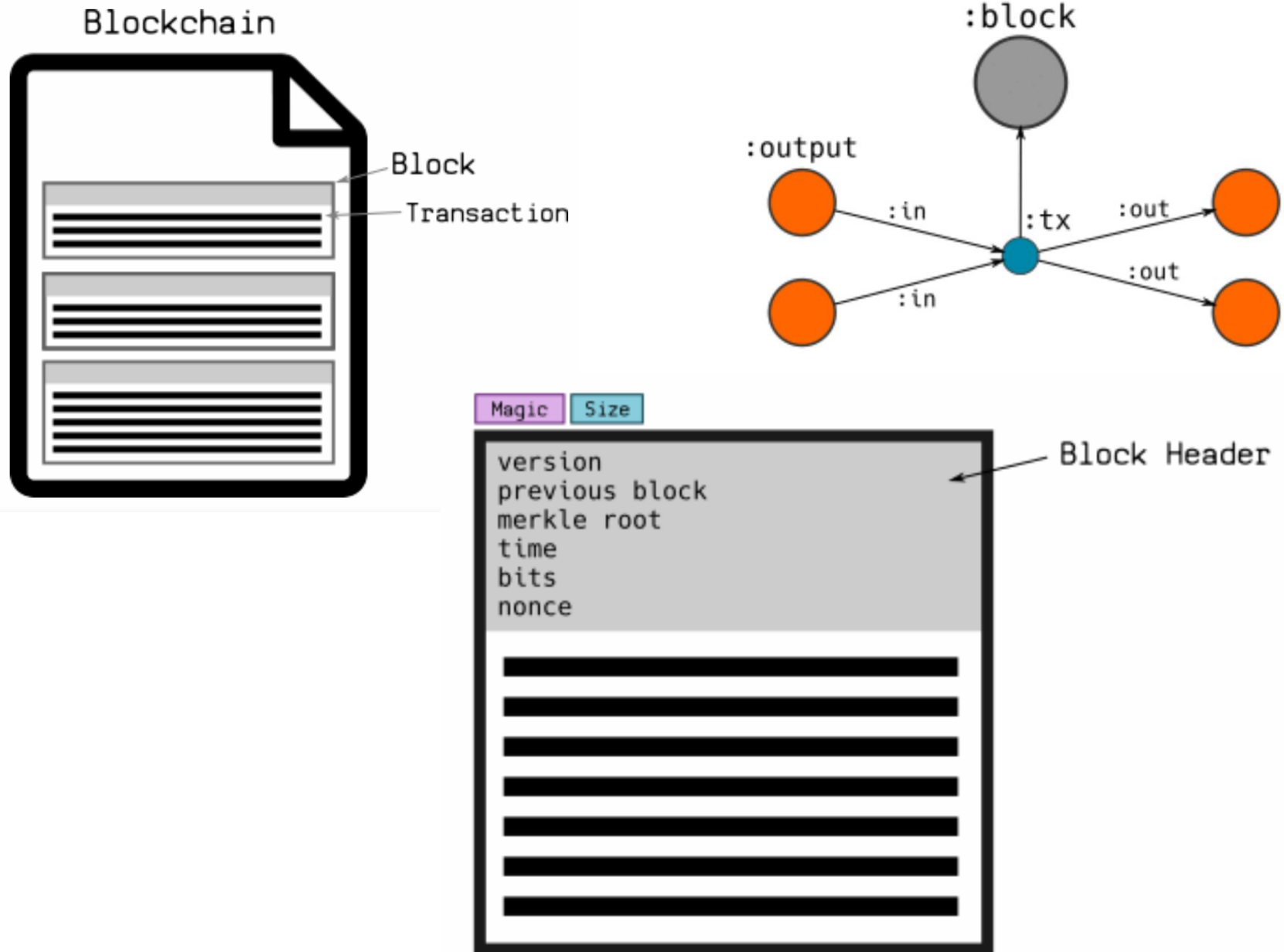
- Involves solving a computational challenging puzzle in order to validate transactions and create new blocks in the Bitcoin blockchain
- to link the new block to the last block in the valid blockchain
- the process is known as 'mining', and the nodes in the network that engage in mining are known as 'miners' - incentive in economic payoffs
- Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain (calculating the entire chain of 'hard mathematical problems')
- This protects the blockchain from tampering.
- Principle - A solution that is difficult to find but is easy to verify

# PoW and PoS

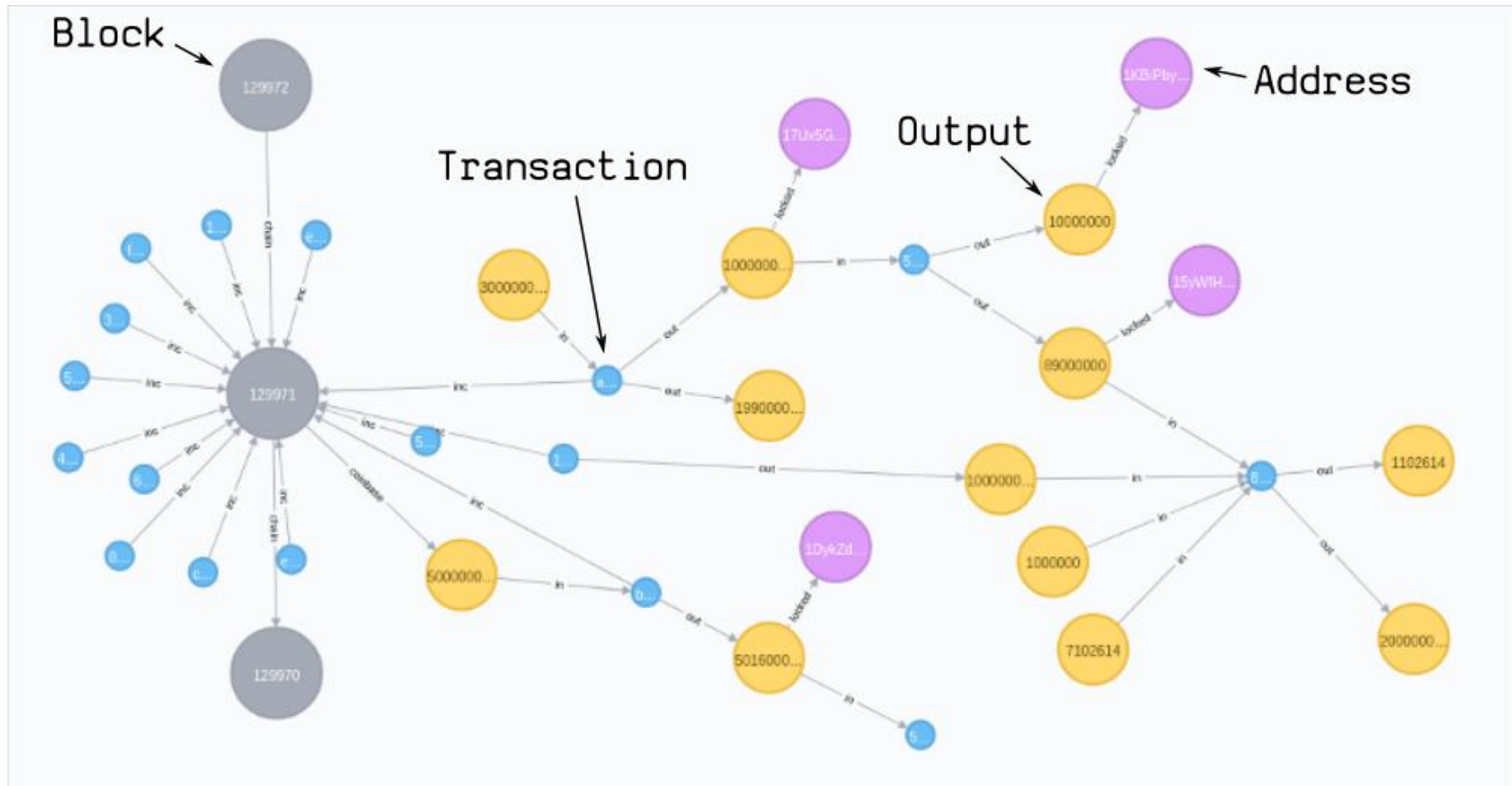
- Bitcoin Proof of Work –
- Given data A, find a number x such as that the hash of x appended to A results in a number less than B (to a number of leading 0's)
- Proof of Stake - the creator of the next block is chosen via various combinations of random selection and wealth or age (*i.e.*, the stake)



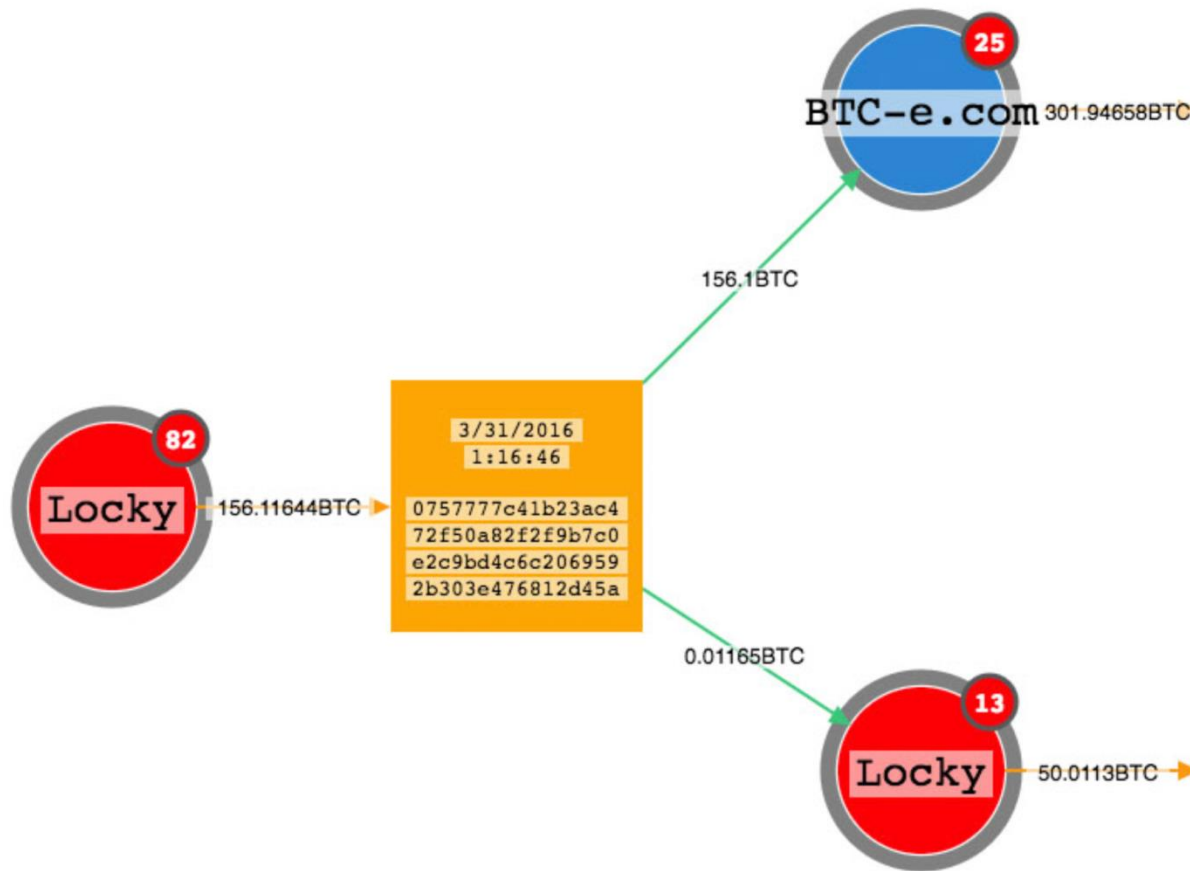
# Blockchain, block and transactions



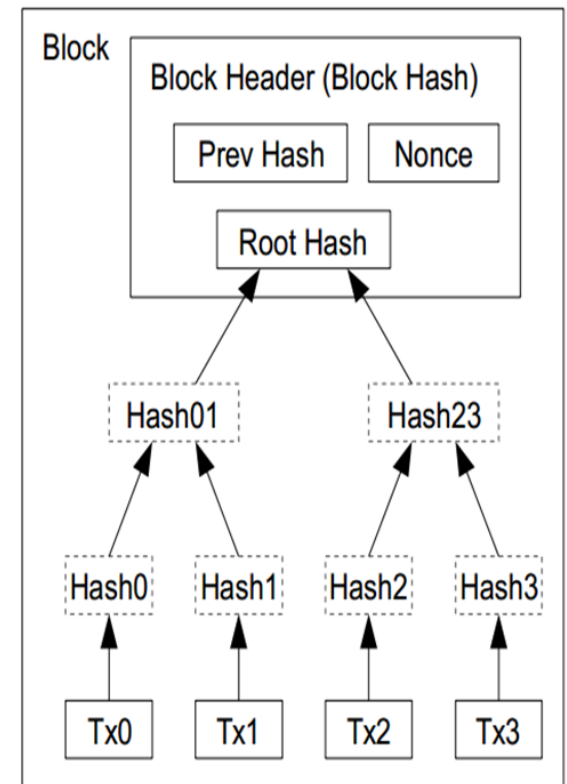
# Blockchain



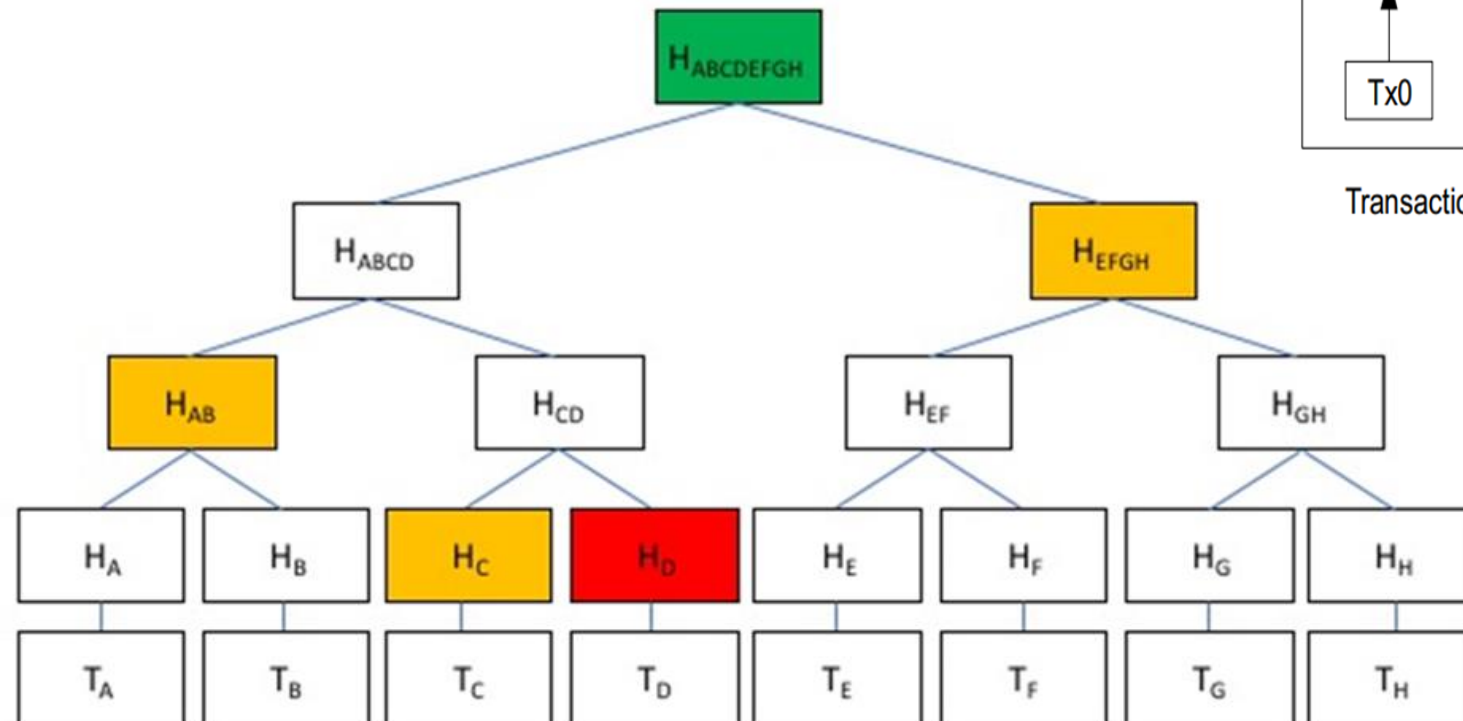
# Blockchain transaction



# Merkle Tree



Transactions Hashed in a Merkle Tree



# Bitcoin









- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008/2009
- Cryptocurrency - uses cryptography to control its creation and management
- Who is Nakamoto? Craig Wright?
- Effectively a bank run by an ad hoc network
  - A distributed transaction log
  - 1 BTC = 8200 USD (Sept 29, 2019)
- The hype surrounding Bitcoin has many starting to believe it may be a bubble – but....








# Some facts

- Cryptocurrencies: 2905
- Markets: 20998
- Market Cap: \$213,032,707,508
- 24h Vol: \$46,165,751,668
- BTC Dominance: 67.8%
- (Source: <https://coinmarketcap.com>)

# Cryptocurrencies








#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	 <b>Bitcoin</b>	\$144,455,489,958	\$8,040.95	\$13,005,462,023	17,964,975 BTC
2	 <b>Ethereum</b>	\$18,287,731,592	\$169.41	\$6,473,569,110	107,948,860 ETH
3	 <b>XRP</b>	\$10,357,506,978	\$0.240425	\$946,119,616	43,080,011,224 XRP *
4	 <b>Tether</b>	\$4,129,967,123	\$1.01	\$15,829,967,177	4,108,044,456 USDT *
5	 <b>Bitcoin Cash</b>	\$3,959,726,733	\$219.61	\$1,516,530,619	18,030,700 BCH
6	 <b>Litecoin</b>	\$3,426,571,209	\$54.08	\$1,854,783,137	63,363,854 LTC

# Cryptocurrencies

 <b>Monero</b>	\$963,945,669	\$55.93	\$59,094,655	17,233,953 XMR
 <b>Cardano</b>	\$960,526,369	\$0.037047	\$41,156,622	25,927,070,538 ADA
 <b>TRON</b>	\$883,240,683	\$0.013246	\$506,066,791	66,682,072,191 TRX
 <b>Huobi Token</b>	\$753,100,338	\$3.07	\$72,515,512	245,696,127 HT *
 <b>IOTA</b>	\$733,970,768	\$0.264063	\$3,332,158	2,779,530,283 MIOTA *
 <b>Dash</b>	\$628,447,978	\$69.33	\$184,275,507	9,064,516 DASH
 <b>Chainlink</b>	\$598,412,555	\$1.71	\$78,227,893	350,000,000 LINK *



# Exchanges

1	 BitMEX	\$1,945,073,339	\$21,619,950,029	\$78,603,463,200	1
2	 FCoin	\$1,174,570,785	\$5,800,251,354	\$34,696,459,348	60
3	 Fatbtc	\$874,293,034	\$5,875,125,829	\$25,383,447,191	120
4	 LATOKEN	\$832,990,099	\$5,395,794,144	\$25,091,907,274	259
5	 EXX	\$828,545,257	\$8,195,363,881	\$32,173,921,698	25
6	 BiKi	\$794,923,483	\$4,108,828,008	\$18,637,217,606	80
7	 BKEX	\$770,386,167	\$9,463,049,932	\$32,662,263,523	80

1D

5D

1 M

1 Y

5 Y

Max



1D

5D

1 M

1 Y

5 Y

Max



Max supply:  
\$21,000,000  
Current  
circulation:  
17,963,337  
Market Cap:  
\$147.5 B USD

# Bitcoin: Rise and Fall

## Rise (Feb-Dec 2017)



## Golden Age (17 Dec 2017 – for one month)



## Fall (since Feb 2018....) →



- Facebook: Libra (Coin) – Calibra (Wallet)

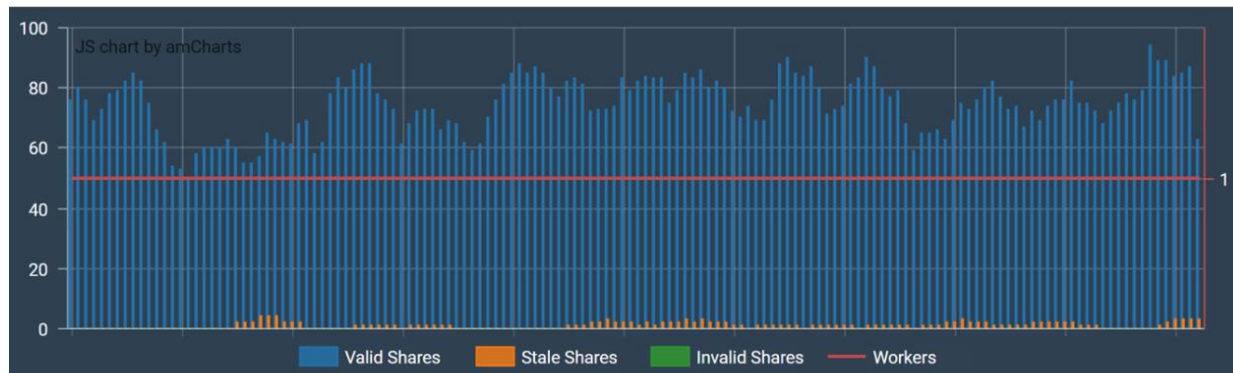
# India scene

- Banning of Cryptocurrency & Regulation of Official Digital Currency Bill 2019, India
- No person shall mine, generate, hold, buy or sell or deal in, issue, transfer, dispose of or use cryptocurrency in the territory of India
- Why?
- Exception - 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

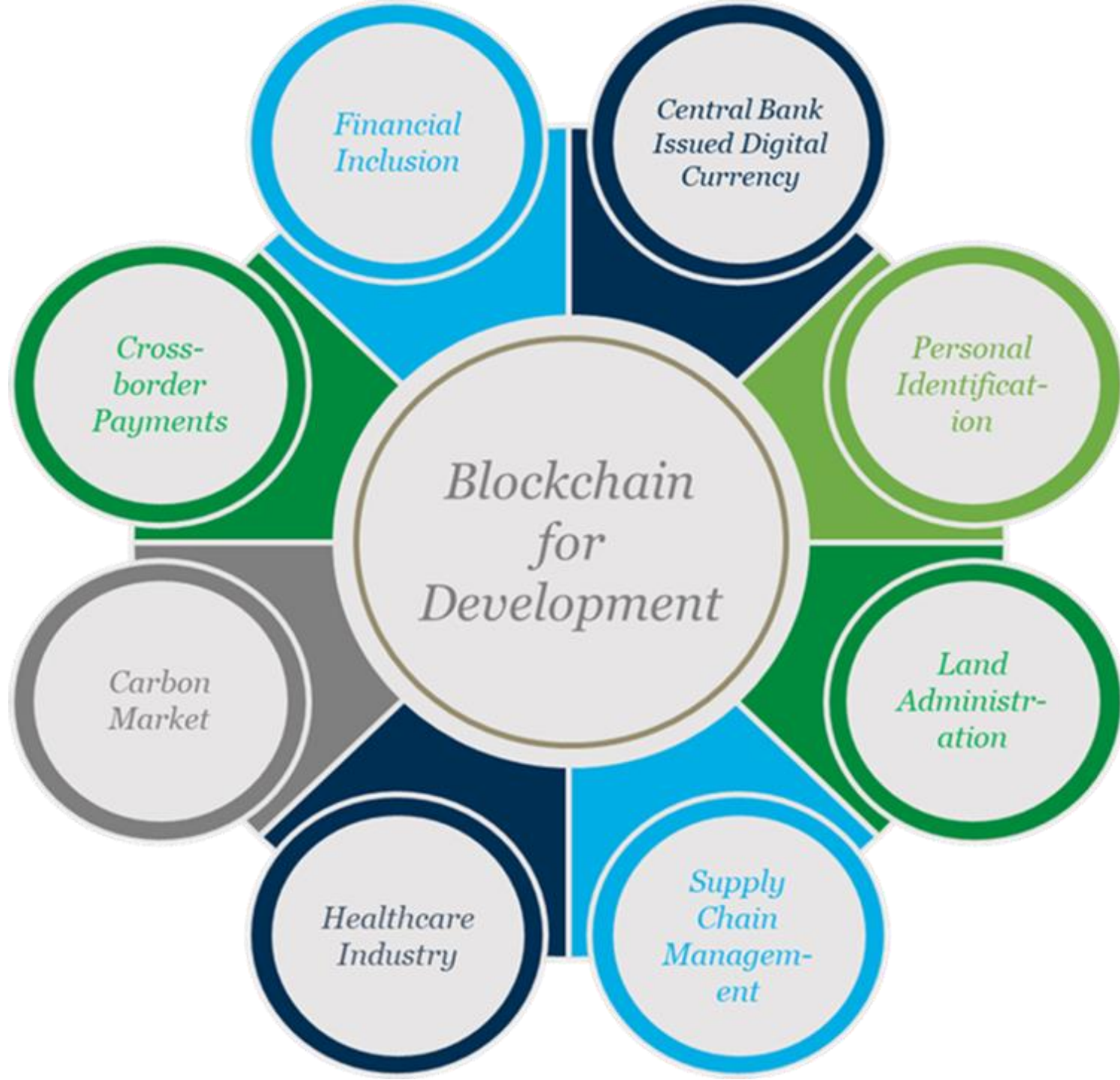
# Mining experiment (Don't do it!!)



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



Yield ~ 0.02 ether (~5 USD)



# BCT and DLT

- While historically, the focus has been facilitating the exchange of assets, this technology can also be used as a broader solution to public reporting and auditing requirements



# Use cases

- Supply Chain Management
- (medicine supply)
- (Farm to plate)
- (Music industry)
- Agriculture Insurance
- Construction Blockchain
- Crypto wills
- Pothole complaint and resolution in Metropolitan area....

# Moving forward in Blockchain space

- We all have a responsibility to help advance financial inclusion, support ethical actors, and continuously uphold the integrity of the Blockchain ecosystem....
- Ethics and integrity – Capacity building for Global good

# BitCoin: Challenges

- Creation -- How is it created in the first place?
  - What prevents anyone from creating lots of coins?
- Validation - Is the coin legit? (proof-of-work)
  - How do you prevent a coin from double-spending?
- Buyer and Seller protection in online transactions
  - Buyer pays, but the seller doesn't deliver
- Trust on third-parties - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank or clearing house

# Information Security objectives

- Cryptography, Information Security, Cyber Security, Network Security, Web Security
- Data Confidentiality (Encryption Algorithms)
- Data hiding (Steganography)
- Data Integrity (Hash functions)
- Authentication (Identity and Access Management)
- Non-repudiation (Digital signature)
- Privacy, Anonymity, Security Policy
- Vulnerability Assessment and Penetration Testing...
- Zero Knowledge Proof (Ack: Prof B Roy)

# Attacks

- Theft of sensitive information
- Disruption of service
- Illegal access to resources
- E.g. Stealing credit card details
- E.g. Ransomware
- E.g. Resource (Compute) Hijacking for Cryptocurrency Mining

# Crypto Key management issues

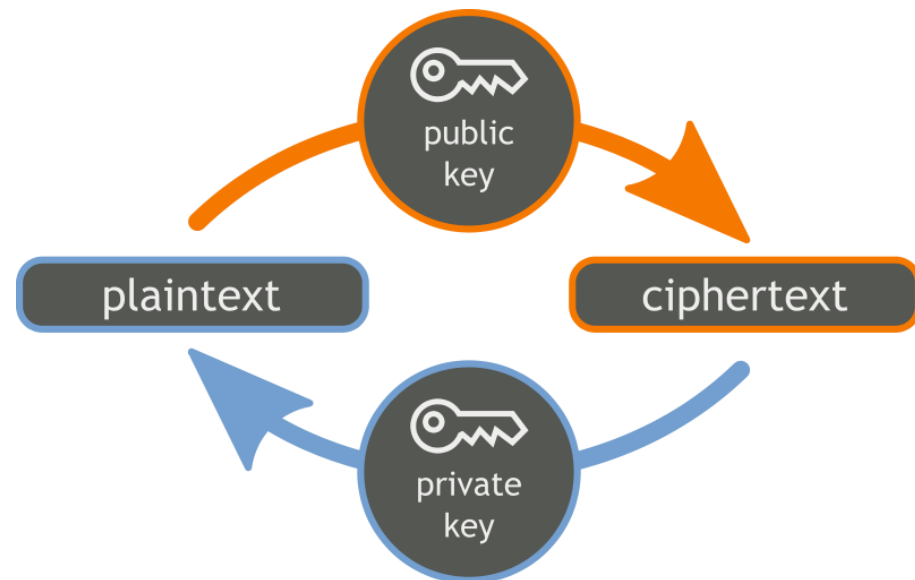
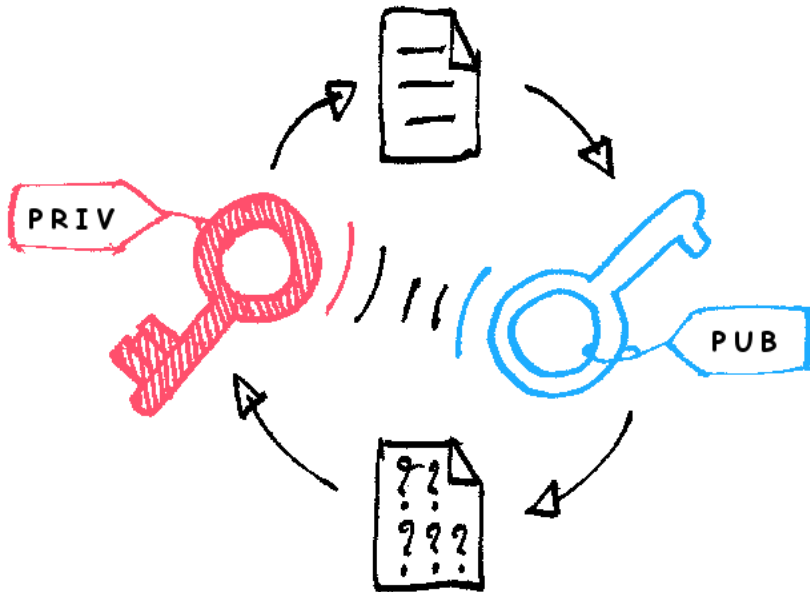
- SKC (Symmetric key cryptography)
- 1 user wishes to communicate with another user – requires 1 key (**secure key sharing??**)
- 1 user wishes to communicate with 2 users – requires 2 keys
- N users – wish to communicate to each other – require  $N*(N-1)$  keys!!!  $\rightarrow O(n^2)$
- PKC (Public Key Cryptography)
- N users require –  $2N$  keys (each has pair of keys)!!
- (**un-secure key sharing**, public keys!!!)
- Key generation, Key exchange (distribution), Key management (expiry, revoking)

# Public key cryptography

(each user has a key-pair)

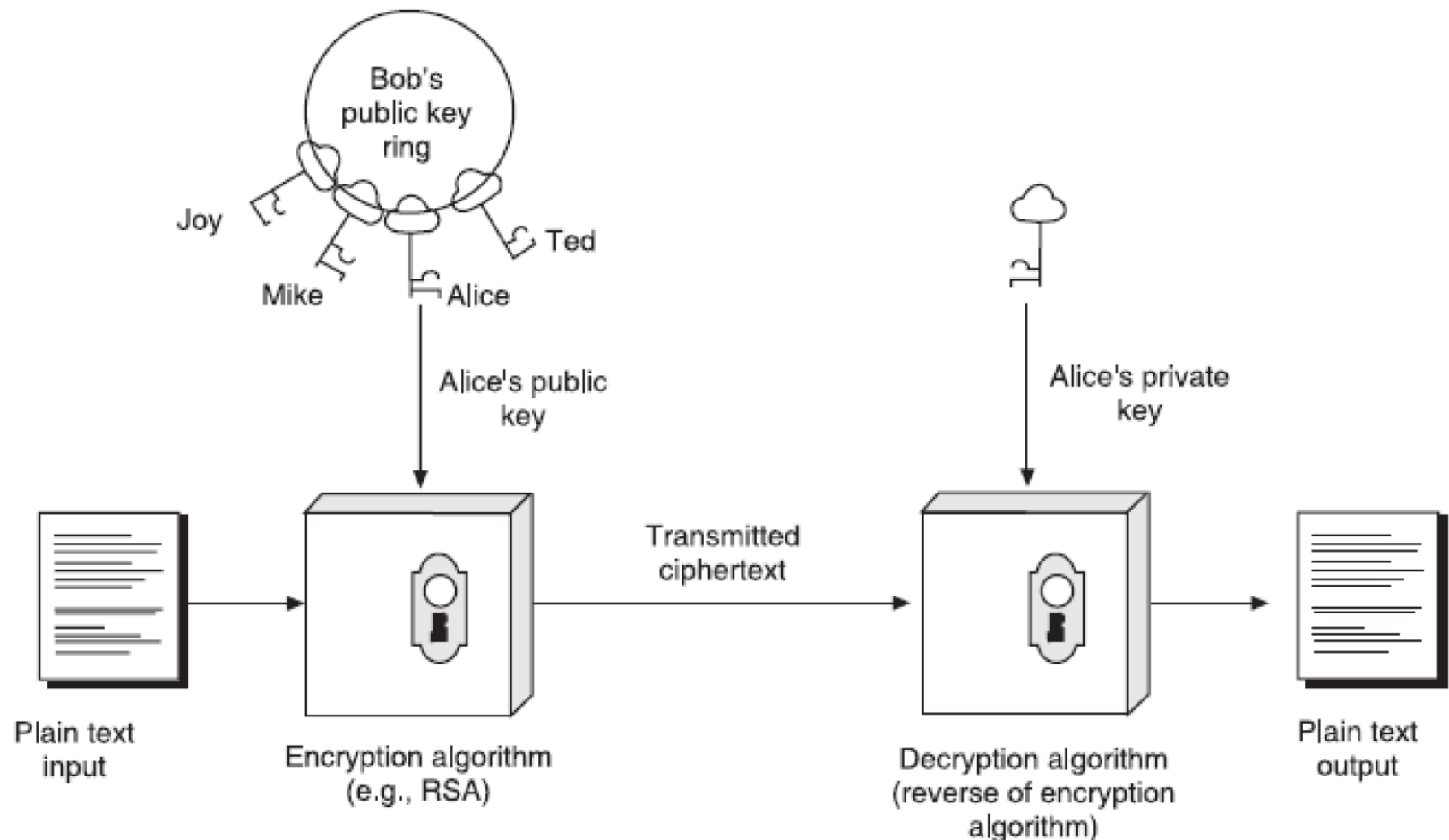
Public key is published – known to all

Private key is known to user himself/herself



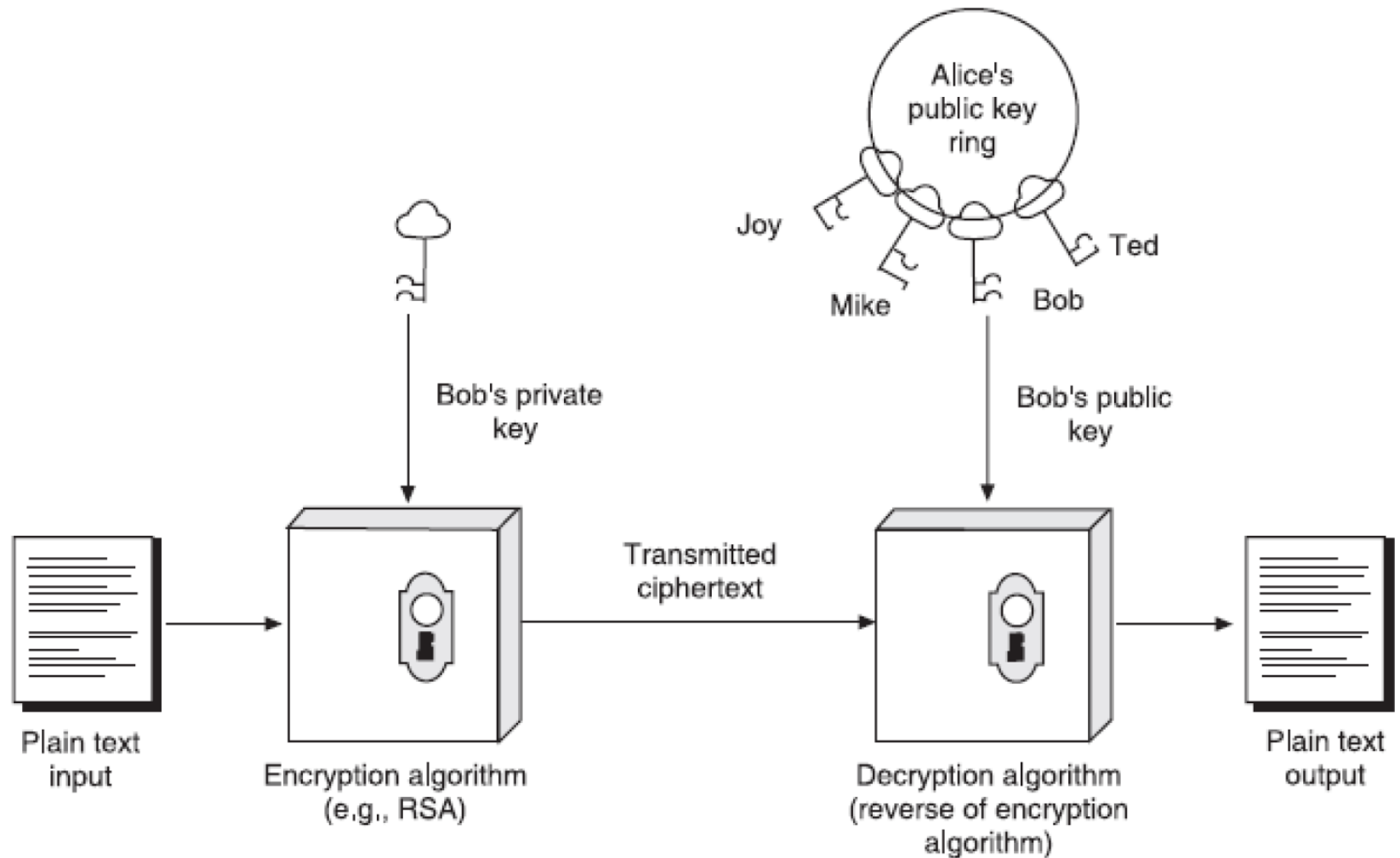
# Public key ring

## PKC Encryption





# PKC in Authentication

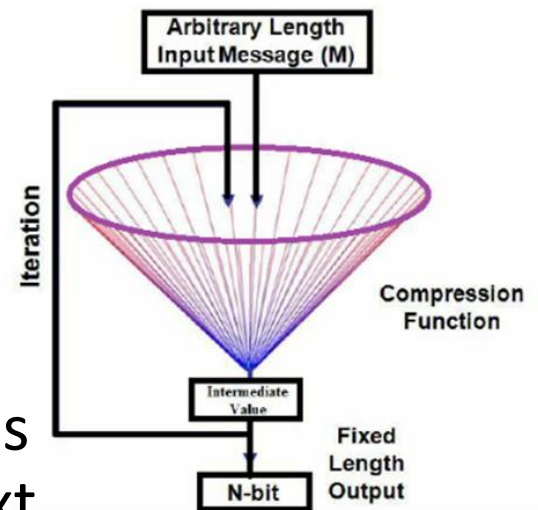


# Cryptographic hash functions

- **Hash Function:** takes input (of variable-length) and returns a fixed size output string  $h$  (usually much smaller than input)

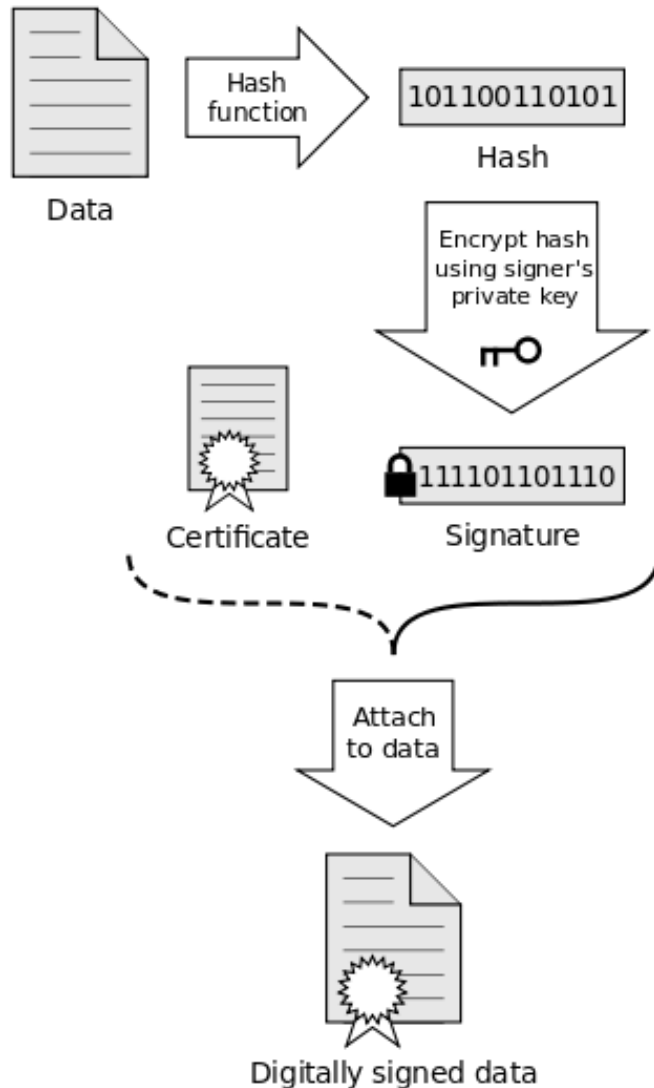
$$H: \{0,1\}^* \rightarrow \{0,1\}^n, \quad h = H(M)$$

- One way
- A block cipher is a function which maps  $n$ -bit plaintext blocks to  $n$ -bit ciphertext blocks
  - $E: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$
- To allow unique decryption, the encryption function must be one-to-one

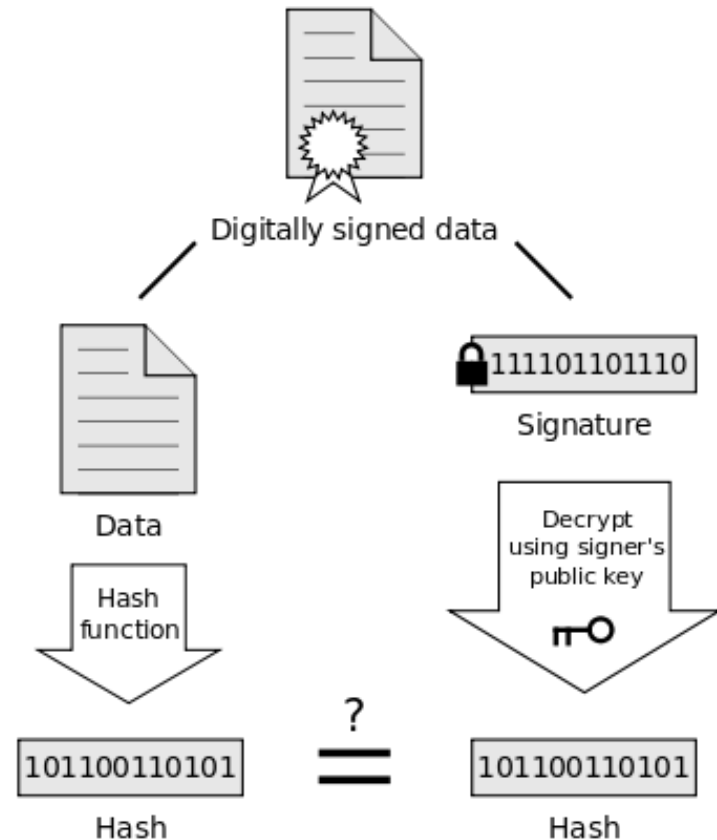


# Digital Signature

## Signing



## Verification



If the hashes are equal, the signature is valid.

# Blockchain

- Blockchain is a distributed ledger with confirmed and validated blocks organized in an append-only chain using cryptographic links
- Form of a database (replicated across nodes)
- Transaction(s) → Blocks → Blockchain
- Append-only tree data structure
- Managing the append of the new valid blocks
- Blockchain must contain only blocks that satisfy a given predicate

# Blockchain characteristics

- Blockchain/DLT (Distributed Ledger Technology) offers four unique inherent characteristics under certain conditions depending on design and/or implementation:
  - Immutability
  - Traceability
  - Transparency
  - Distributed

# Blockchain properties (requirements)

- Validation and Synchronization
- Consensus and Update Agreement
- Partition-prone message-passing system
- A formalization of distributed ledgers
- the Monotonic Prefix Consistency
- Distributed maintenance of the Blockchain by many (distrusting) parties makes it achieving “distributed consensus” in real time

# Security in Bitcoin

- Authentication (PKC – Digital Signatures)
  - Am I paying the right person? Not some other impersonator?
- Integrity (Hash and Chain of Digital Signatures)
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability (Message broadcast on P2P network)
  - Can I make a transaction anytime I want?
- Confidentiality (pseudo anonymity)
  - Are my transactions private? Anonymous?

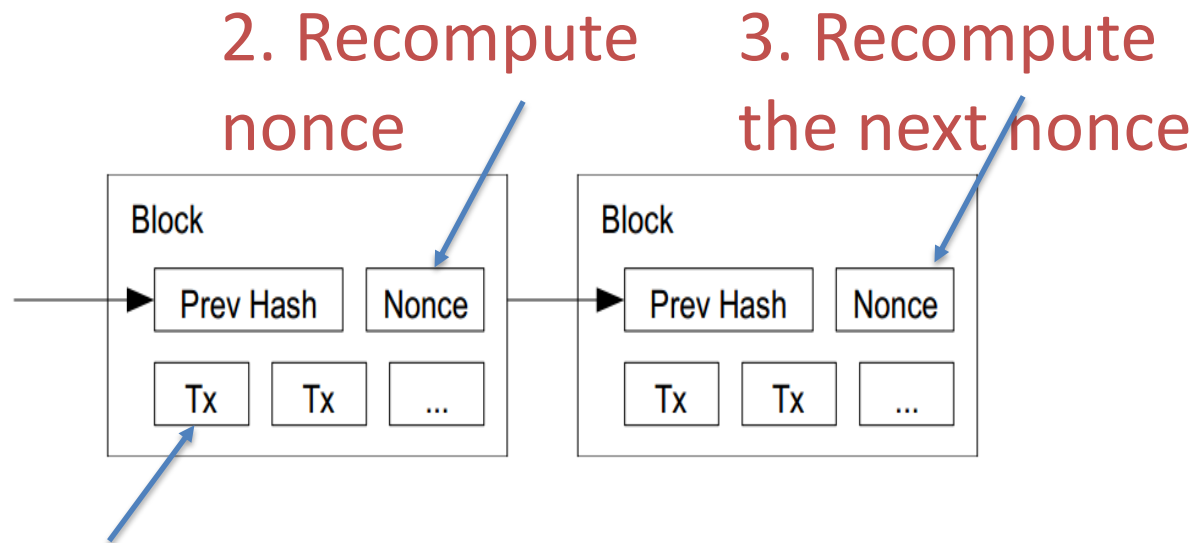
# Back to BitCoin challenges

- Validation
  - Is the coin legit? (proof-of-work)
    - Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending?
    - Broadcast to all nodes (Each node verifies that this is the first spending of (unspent) bitcoin by the payer)
- Creation of a virtual coin
  - How is it created in the first place?
    - Provide incentives for miners
  - What prevents anyone from creating lots of coins?
    - Limit the creation rate of the Bitcoins



# Reverting (changing tx) is Hard

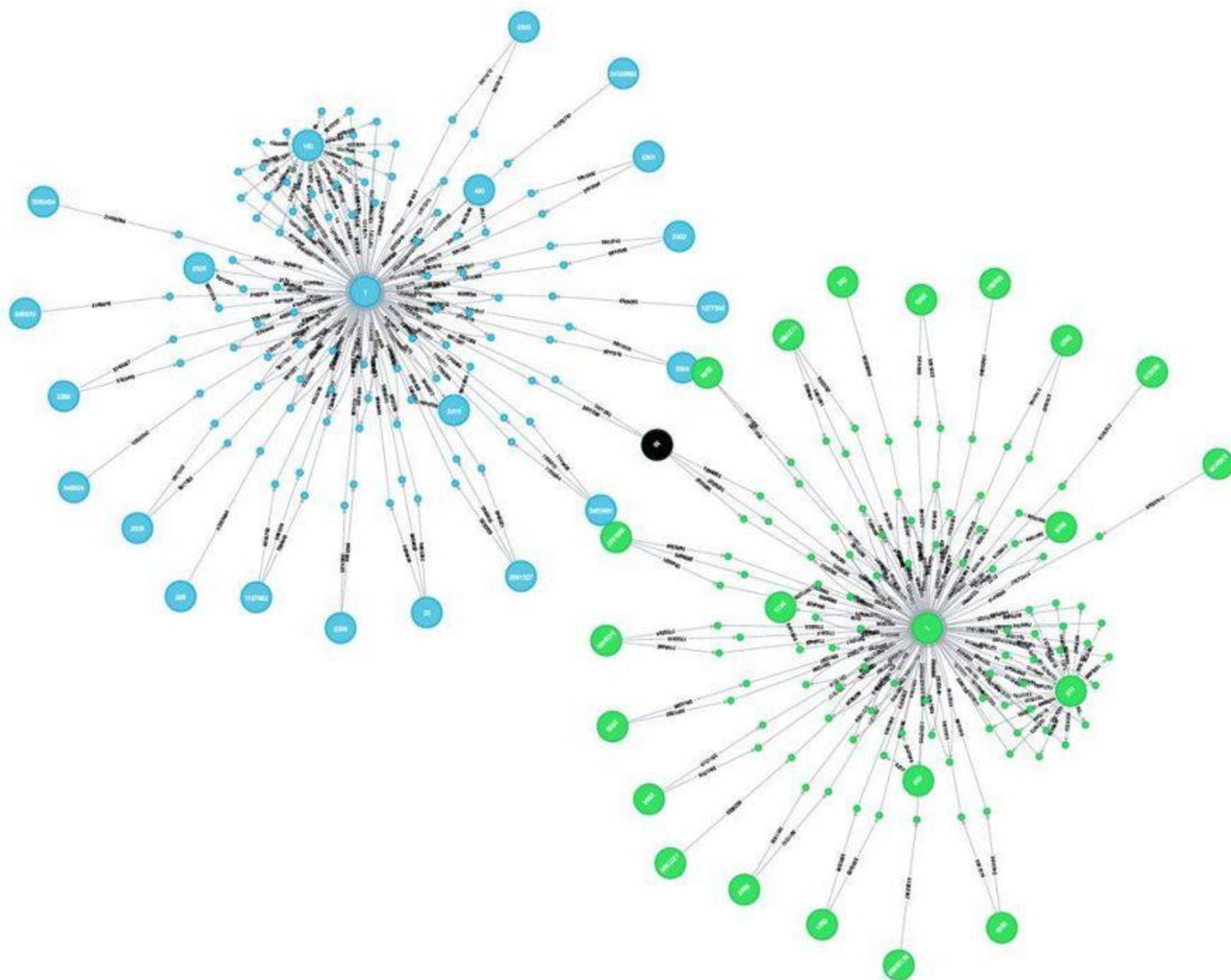
- Reverting gets exponentially hard as the chain grows



1. Modify the transaction  
(revert or change the payer)

# Practical Limitation

- 10 mins to verify a transaction
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction (\$\$\$) wait longer. Because if you wait longer it becomes more secure.
  - For large \$\$\$, you wait for six blocks (1 hour)



# Blockchain Basics (list)

- Keys
- Addresses
- Wallets
- Transactions
- Scripting
- Mining
- Consensus
- Forks



## Core issues



- Volatility, Usability
- No Ease of use (private key management)
- User community, Developer community
- Incentive to mine and validate?? (Energy cost, waste)
- Nothing for small User
- Trading interest

VJTI Blockchain pic.

# Bitcoin v/s Ethereum

- Bitcoin is more a cryptocurrency, Ethereum is a token capable of facilitating smart contracts
- Bitcoin and Ethereum are powered by their native coin BTC and ETH
- Both use proof-of-work (POW) consensus mechanism
- Ethereum plans to move on to proof-of-stake (POS)
- BTC – 21M, ETH – no cap (~15M a year)
- Satoshi Nakamoto (Jan 2009), Vitalik Buterin (July 2015)
- Satoshi –  $10^{-9}$  BTC, Wei –  $10^{-18}$  Ether
- Miner fees - Transaction fees, Gas fees
- Reward – 12.5 BTC, 2 ETH
- Validation time - 10 min, 15 sec

# Consensus mechanisms

- Proof of Work,
- Proof of Stake,
- Delegated Proof of Stake,
- Proof of Authority,
- Proof of Contribution,
- Proof of Burn...



# Blockchain properties

- Immutability (Append-only tree data structure)
- Traceability and Transparency
- Distributed
- Validation and Synchronization
- Consensus and Update Agreement

# Blockchain foundations

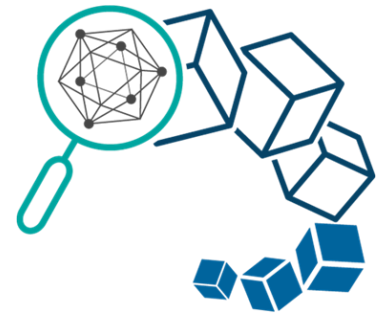
- Confidentiality (SKC, PKC)
- Integrity (Hash function)
- Authentication (Passwords)
- Non-Repudiation (Digital signature)
- Privacy
- Anonymity
- Hash function – PoW computation
- Merkle tree – organizing transactions in block, blockchain
- Wallet – address, private key/public key

# Sustainability

- Utility ecosystem (to support business environments, fast track onboarding for interconnected clients, easy spend/usage across variety of services/dAPPs (interoperable), incentive to hold/store, incentive to spend, incentive to support, rolling economy)
- Rewards and fees: incentives to mine, incentive to validate, incentive to support/contribute, incentive to develop dAPPs
- Trust, Fraud detection and prevention
- Formal verification of participating entities (Block producers, Smart contract runners, Super node,
- GDPR compliance, Privacy v/s KYC and AML compliance
- Forward Value and easy Exchange
- QoS benchmarks

# Addressing issues:

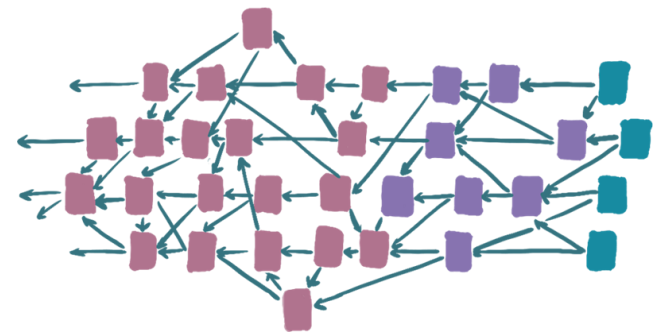
## Different Blockchains



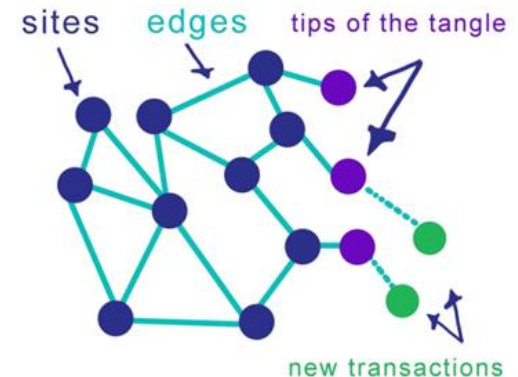
- Scalability, Security, Usability, Sustainability
- Consensus mechanisms: PoW, PoS, DPoS  
PoA, PoC, AI-DPoC
- Extension: Main chain, off chain, side chain, Sharding
- Community – Mass Adoption???
- Bitcoin, Ethereum, Hyperledger, Ripple, Hashgraph, IOTA, QLDB ...
- “How could Blockchain technology potentially benefit us?” rather than “How can we make our problem fit into the Blockchain technology paradigm?”
- Use cases



# Moving forward beyond Cryptocurrencies



- Blockchain - a data structure of back-linked list of blocks of transactions, ordered with respect to time and provides tamper evident log
- Immutable records, Supply Chain Management
- Blockchain ecosystems (rather than coins)
- Day-to-day use
- Smart contracts (Ethereum , Solidity)
- Specialized use – IOTA
- dAPPs (beyond BitTorrent...)



# Scalability factors

- Consensus mechanism
- Block generation / production (Incentive v/s Energy consumption (difficulty level))
- Block size
- Network Delay
- Transaction Finalization Time (TFT)
- No of blocks required for Confirmation
- Block level or Transaction level confirmation (tangle, hash graph, hyper ledger)
- Extension innovations (Main chain, Side chain, off chain etc.)

# Consensus Mechanisms



- Based on Behaviours, Risk factors, and Governance model
- (majority <percentage> is predefined by a policy, Collaborative, Cooperative, Inclusive, Participatory)
- Proof of Work (PoW) //processing time, difficulty level
- Proof of Stake (PoS) //to hold stake
- Proof of Burn (PoB) //destroy stake for commitment
- Proof of Elapsed Time (PoET) //wait time
- Delegated Proof of Stake (DPoS) //approval to selected
- Proof of Activity – mix between PoW and PoS, Proof of Stake Velocity (PoSV), Proof of Importance (PoI)
- Proof of Reputation (PoR) //to keep network secure
- Proof of Authority (PoA) with ZKP (Zero Knowledge Proof)
- Artificial Intelligence Delegated Proof of Contribution (AI-DPoC)

# Blockchain Analysis

- Process of inspecting, identifying, clustering, modelling and visually representing data of a blockchain
- Useful for discovering knowledge about actors transacting on the chain
- Data in most blockchains are public meaning that anyone can harness the addresses.
- By using **common-spend clustering algorithms**, it is possible to map the spendings of certain entities on the blockchain



bitcoin-24

deepbit  
slush

bitcoinica

bitcoin.de

ozcoin

silk road

mybitcoin

btc-e

instawallet

okpay

bitstamp

bitfloor

bitpay

glbse

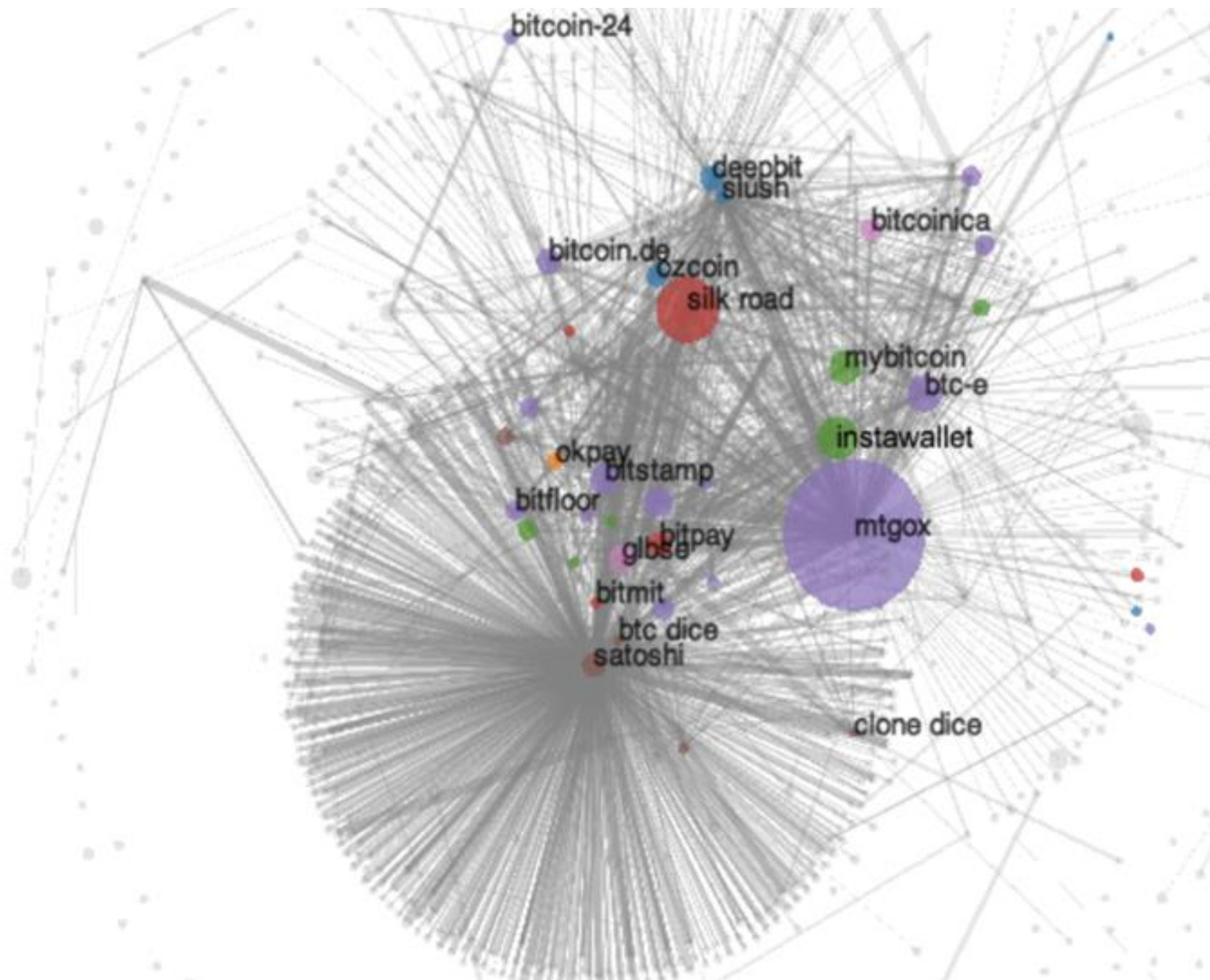
bitmit

btc dice

satoshi

mtgox

clone dice



# Money Flow - Tracking and Tracing

- Tracking - looking for transactions that **use this transaction output and its subsequent transactions** (forward direction)
- Tracing - looking for transactions that **result in this transaction output and its previous transactions** (backward direction)
- **User Deanonymization** - Analyzing the underlying network protocol to map wallet addresses to **(probable)** IP addresses.

# Standardization efforts ISO/TC 307 BCT and DLT (22739 to 23244 series)

Permission

Consensus

Incentive Mechanism

Application – universal or domain specific

Security and Risk management

ISO TC 307 Meeting – Nov 19-23 2019

Hyderabad, India

Standard and/or project under the direct responsibility of ISO/TC 307 Secretariat (11)	↓ Stage ↑	ICS
<a href="#">ISO/CD 22739</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Terminology	30.60	35.030 35.240.40 01.040.35 35.240.99
<a href="#">ISO/NP TR 23244</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations	10.99	
<a href="#">ISO/NP TR 23245</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities	10.99	
<a href="#">ISO/NP TR 23246</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies	10.99	
<a href="#">ISO/AWI 23257</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Reference architecture	20.00	
<a href="#">ISO/AWI TS 23258</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Taxonomy and Ontology	20.00	
<a href="#">ISO/AWI TS 23259</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Legally binding smart contracts	20.00	
<a href="#">ISO/CD TR 23455</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	30.00	35.030 35.240.40 35.240.99
<a href="#">ISO/NP TR 23576</a> <a href="#">[Under development]</a> Blockchain and distributed ledger technologies -- Security management of digital asset custodians	10.99	