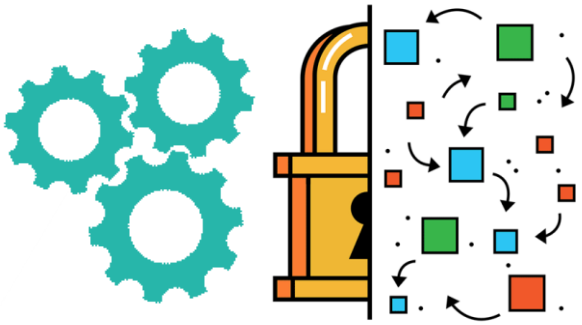
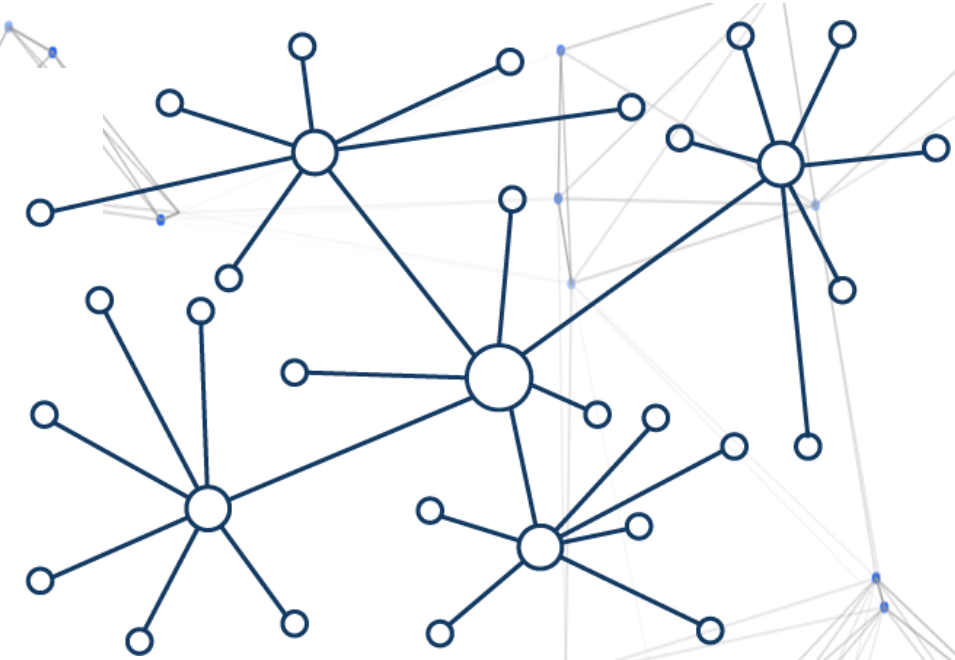




Blockchain: Scalability and Sustainability - Challenges or Opportunities?

Dr. Dhiren Patel

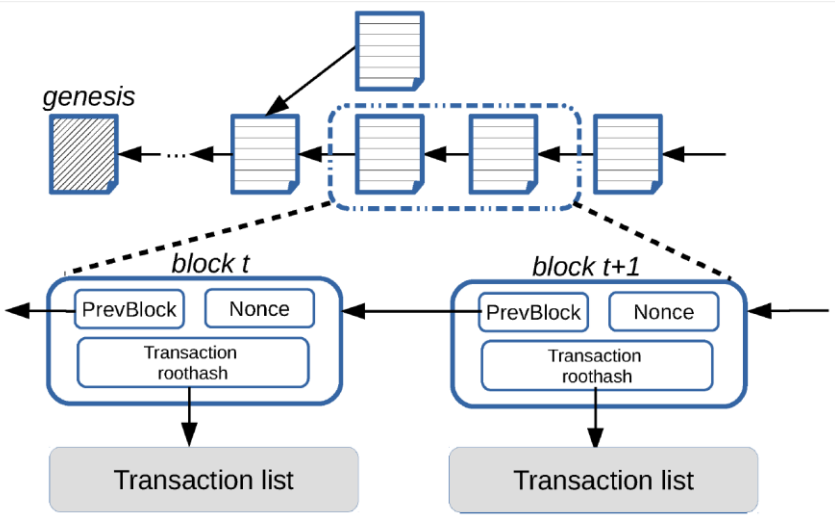
Technical Advisor

EcoVerse™

DeLight Chain

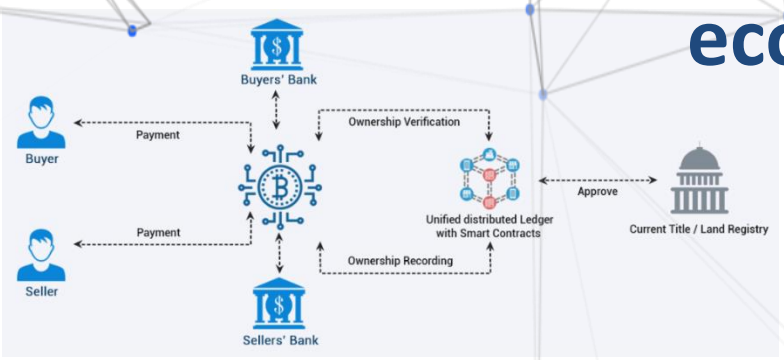
Blockchain

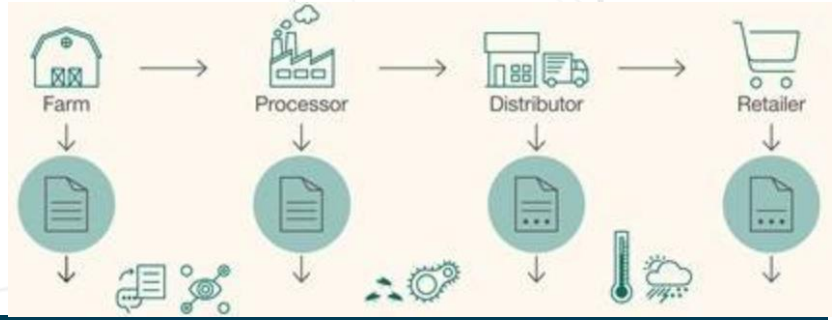
- propagated and synchronized among the nodes via a p2p protocol and a consensus mechanism
- Blockchain capability - create, validate, authenticate and audit contracts and agreements in real-time, across borders, without third-party intervention
- Bitcoin is invented to disrupt the “status-quo”. It came to resolve utter disappointment with corruption in financial institutions and the governments that propped them up

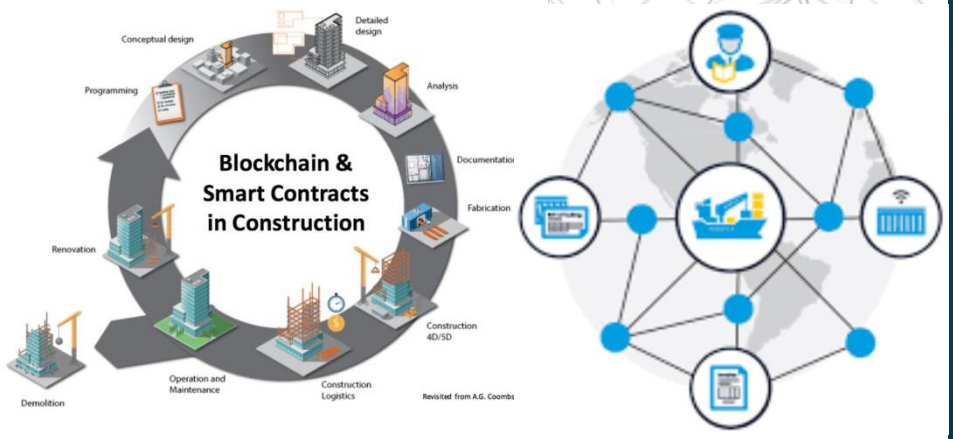


Blockchain is a data structure - back-linked list of blocks of transactions, ordered wrt time – provides tamper evident log

From bitcoin blockchain to all purpose blockchain ecosystem



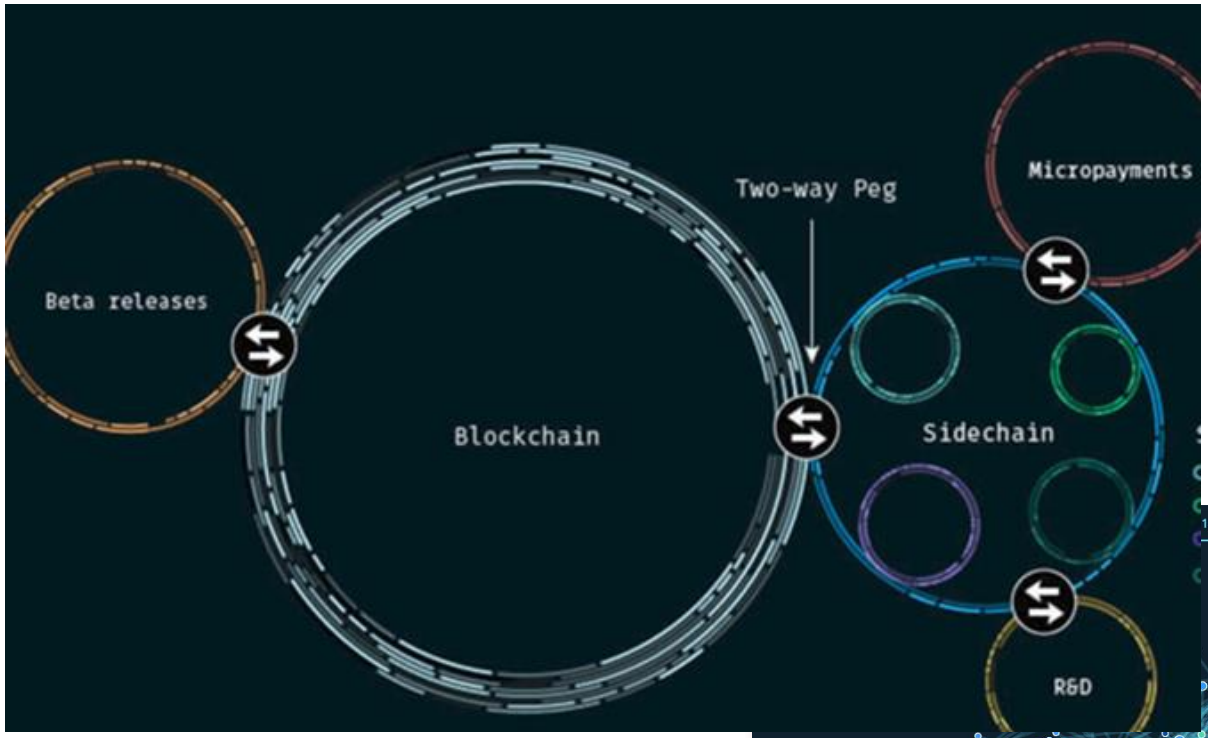


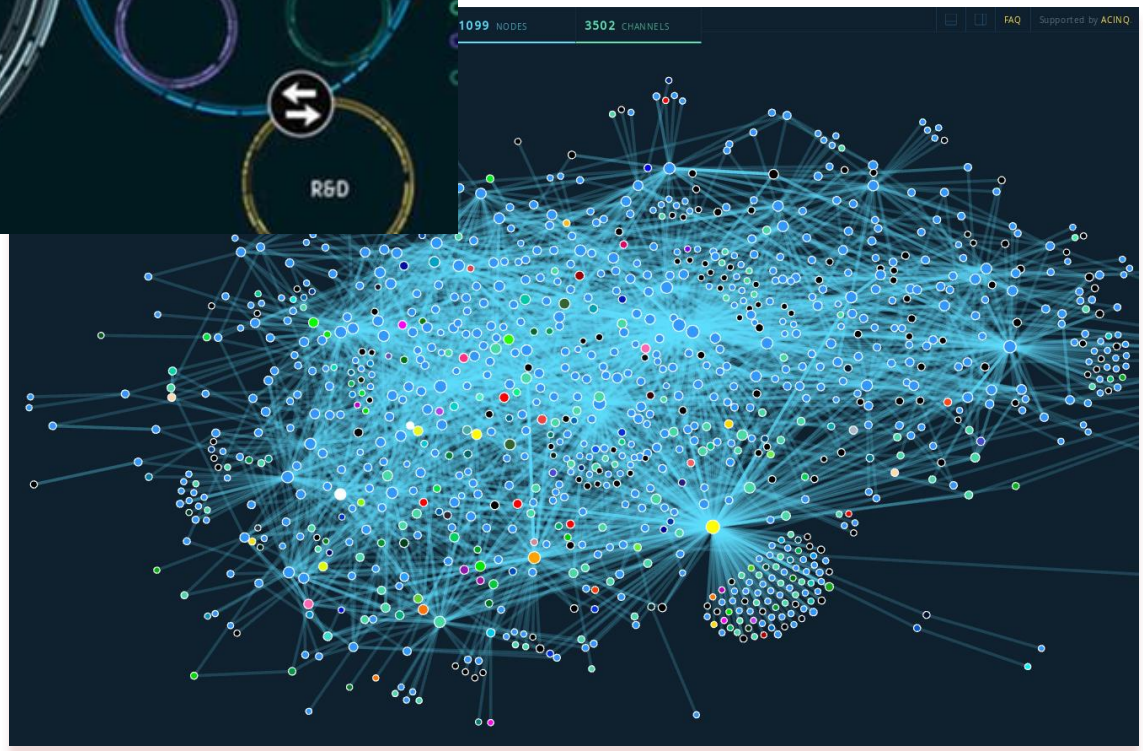


Scalability factors

- 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
- Transaction level confirmation (tangle, hash graph, hyper ledger)
- Extension innovations (Main chain, Side chain, off chain etc.)

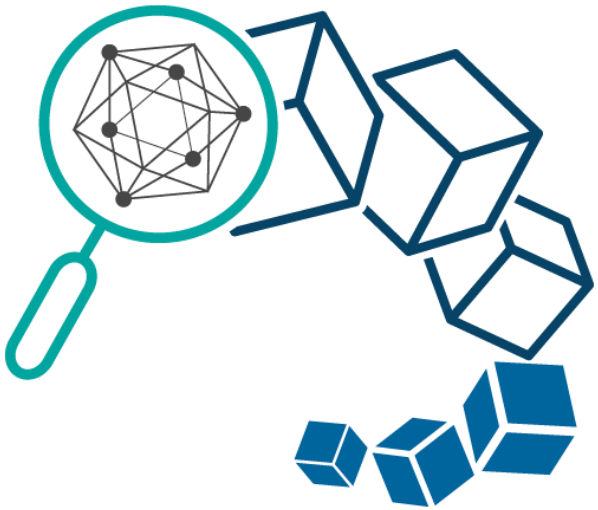
Side chain and Lightning network

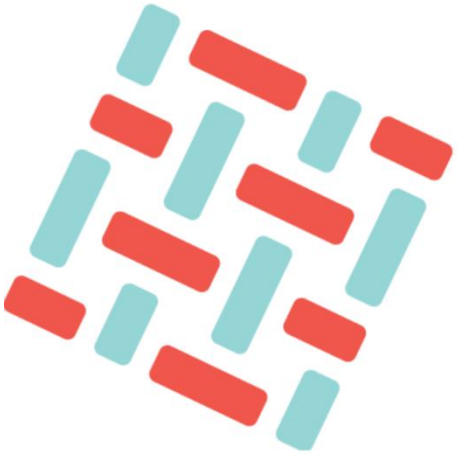




Towards Scalability

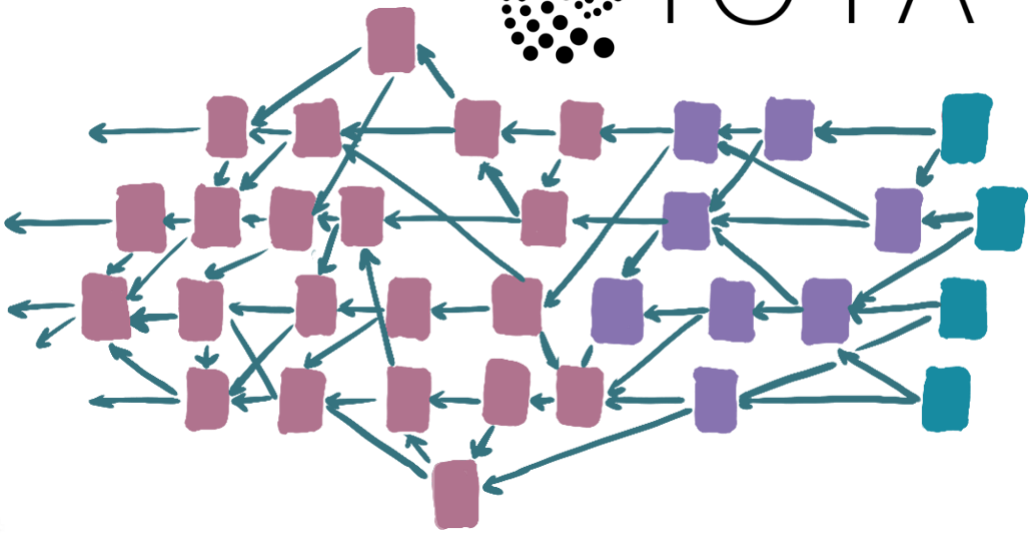
ethereum





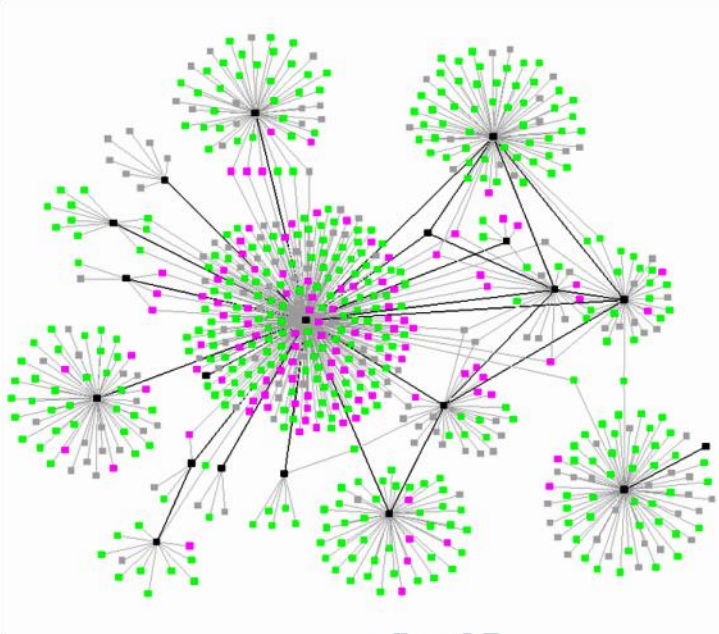
HYPERLEDGER
FABRIC

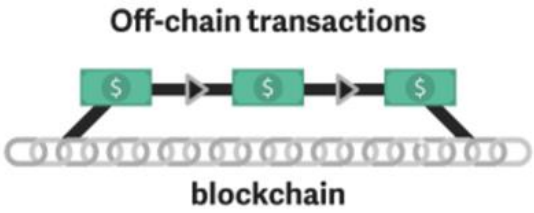
IOTA

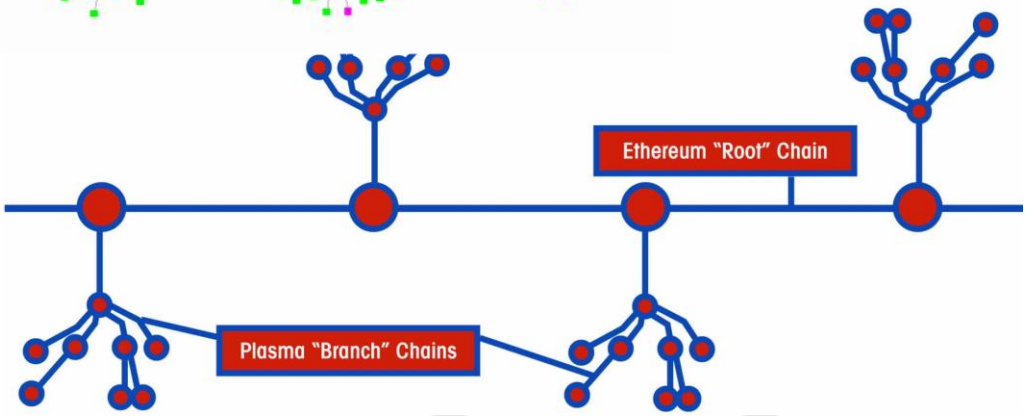


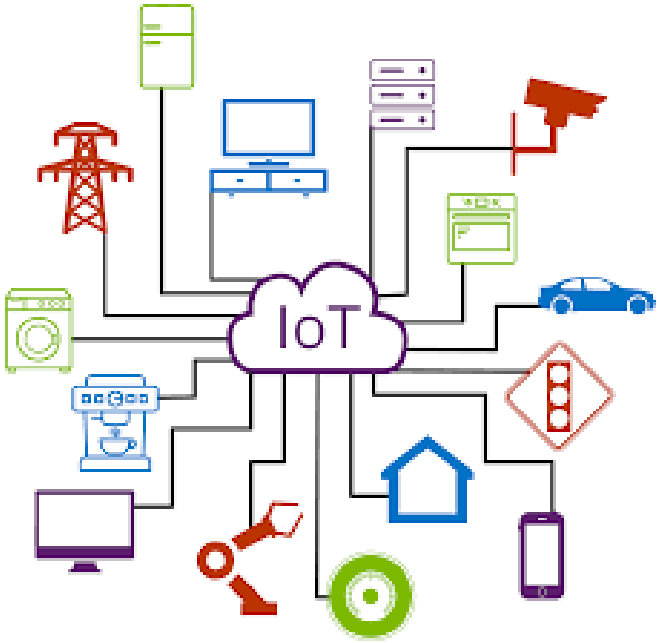
Hycon

Plasma framework

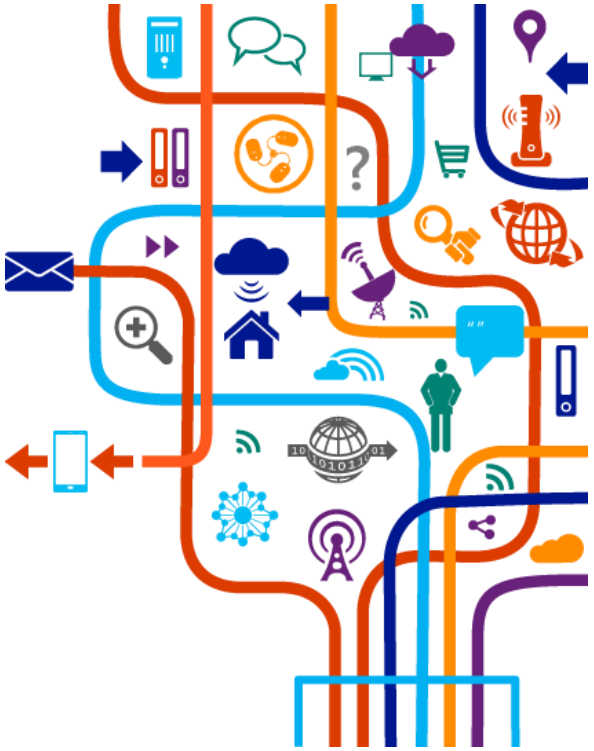


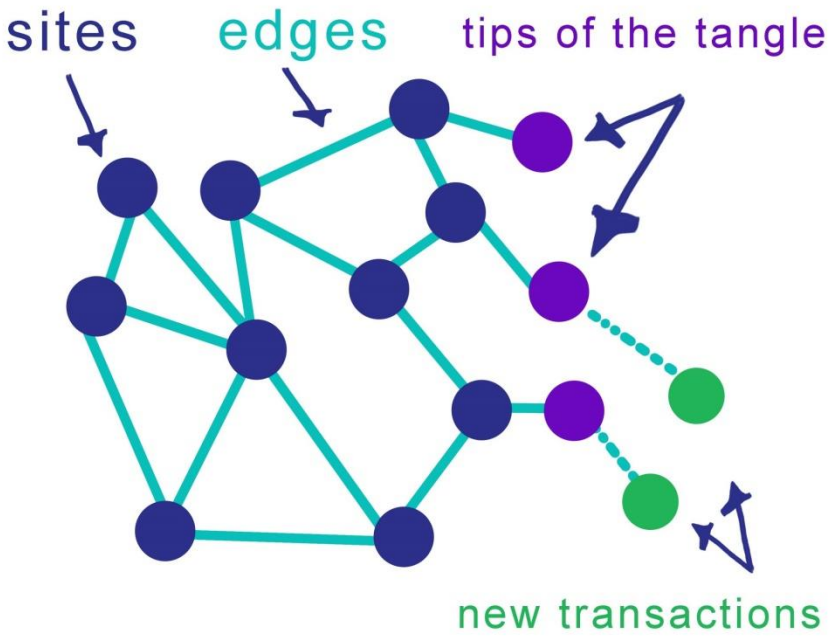






iota





Consensus Mechanisms

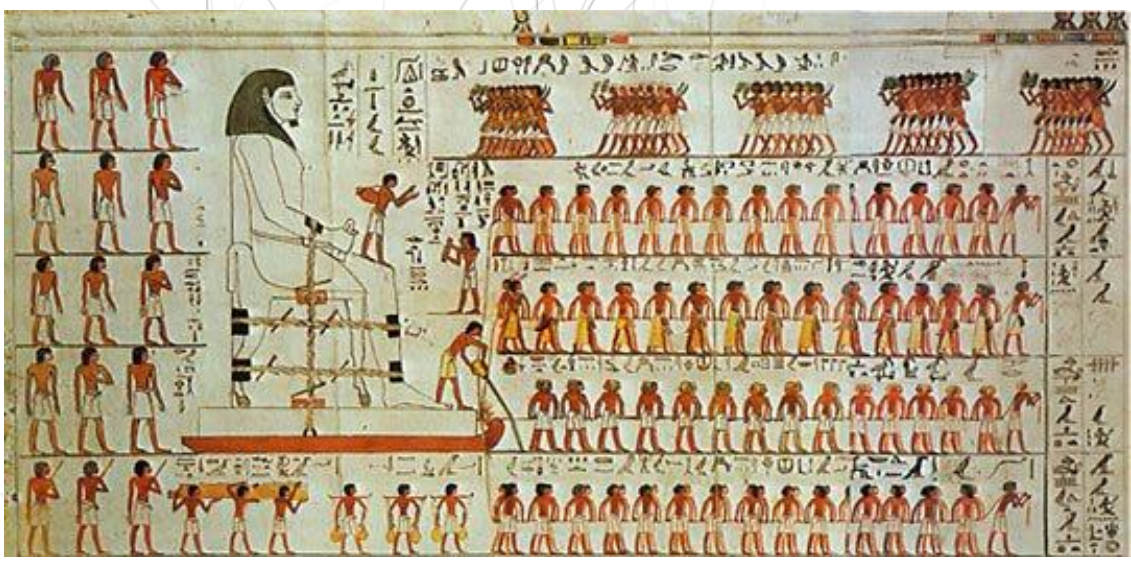
- Agreement amongst a majority of nodes (majority <percentage> is predefined by a policy), that a transaction is valid, and that there is a consistent set and a guaranteed ordering of the transactions to be stored in distributed ledger
- Permissionless blockchains: All the nodes can validate transactions in anonymous form
- Permissioned Blockchain: only predefined and authenticated nodes can validate transactions
- Cryptocurrency complaint to financial regulations, GDPR and legal obligations
- Consensus should be Agreement Seeking, Collaborative, Cooperative, Inclusive, Participatory with democratic DAO or dAPP committee

Consensus Mechanisms

- Based on Behaviours, Risk factors, and Governance model
- Proof of Work (PoW) //processing time
- Proof of Stake (PoS) //to hold stake
- Proof of Elapsed Time (PoET) //wait time
- Delegated Proof of Stake (DPoS) //approval
- 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)

Gift economy

- Happiness
- Self-realization
- Gratitude and recognition
- integrative societal model
- Economy operating on the act of offering and receiving unconditional consideration



Self sustainable

- Equitable opportunities
- Rewards properly distributed
- Accumulation of wealth with integrity
- All decisions made democratically
- Artificial Intelligence Delegated Proof of Contribution (AI-DPoC) consensus

ISO/TC 307 AWI 23258
BCT and DLT: Taxonomy and Ontology

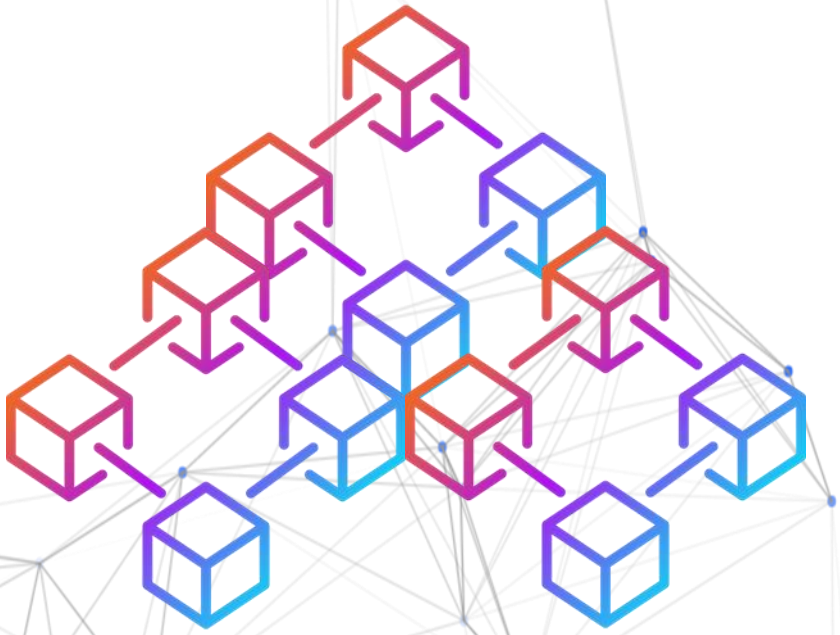
Permission

Consensus

Incentive Mechanism

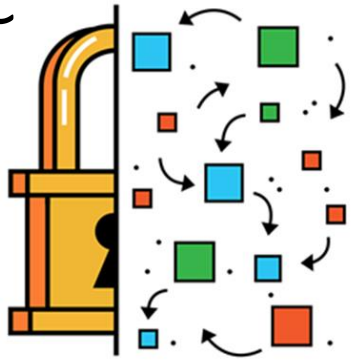
Application – universal or domain specific

Security and Risk management



Securing Blockchain

- Crypto primitives, Federated Identity, RBAC
- Taking in consideration DLT use cases, security risks and vulnerability may lead to associated financial and social risks.
- In Delight chain, several security features, such as integrity, order of event, and authenticity of data stored in a block should be provided by design
- Chain should be able to distinguish honest and dishonest miners quickly

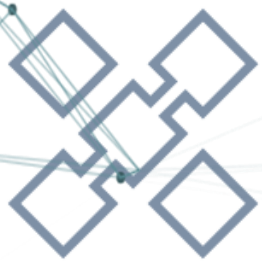


Attack landscape at different layers and Mitigation by design

- *Finney attack and Brute force attack (*pre-mined block broadcast/double spending*)*
- *Race attack (*taking advantage of delay*)*
- *One-confirmation attack (*vector 76, rejection of first transaction*)*
- *Punitive and Feather Forking (*dishonest miners*)*
- *Goldfinger attack (*51% power*)*
- *Selfish mining attack (*inappropriate incentives*)*
- *Coin hopping attack (*hash rate changing*)*
- *Nothing-at-stake attack (*no cost for block validation*)*
- *Sybil attack (*spoofed identity to achieve majority*)*
- *Existence of more than 1/3 dishonest nodes (BFT)*
- *Time jacking attack (*speed up or slow down clocks*)*
- *Consensus security* (majority)
- *Consensus spoofing (*Hard/soft fork management*)*
- *Admin app vulnerabilities (*bribery attack*), User app vulnerabilities (*key stealing/destroying*)*
- *Admin API/User API/External interface vulnerabilities*
- *Crypto services/ledger/state management vulnerabilities*
- *DDoS attack, Eclipse/Net-split attack, Key-revocation, Insecure RNG ….*

existing standard relevant to security of blockchain and DLT

- ISO/IEC 18014 (IT Security Techniques, Time Stamping)
- ISO/IEC 14888 (Digital Signature Mechanisms)
- ISO/IEC 15408 (Common Criteria Security Evaluation)
- ISO/IEC 29128 (Verification of Cryptographic Protocols)
- ISO/IEC 27000 series (Information Security Management Standards)
- ISO/IEC DIS 19086-4, Information technology - Cloud computing - Service level agreement (SLA) framework - Part 4: Security and privacy
- ISO/IEC AWI 20547-4, Information technology - Big data reference architecture - Part 4: Security and privacy fabric



EcoVerse™

SCALABLE FLEXIBLE USABLE

- **Delight chain's Eco Verse** is designed to enable vertical and horizontal scaling of decentralized applications, achieved through an operating system-like construct upon which applications can be built
- The software provides accounts, authentication, databases, asynchronous communication and the scheduling of applications across multiple CPU cores and/or clusters
- It has Cyber security and Access control, Data Quality assurance
- The resulting architecture has the potential to scale to millions of transactions per second, eliminates user fees and allows for quick and easy deployment of decentralized applications

DeLight Chain

Security countermeasures to protect information, assets and security of Eco Verse

1. Network Security - Authentication and authorization, Access control, Intrusion Detection and Prevention, Targeted attack resistance
2. Proper choice and configuration of cryptographic algorithms and protocols
3. Key management - cryptographic operations which requires the private key are conducted inside temper resistance device/environment
4. Security management process (e.g. ISMS - ISO/IEC 27000, ISO AWI 23257)
   - Risk analysis – assets, attacks, possibility of attacks, potential loss
   - Threat modelling and mitigation - potential attack surface, attack methodology and mitigations, threat modelling is needed as an input to risk analysis
   - Audit
5. Secure implementation – formal verification and certification
6. Ensuring availability of each node (with Chain of Trust)

DeLight Chain

Sustainability – Eco Verse / Delight Chain

- Utility ecosystem (to support business environments, fast track on-boarding 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 compliant, Privacy v/s KYC and AML compliance
- Forward Value and easy Exchange
- QoS benchmarks

DeLight Chain

- Unified and Compliant crypto curreny to spend across multiple service providers without any national boundaries
- **Scalable, Flexible, Secure blockchain ecosystem**
- **Two coin system** (Stable ECX (centralized) and Value driven ECR and ECR'(decentralized))
- **Easy storage and exchange in Secure Wallet**
- **Easy Upgrades and Bug Recovery, Low latency**
- **Support Millions of Users, Free Usage**
- **Building the coin world for everyone**

DeLight Chain

Thank you for your time and attention

Dr. Dhiren Patel

DeLight Chain