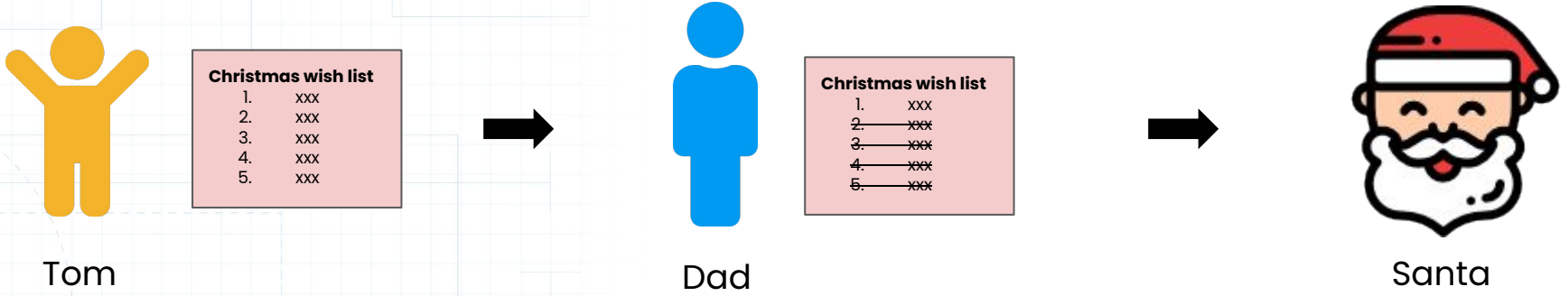
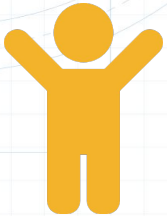
Algorand Blockchain

What is Blockchain?



What is a Blockchain?



Tom

Christmas wish list
1. xxx
2. xxx
3. xxx
4. xxx
5. xxx

Christmas wish list
1. xxx
2. xxx
3. xxx
4. xxx
5. xxx

Christmas wish list
1. xxx
2. xxx
3. xxx
4. xxx
5. xxx

Christmas wish list
1. xxx
2. xxx
3. xxx
4. xxx
5. xxx

Christmas wish list
1. xxx
2. xxx
3. xxx
4. xxx
5. xxx

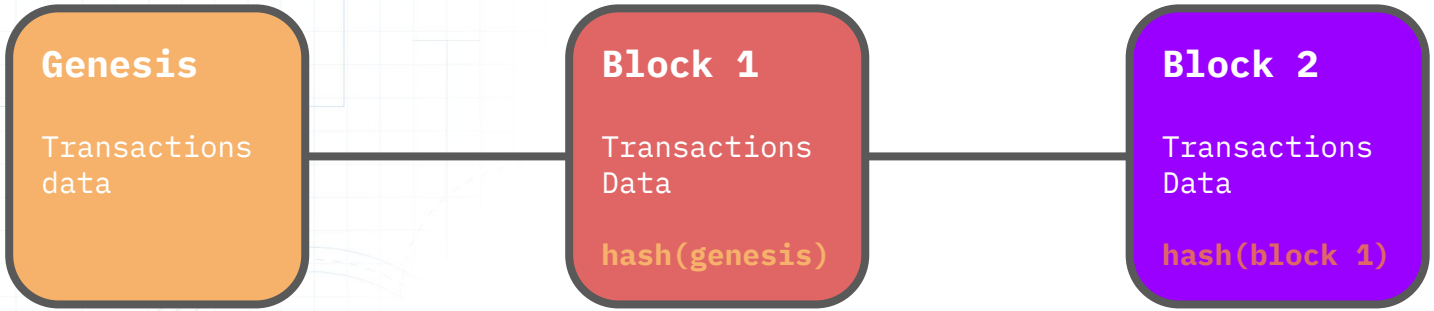
Elves

Dad

Santa

What is a Blockchain?

- A public ledger of transactional data, distributed across a system of multiple nodes in a network.
- Nodes work together using the consensus protocol to add transactions to the ledger.
- The ledger is publicly verifiable, permissionless, and tamper-proof.



Real World Usage

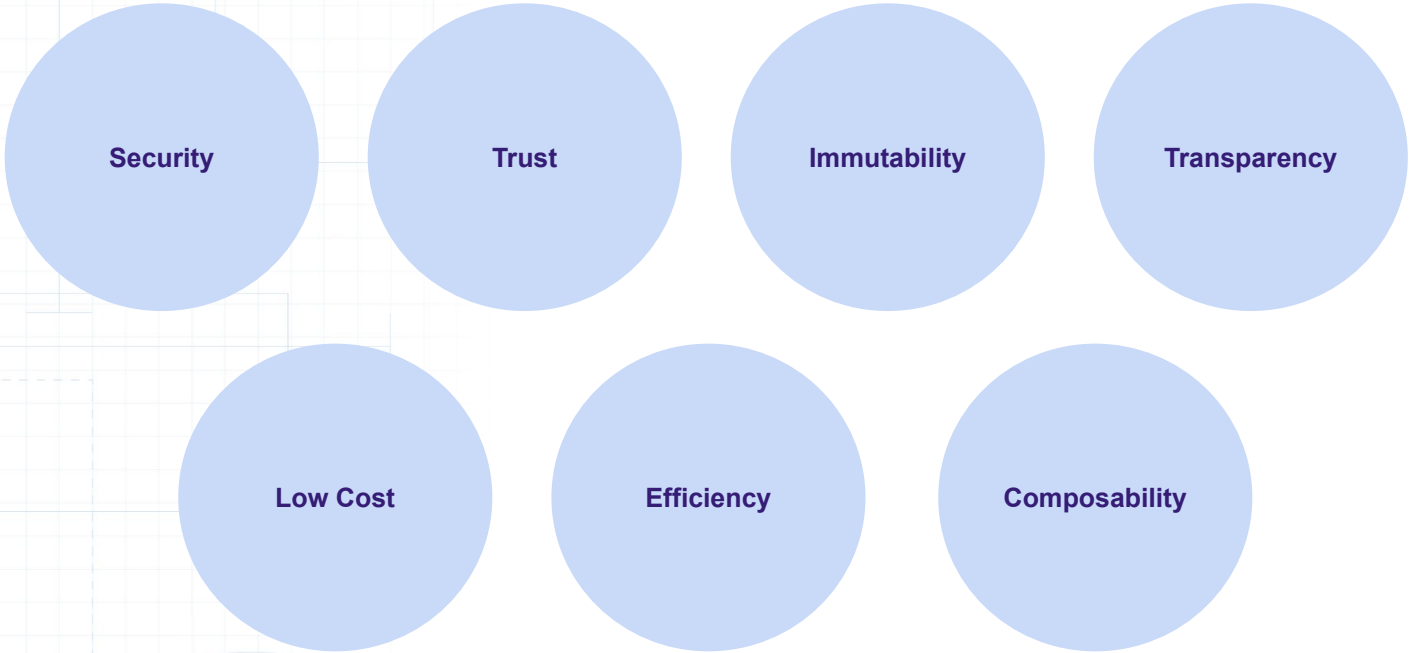
DE BEERS GROUP

- Tracks each step of the diamond's journey - from mining, processing, retailer, and end user.

SINGAPORE AIRLINES

- Manage its loyalty point system - KrisFlyer miles on their digital wallet.

Benefits of Blockchain



Blockchain Projects

- Ethereum
- Terra (LUNA)
- BSC (BNB)
- Avalanche (AVAX)
- Solana (SOL)
- Fantom (FTM)
- Polygon (MATIC)
- Tron (TRON)
- Cronos (CRO)
- Waves (WAVES)

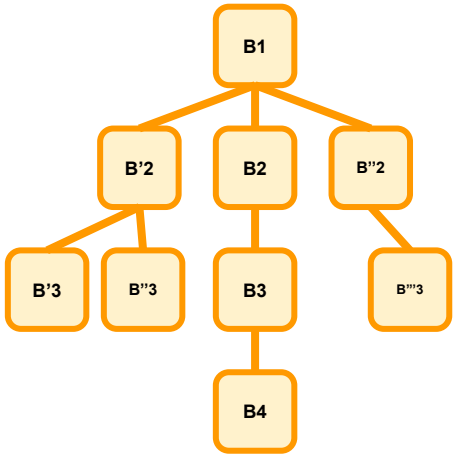
Source: Defi Llama

Consensus Protocols

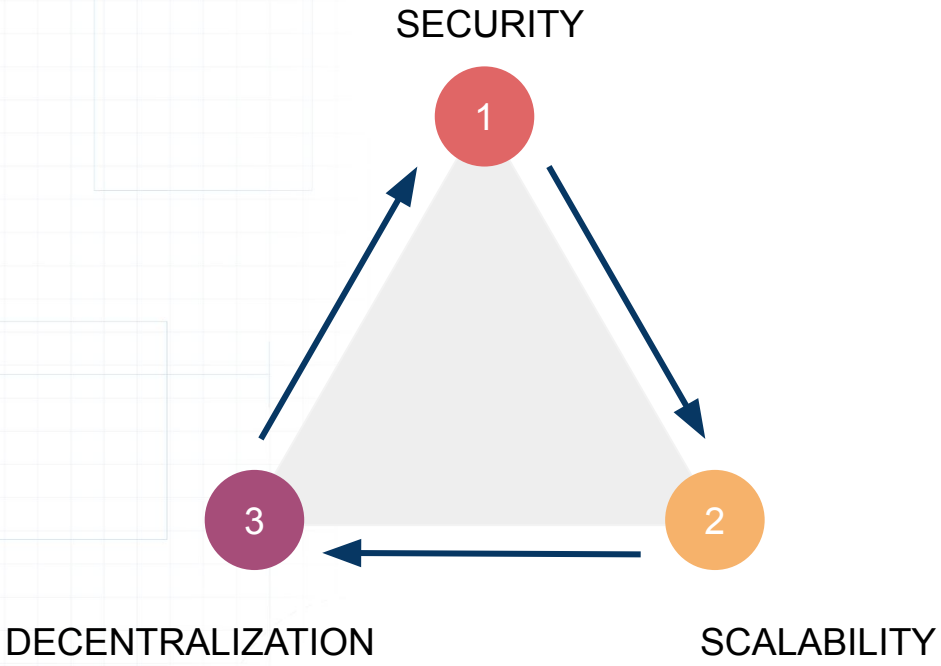
Name	Mechanics	Critical Issues
Proof of Work (PoW) E.g. Bitcoin, Ethereum	• Miners (nodes) **compete with each other** to append the next block. • Rewards are given for the node that manages to **produce the cryptographic hash**.	• Huge electrical consumption • Takes a long time to produce a block
Proof of Stake (PoS) E.g. Cardano, Avalanche, Solana	• Accounts will **stake their coins** to verify transactions and produce blocks. • Validator nodes are chosen to review blocks. • Voting power is **proportional** to their staked coins.	• Benefits wealthy participants • Minimum staking period • Known validator nodes are prone to DDoS attacks.

Forking and Finality

- Fork happens when two or more miners find a block at nearly the same time.
- The fork is resolved when network accepts the longest chain.
- Finality is the guarantee that cryptocurrency transactions cannot be altered once it is completed.
- Measures the amount of time one has to wait for a reasonable guarantee that crypto transactions are completed.



Blockchain Trilemma



Blockchain Trilemma

Name	Issues to solve	Is affected by
Security	• Prevent adversaries from validating fraudulent transactions. • Tackle 51% attacks - *gain control of hashing power to invalidate transactions*.	• Requires additional nodes to reduce coordinated attacks.
Scalability	• Support high transactional throughput	• Centralized servers are more powerful
Decentralization	• No one entity can control or censor the data that is being transacted.	• Transaction speeds drop (PoW)

Ethereum Blockchain Project

- Current uses Proof of Work consensus. They are upgrading it to use Proof of Stake soon.
- Scalability Issue - high gas fees, network congestion, power consumption

Quiz #1

Which option is not a feature of a blockchain?

1. Blocks in a blockchain contain a list of transactions.
2. A block contains a cryptographic hash of the previous block.
3. **An administrator can reverse a transaction on the blockchain.**
4. Blocks are added to the blockchain via consensus protocol.

Quiz #2

Which of these statements is false about the benefits of blockchain?

1. Transactions in a block cannot be tampered with.
2. Decentralized applications can leverage on each other on the blockchain.
3. Transactions on the blockchain can be publicly viewed.
4. **Submitting a transaction to a blockchain is free.**