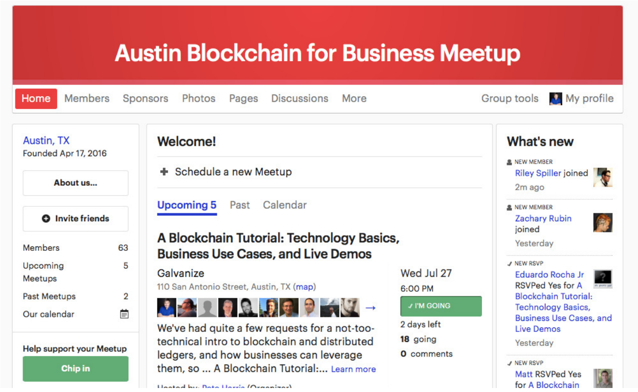


Austin Blockchain for Business Meetup

Austin, TX
Founded Apr 17, 2016

About us...

Invite friends

Members	63
Upcoming Meetups	5
Past Meetups	2
Our calendar	

Help support your Meetup

Chip in

Welcome!

+ Schedule a new Meetup

Upcoming 5 Past Calendar

A Blockchain Tutorial: Technology Basics, Business Use Cases, and Live Demos

Galvanize
110 San Antonio Street, Austin, TX (map)

Wed Jul 27
6:00 PM
✓ I'M GOING
2 days left
18 going
0 comments

We've had quite a few requests for a not-too-technical intro to blockchain and distributed ledgers, and how businesses can leverage them, so ... A Blockchain Tutorial:... Learn more

Hosted by: Pete Harris (Organizer)

What's new

NEW MEMBER
Riley Spiller joined
2m ago

NEW MEMBER
Zachary Rubin joined
Yesterday

NEW RSVP
Eduardo Rocha Jr RSVPed Yes for A Blockchain Tutorial: Technology Basics, Business Use Cases, and Live Demos
Yesterday

NEW RSVP
Matt RSVPed Yes for A Blockchain

https://www.meetup.com/Austin-Blockchain-for-Business-Meetup/

www.persistent.com

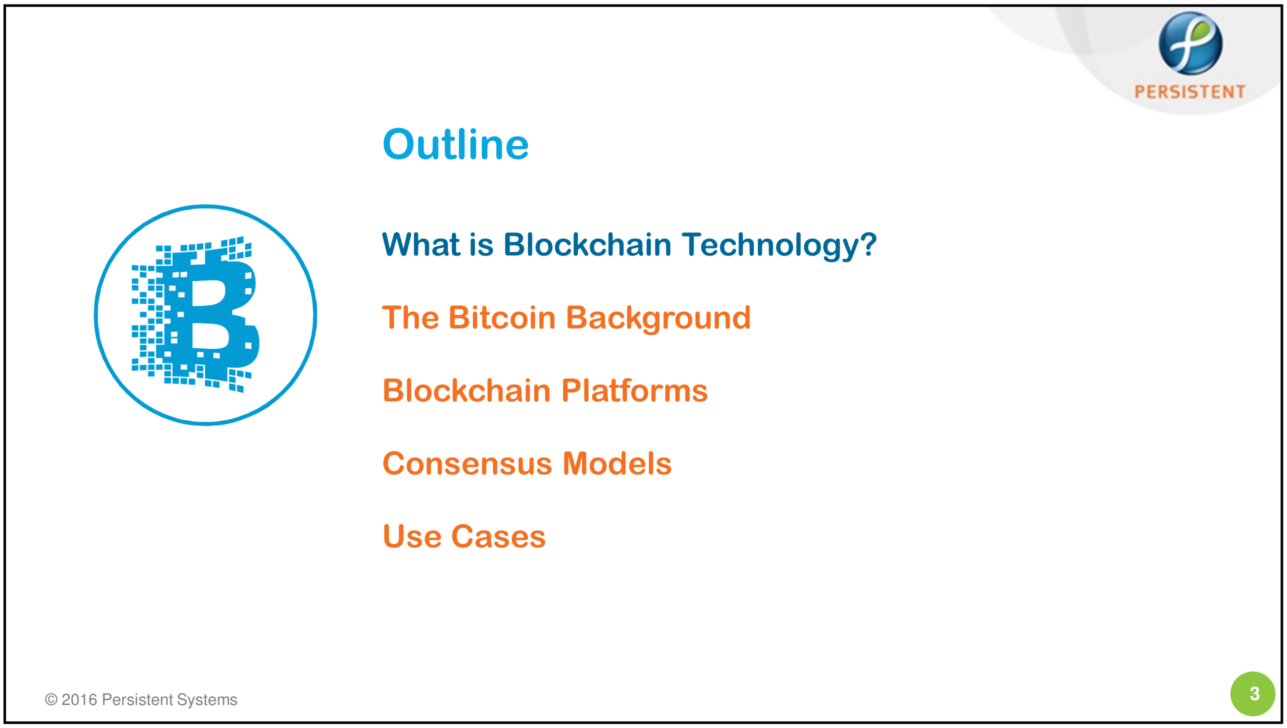
PERSISTENT
Partners in Innovation

Blockchain Technology

Siddhartha Chatterjee

sid_chatterjee@persistent.com

July 2016



Outline

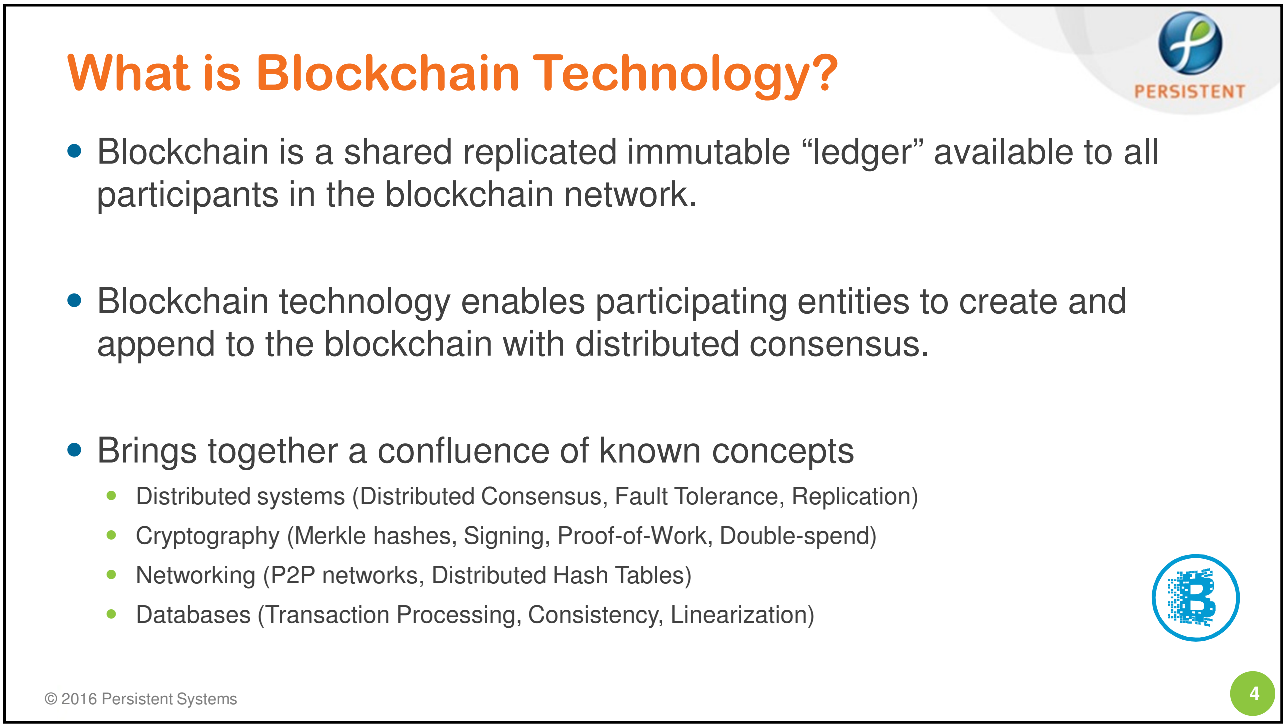
What is Blockchain Technology?

The Bitcoin Background

Blockchain Platforms

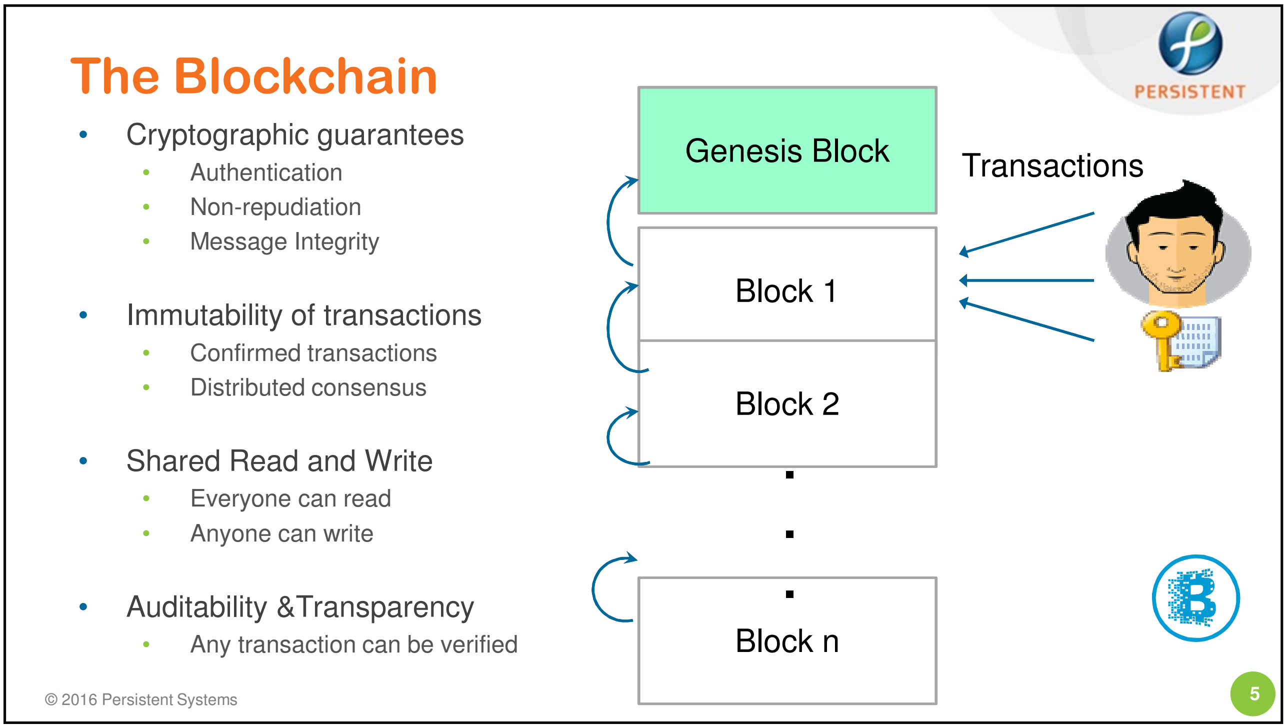
Consensus Models

Use Cases



What is Blockchain Technology?

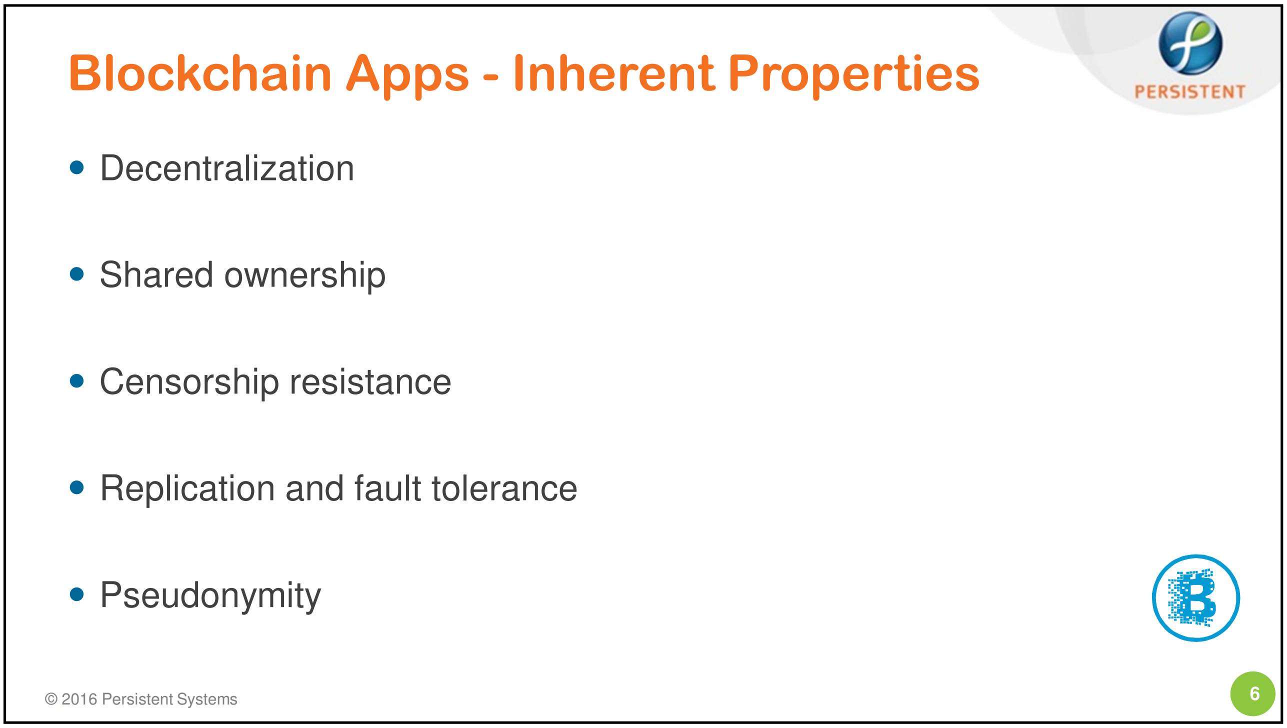
- Blockchain is a shared replicated immutable “ledger” available to all participants in the blockchain network.
- Blockchain technology enables participating entities to create and append to the blockchain with distributed consensus.
- Brings together a confluence of known concepts
  - Distributed systems (Distributed Consensus, Fault Tolerance, Replication)
  - Cryptography (Merkle hashes, Signing, Proof-of-Work, Double-spend)
  - Networking (P2P networks, Distributed Hash Tables)
  - Databases (Transaction Processing, Consistency, Linearization)



The Blockchain

- Cryptographic guarantees
  - Authentication
  - Non-repudiation
  - Message Integrity
- Immutability of transactions
  - Confirmed transactions
  - Distributed consensus
- Shared Read and Write
  - Everyone can read
  - Anyone can write
- Auditability &Transparency
  - Any transaction can be verified

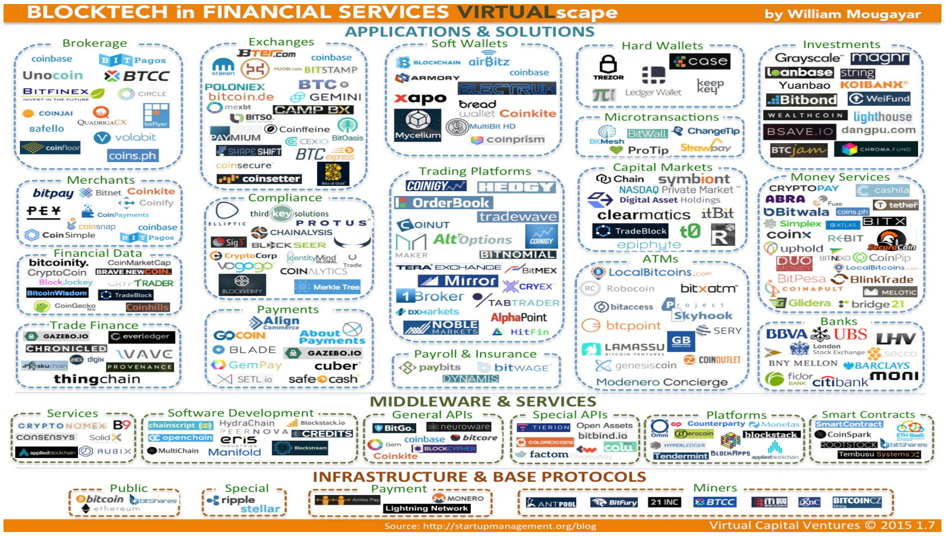
Genesis Block
Block 1
Block 2
Block n
Transactions



Blockchain Apps - Inherent Properties

- Decentralization
- Shared ownership
- Censorship resistance
- Replication and fault tolerance
- Pseudonymity

Blockchain FinTech Landscape



https://www.persistent.com/wp-content/uploads/2016/03/The-Blockchain-Landscape-.pdf

Source: Startup Management

Outline

What is Blockchain Technology?

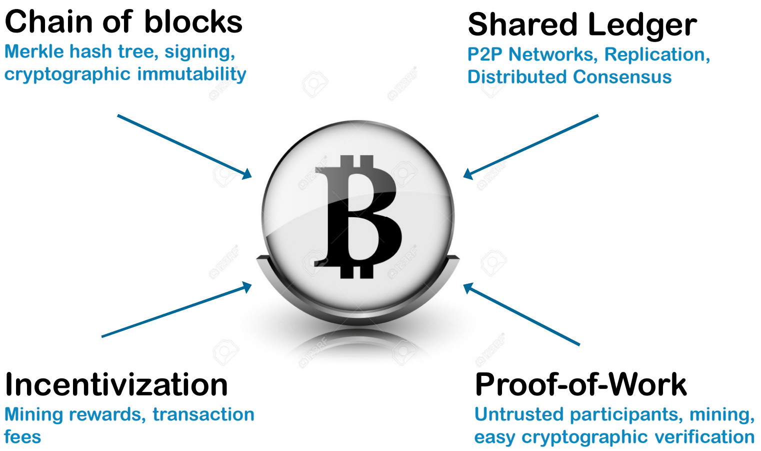
The Bitcoin Background

Blockchain Platforms

Consensus Models

Use Cases

Bitcoin - Blockchain based Cryptocurrency



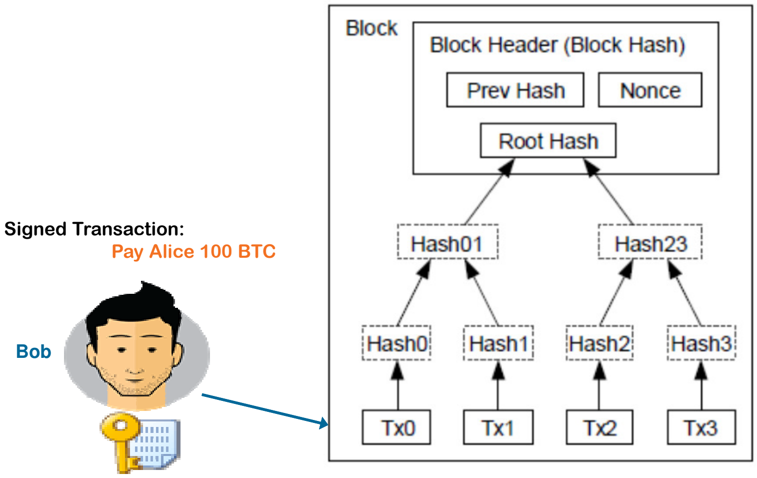
Chain of blocks
Merkle hash tree, signing, cryptographic immutability

Shared Ledger
P2P Networks, Replication, Distributed Consensus

Incentivization
Mining rewards, transaction fees

Proof-of-Work
Untrusted participants, mining, easy cryptographic verification

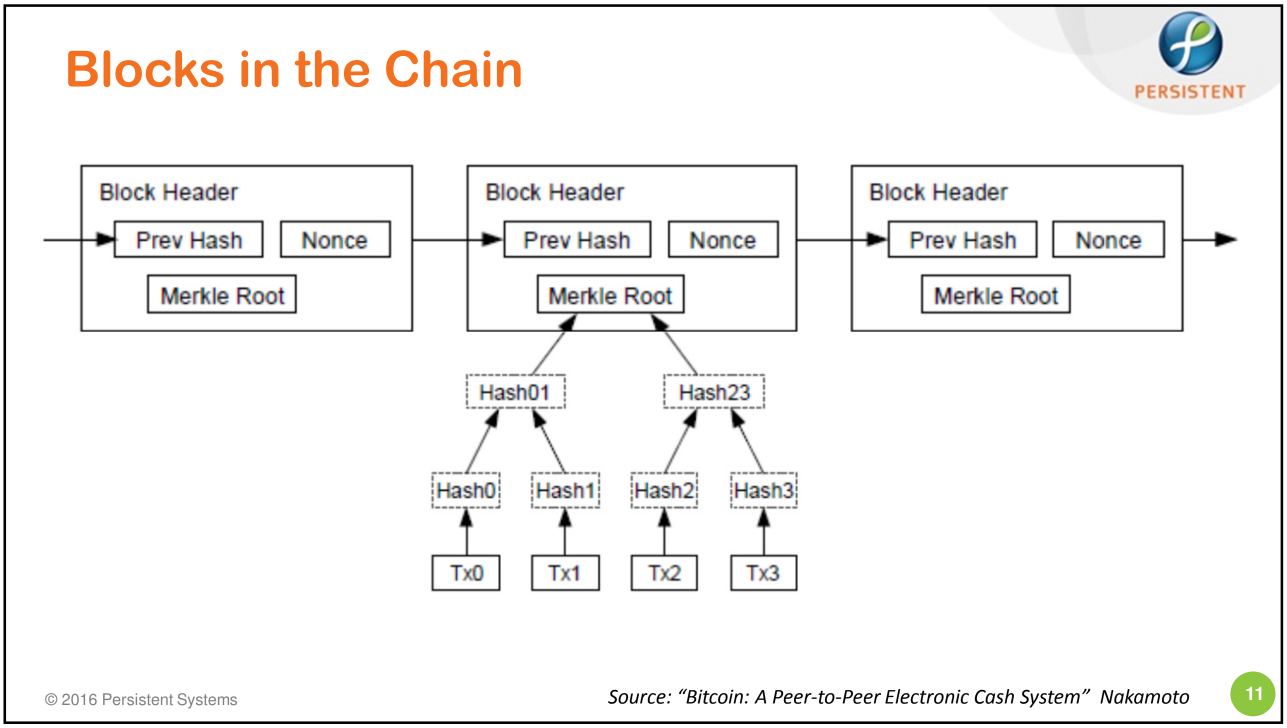
Transactions and blocks – Merkle hash trees



Transactions Hashed in a Merkle Tree

- Transaction verification
  - Sender account has enough balance
  - Well-formed transaction
- Include all valid transactions in a block
  - Compute root hash and block header
- Generate proof-of-work
- Transaction confirmation
  - Multiple confirmations after the current block is added to the blockchain.

Source: "Bitcoin: A Peer-to-Peer Electronic Cash System" Nakamoto



Blocks in the Chain

PERSISTENT

Block Header
Prev Hash
Nonce
Merkle Root

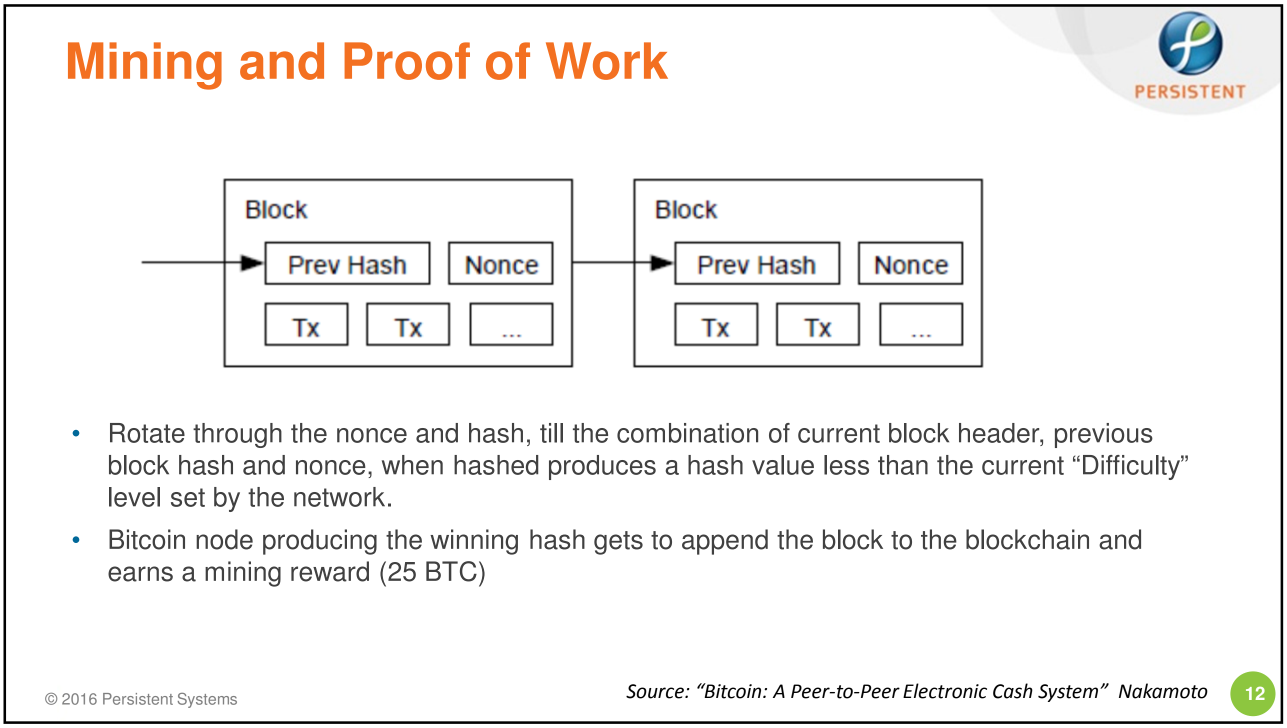
Block Header
Prev Hash
Nonce
Merkle Root

Block Header
Prev Hash
Nonce
Merkle Root

Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Source: "Bitcoin: A Peer-to-Peer Electronic Cash System" Nakamoto

11



Mining and Proof of Work

PERSISTENT

Block
Prev Hash
Nonce
Tx
Tx
...

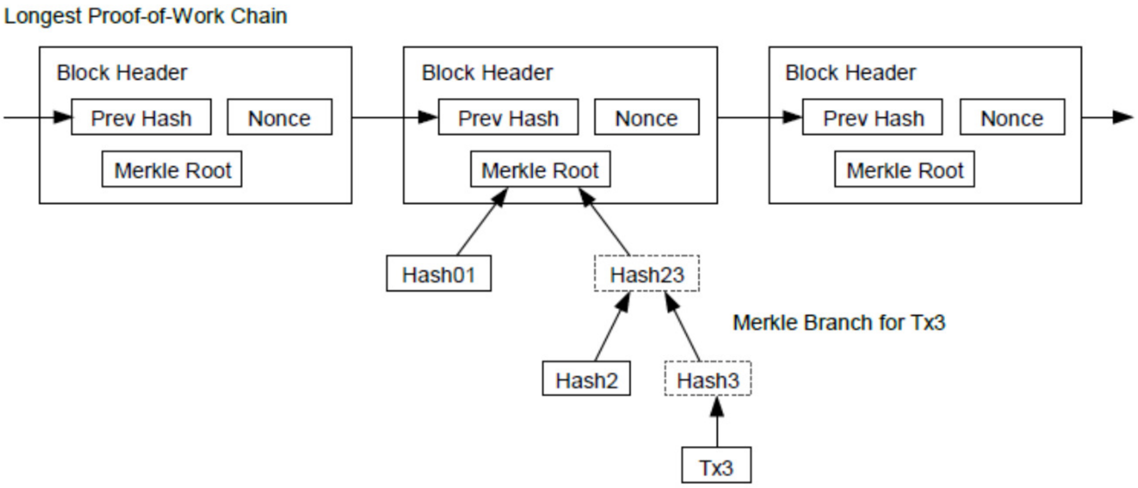
Block
Prev Hash
Nonce
Tx
Tx
...

- Rotate through the nonce and hash, till the combination of current block header, previous block hash and nonce, when hashed produces a hash value less than the current "Difficulty" level set by the network.
- Bitcoin node producing the winning hash gets to append the block to the blockchain and earns a mining reward (25 BTC)

Source: "Bitcoin: A Peer-to-Peer Electronic Cash System" Nakamoto

12

Transaction Verification



Source: "Bitcoin: A Peer-to-Peer Electronic Cash System" Nakamoto

Outline

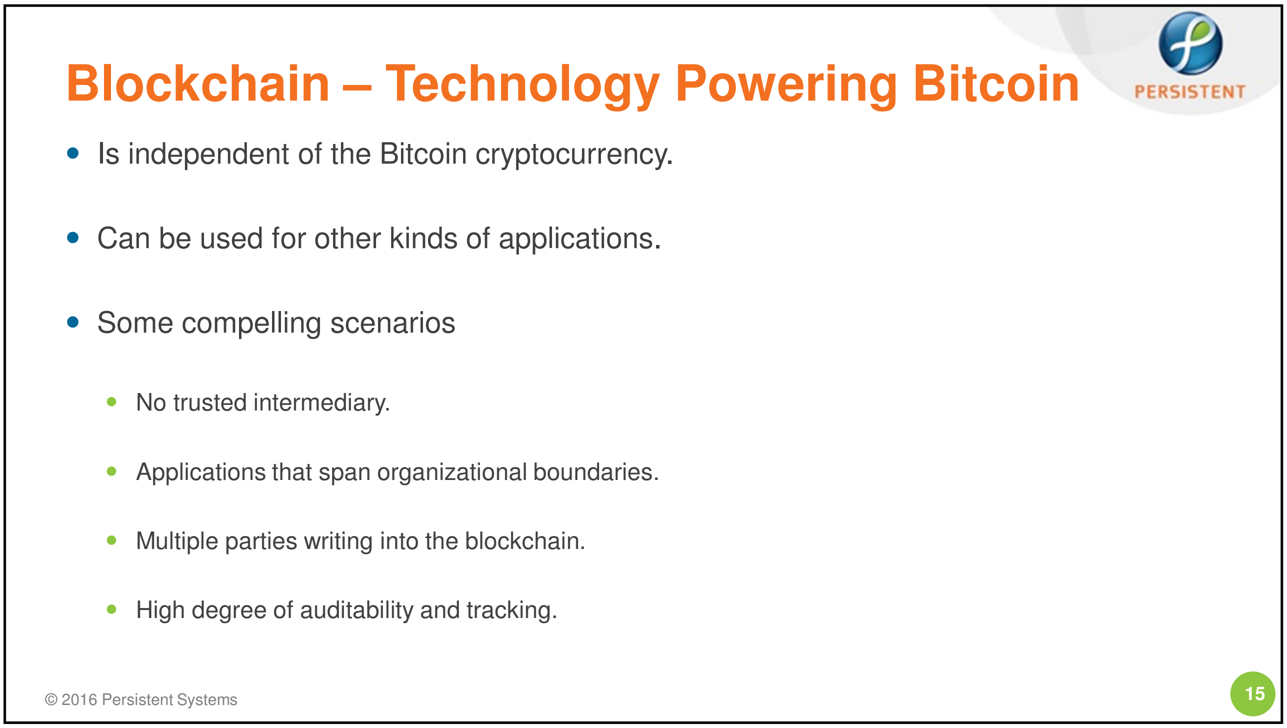
What is Blockchain Technology?

The Bitcoin Background

Blockchain Platforms

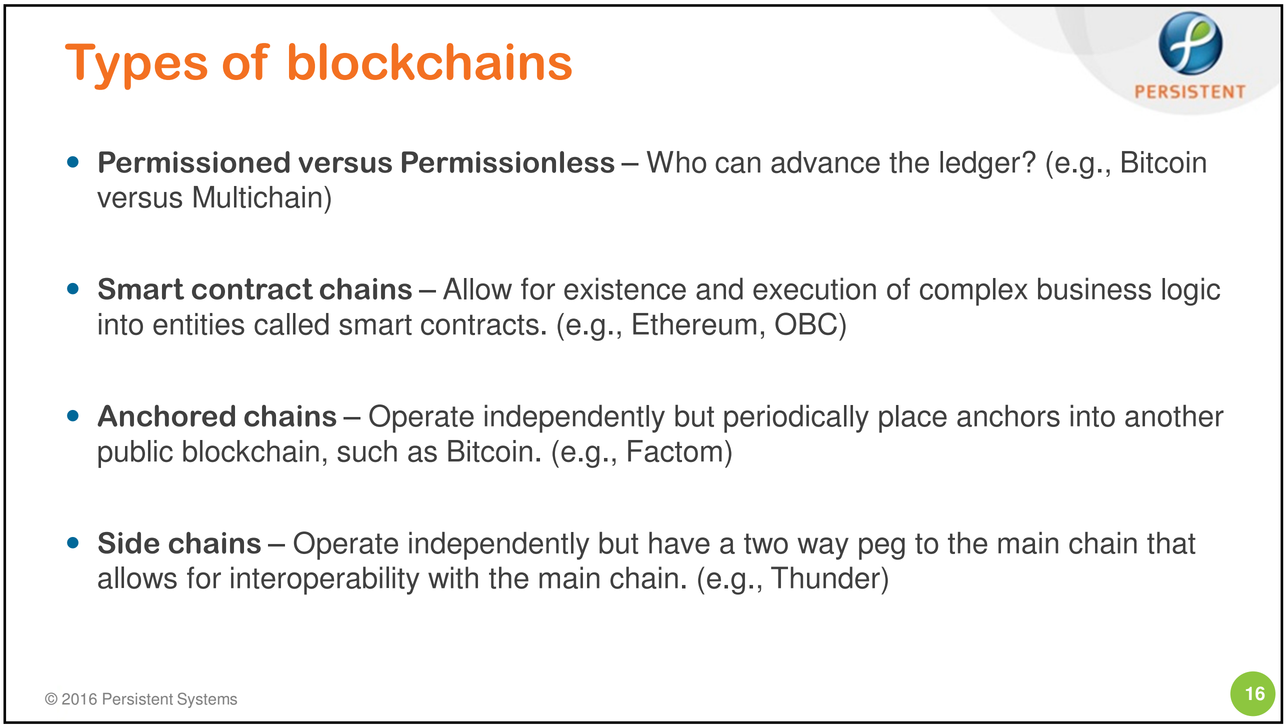
Consensus Models

Use Cases



Blockchain – Technology Powering Bitcoin

- Is independent of the Bitcoin cryptocurrency.
- Can be used for other kinds of applications.
- Some compelling scenarios
  - No trusted intermediary.
  - Applications that span organizational boundaries.
  - Multiple parties writing into the blockchain.
  - High degree of auditability and tracking.



Types of blockchains

- **Permissioned versus Permissionless** – Who can advance the ledger? (e.g., Bitcoin versus Multichain)
- **Smart contract chains** – Allow for existence and execution of complex business logic into entities called smart contracts. (e.g., Ethereum, OBC)
- **Anchored chains** – Operate independently but periodically place anchors into another public blockchain, such as Bitcoin. (e.g., Factom)
- **Side chains** – Operate independently but have a two way peg to the main chain that allows for interoperability with the main chain. (e.g., Thunder)

Blockchain Platforms

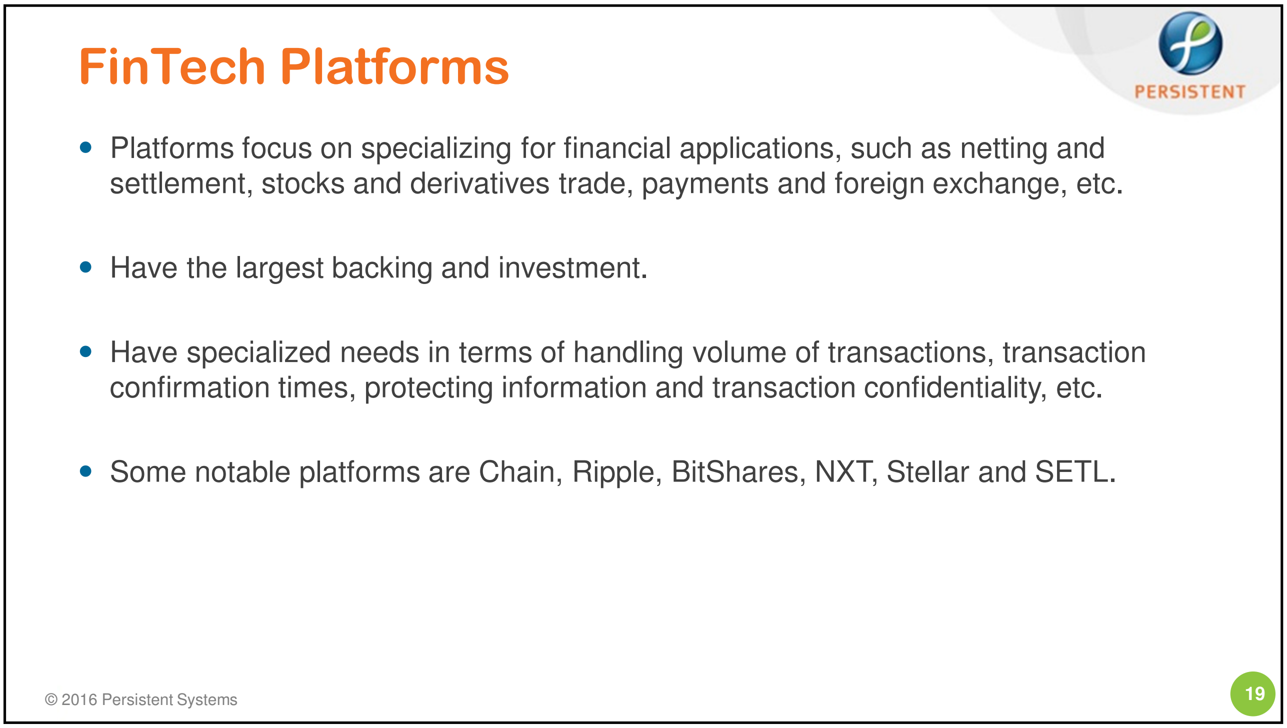
- Bitcoin based platforms
- FinTech platforms
- Smart Contract Platforms
- Consortium Platforms
- Sidechain/Anchored Platforms

17

Bitcoin based Platforms

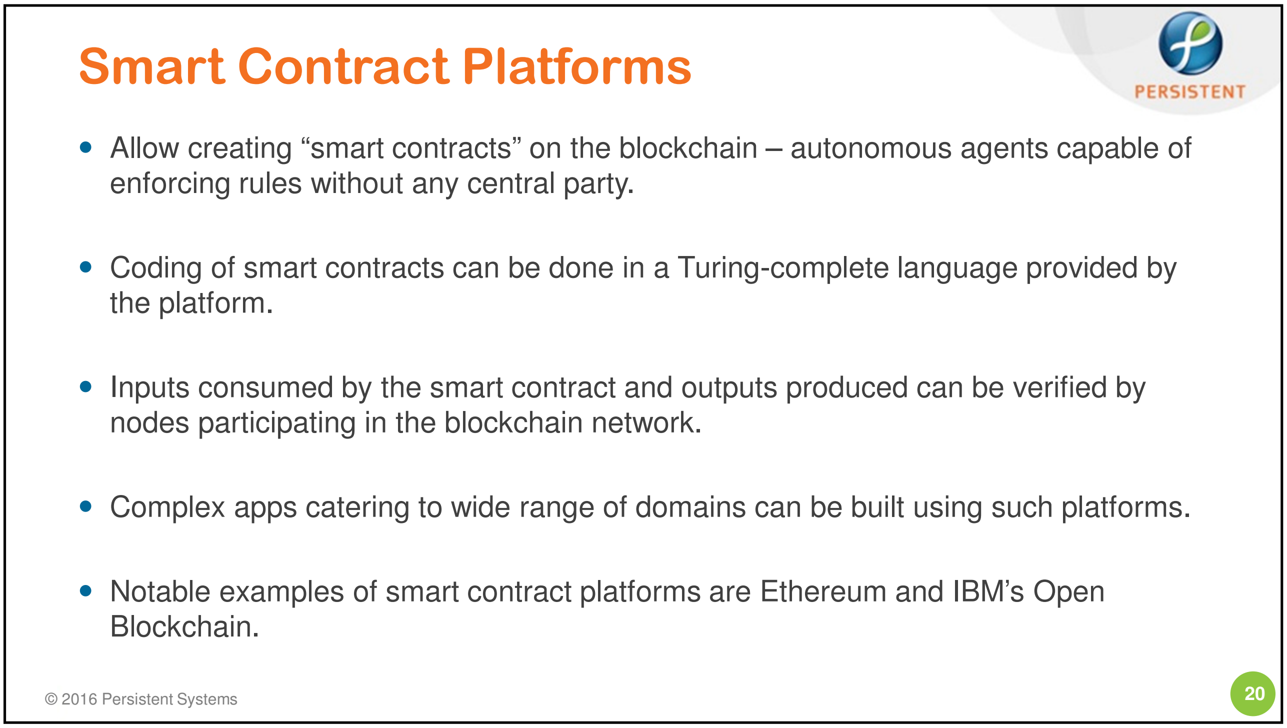
- Add application based meta-data into Bitcoin transactions.
- Transactions are submitted like regular Bitcoin transactions and are mined by Bitcoin nodes.
- Most platforms used Bitcoins as the native token albeit some exceptions.
- Platforms allow for custom asset management, such as smart property, reward points, coupons, financial instruments, currencies, etc.
- Some notable platforms are ColoredCoins, Coinprism, CoinSpark, ChromaWay and Omni.

18



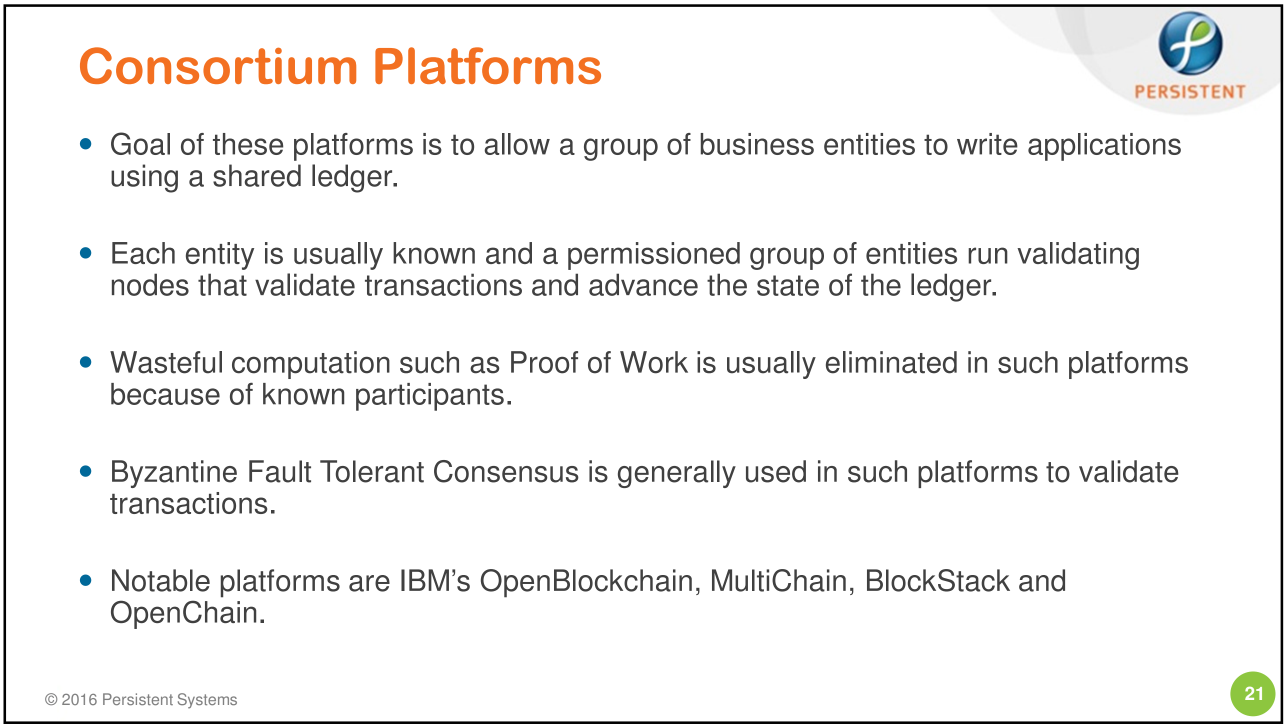
FinTech Platforms

- Platforms focus on specializing for financial applications, such as netting and settlement, stocks and derivatives trade, payments and foreign exchange, etc.
- Have the largest backing and investment.
- Have specialized needs in terms of handling volume of transactions, transaction confirmation times, protecting information and transaction confidentiality, etc.
- Some notable platforms are Chain, Ripple, BitShares, NXT, Stellar and SETL.



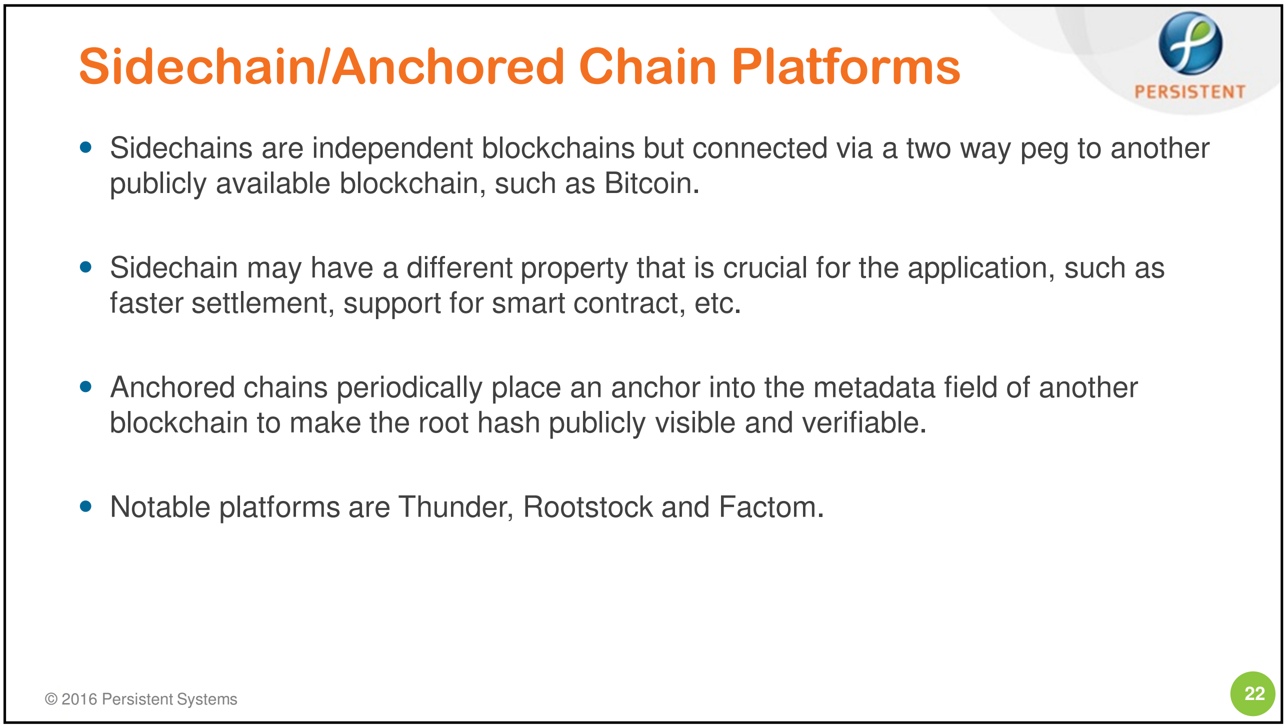
Smart Contract Platforms

- Allow creating “smart contracts” on the blockchain – autonomous agents capable of enforcing rules without any central party.
- Coding of smart contracts can be done in a Turing-complete language provided by the platform.
- Inputs consumed by the smart contract and outputs produced can be verified by nodes participating in the blockchain network.
- Complex apps catering to wide range of domains can be built using such platforms.
- Notable examples of smart contract platforms are Ethereum and IBM’s Open Blockchain.



Consortium Platforms

- Goal of these platforms is to allow a group of business entities to write applications using a shared ledger.
- Each entity is usually known and a permissioned group of entities run validating nodes that validate transactions and advance the state of the ledger.
- Wasteful computation such as Proof of Work is usually eliminated in such platforms because of known participants.
- Byzantine Fault Tolerant Consensus is generally used in such platforms to validate transactions.
- Notable platforms are IBM’s OpenBlockchain, MultiChain, BlockStack and OpenChain.



Sidechain/Anchored Chain Platforms

- Sidechains are independent blockchains but connected via a two way peg to another publicly available blockchain, such as Bitcoin.
- Sidechain may have a different property that is crucial for the application, such as faster settlement, support for smart contract, etc.
- Anchored chains periodically place an anchor into the metadata field of another blockchain to make the root hash publicly visible and verifiable.
- Notable platforms are Thunder, Rootstock and Factom.

Outline

What is Blockchain Technology ?

The Bitcoin Background

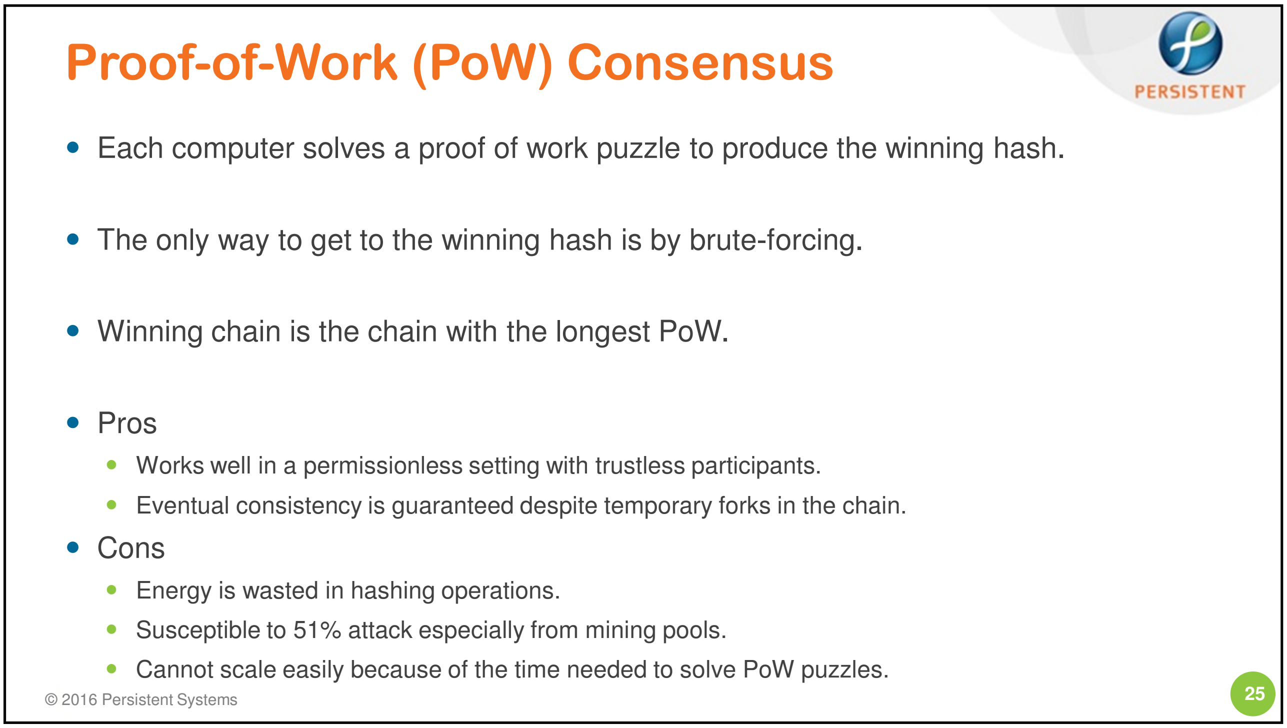
Blockchain Platforms

Consensus Models

Use Cases

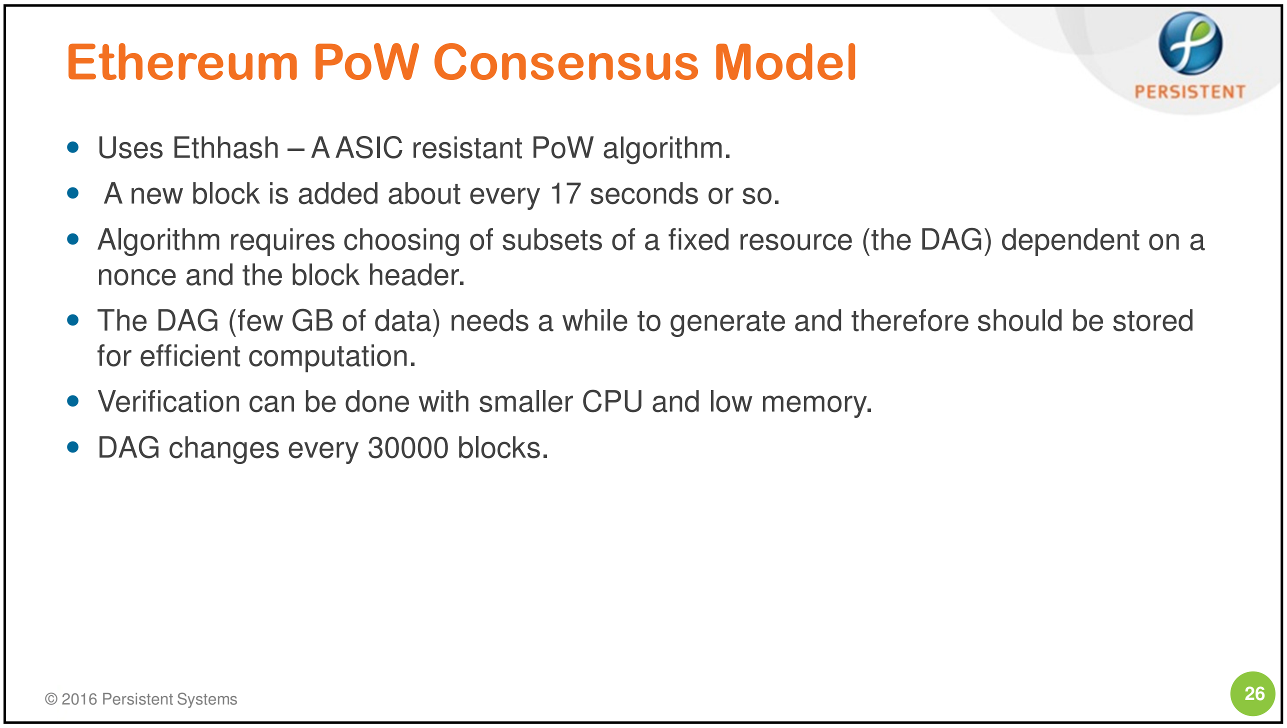
Consensus Models

- Permissionless blockchains
  - Proof-of-Work (e.g., Bitcoin, Ethereum)
  - Proof-of-Stake (e.g., BitShares, NXT)
  - Quorum based Byzantine Fault Tolerance (e.g., Ripple, Stellar)
- Permissioned blockchains
  - Practical Byzantine Fault Tolerance (e.g., OBC)
  - Proof of Elapsed Time (e.g., IntelLedger)



Proof-of-Work (PoW) Consensus

- Each computer solves a proof of work puzzle to produce the winning hash.
- The only way to get to the winning hash is by brute-forcing.
- Winning chain is the chain with the longest PoW.
- Pros
  - Works well in a permissionless setting with trustless participants.
  - Eventual consistency is guaranteed despite temporary forks in the chain.
- Cons
  - Energy is wasted in hashing operations.
  - Susceptible to 51% attack especially from mining pools.
  - Cannot scale easily because of the time needed to solve PoW puzzles.



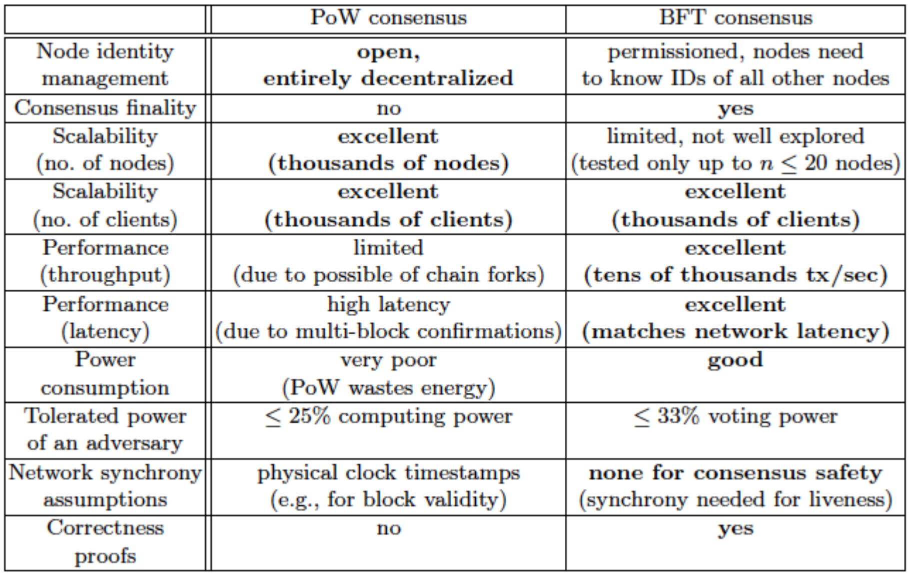
Ethereum PoW Consensus Model

- Uses Ethhash – A ASIC resistant PoW algorithm.
- A new block is added about every 17 seconds or so.
- Algorithm requires choosing of subsets of a fixed resource (the DAG) dependent on a nonce and the block header.
- The DAG (few GB of data) needs a while to generate and therefore should be stored for efficient computation.
- Verification can be done with smaller CPU and low memory.
- DAG changes every 30000 blocks.

Byzantine Fault Tolerant Consensus

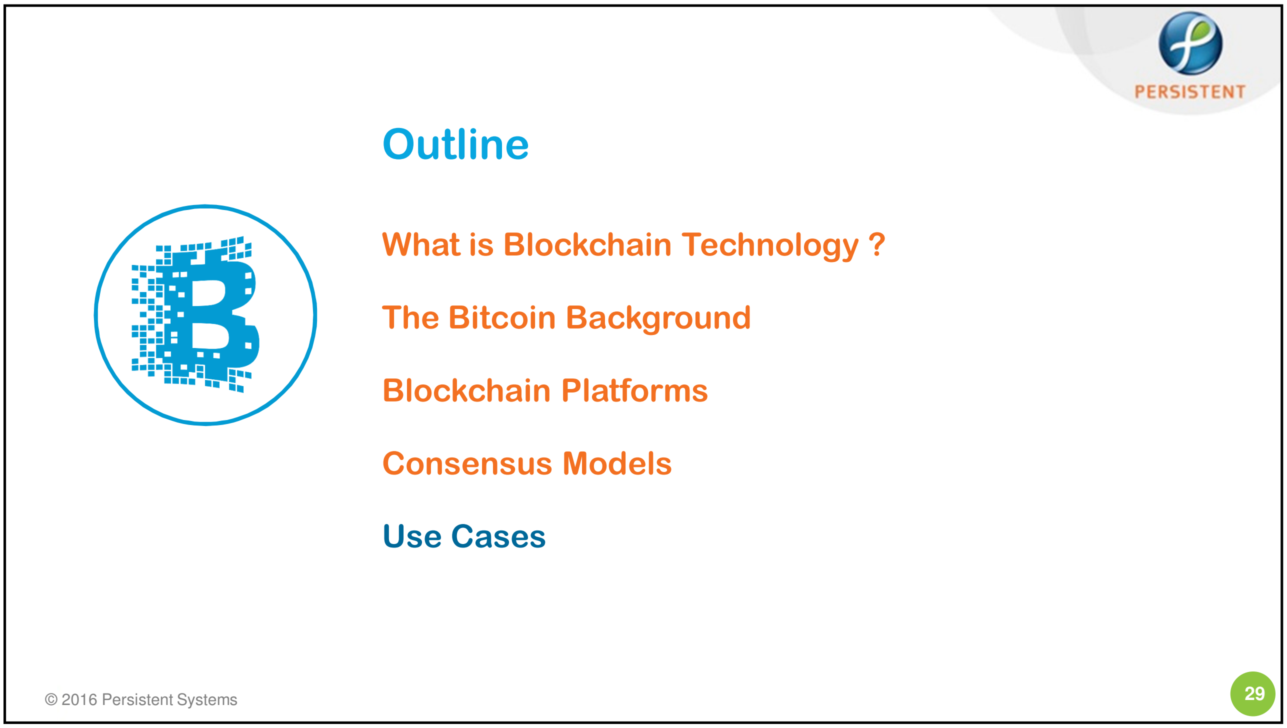
- Can achieve consensus when a fraction of the network is acting Byzantine.
- Used by permissioned blockchain systems where number of replicas are limited.
- Different variations exist (BFT, PBFT, Sieve, etc).
- Pros
  - Tolerates Byzantine faults and still able to achieve consensus.
  - Scalable compared to PoW with small number of replicas.
- Cons
  - Scalability is questionable when a large number of replicas are present. (Studies exist for around 20)
  - Need to know the number of nodes in advance.

PoW versus BFT Consensus



	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all other nodes
Consensus finality	no	**yes**
Scalability (no. of nodes)	**excellent (thousands of nodes)**	limited, not well explored (tested only up to $n \leq 20$ nodes)
Scalability (no. of clients)	**excellent (thousands of clients)**	**excellent (thousands of clients)**
Performance (throughput)	limited (due to possible of chain forks)	**excellent (tens of thousands tx/sec)**
Performance (latency)	high latency (due to multi-block confirmations)	**excellent (matches network latency)**
Power consumption	very poor (PoW wastes energy)	**good**
Tolerated power of an adversary	$\leq 25\%$ computing power	$\leq 33\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	**none for consensus safety** (synchrony needed for liveness)
Correctness proofs	no	**yes**

Source: NetSec 2015 Paper



Outline

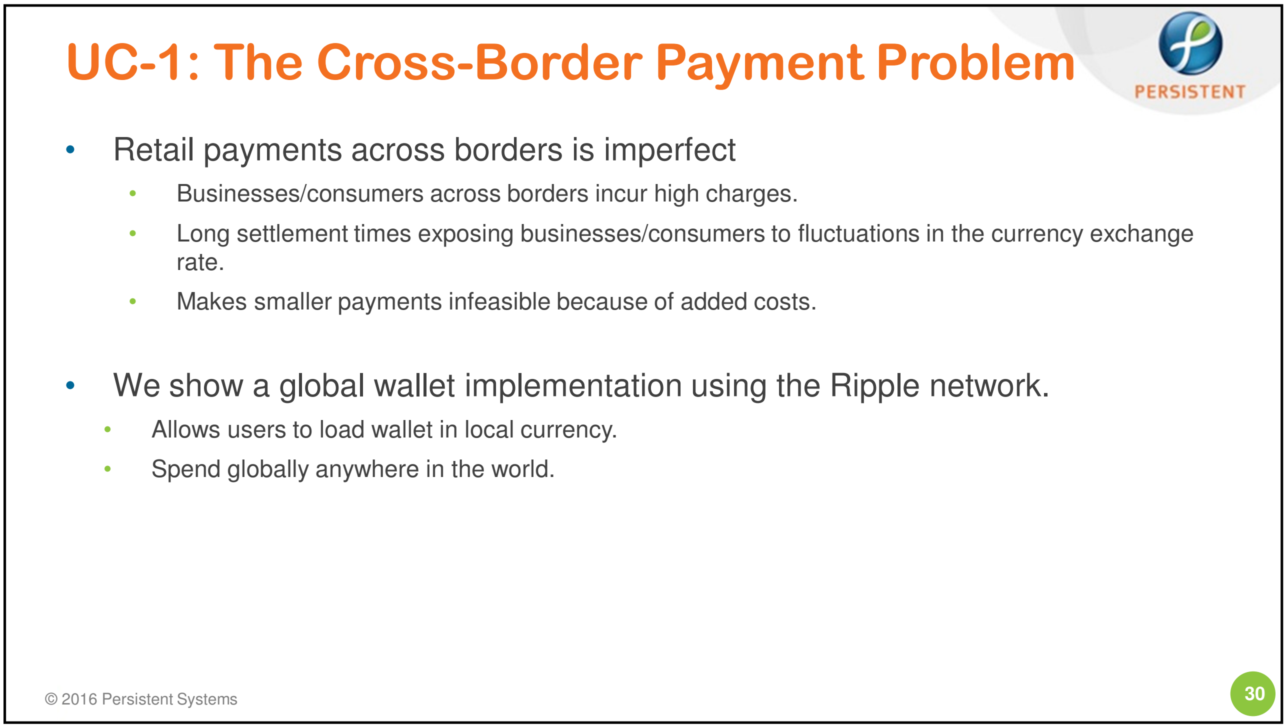
What is Blockchain Technology ?

The Bitcoin Background

Blockchain Platforms

Consensus Models

Use Cases



UC-1: The Cross-Border Payment Problem

- Retail payments across borders is imperfect
  - Businesses/consumers across borders incur high charges.
  - Long settlement times exposing businesses/consumers to fluctuations in the currency exchange rate.
  - Makes smaller payments infeasible because of added costs.

- We show a global wallet implementation using the Ripple network.
  - Allows users to load wallet in local currency.
  - Spend globally anywhere in the world.

UC-1: Cross-Border Payments using Ripple

- Ripple is a Blockchain-based payment protocol.
  - Provides cross-border multi-currency settlement rail.
  - Real time (~6 secs) settlement.
- All transactions are recorded in the public Ripple Consensus Ledger (RCL).
- When new transactions are to be added to the ledger, the Ripple network executes a distributed consensus protocol to reach agreement.

Demo

UC-1: Entities and Paths

Pathfinding: EUR to KRW

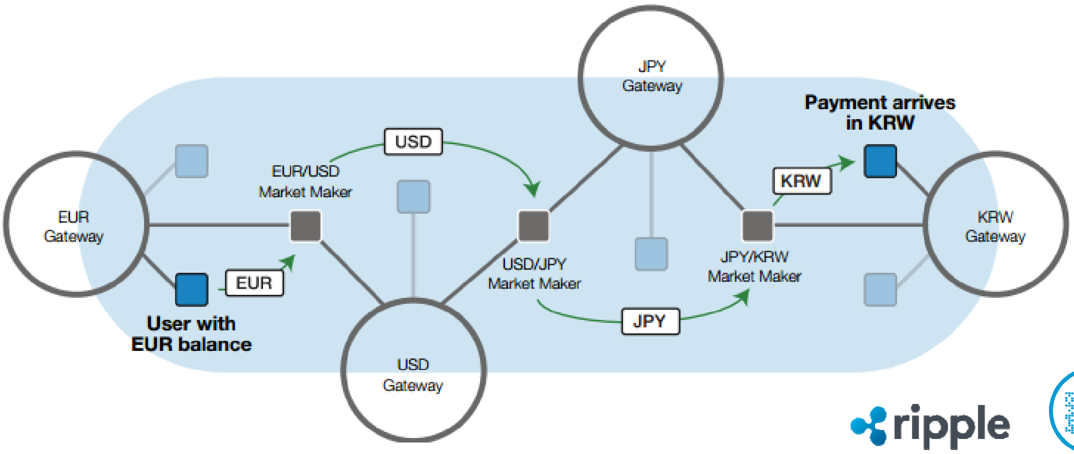


Image source: Ripple.com

ripple

Global Wallet Demo

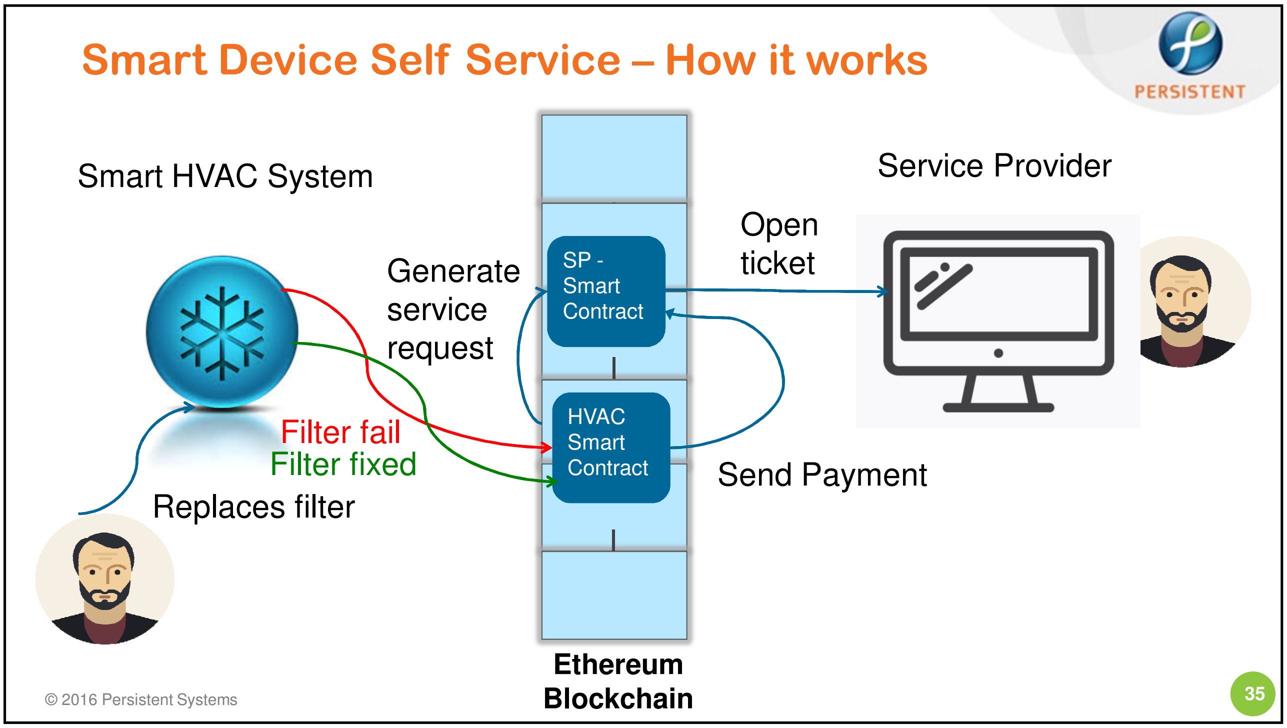
Demo

UC-2: Smart Device Mgmt using Ethereum

- Smart devices can interact via the Blockchain
  - Manage themselves (via smart contract)
  - Interact with other devices
  - Lead to smarter self-managing entities – building, cities and country.
- Smart device self-service request without human intervention.
- All interaction on the Blockchain, which forms the single source of truth.
- Smart contracts can execute and respective state change is logged on the Blockchain for auditing, invoice generation, tracking orders and payment.

Demo

ethereum



Smart Device Self Service – How it works

Smart HVAC System

Service Provider

Generate service request

SP - Smart Contract

Open ticket

HVAC Smart Contract

Filter fail

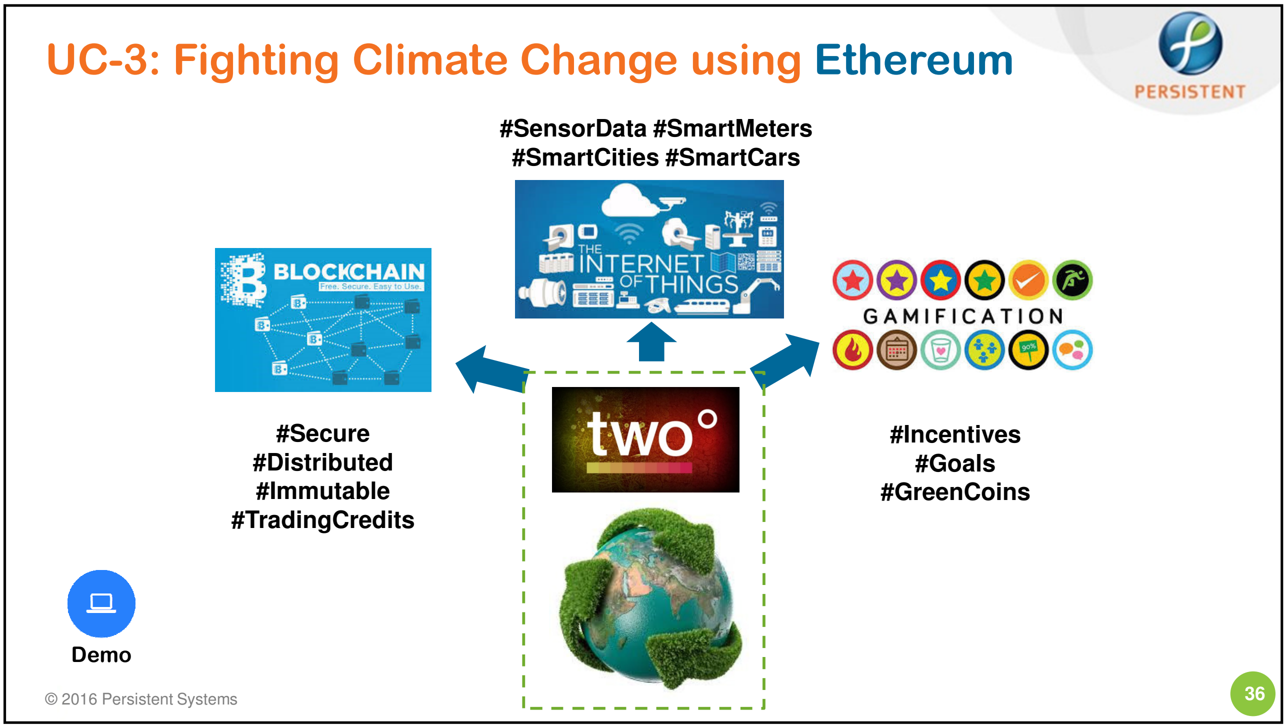
Filter fixed

Replaces filter

Send Payment

Ethereum Blockchain

35



UC-3: Fighting Climate Change using Ethereum

#SensorData #SmartMeters
#SmartCities #SmartCars

#Secure
#Distributed
#Immutable
#TradingCredits

#Incentives
#Goals
#GreenCoins

Demo

36

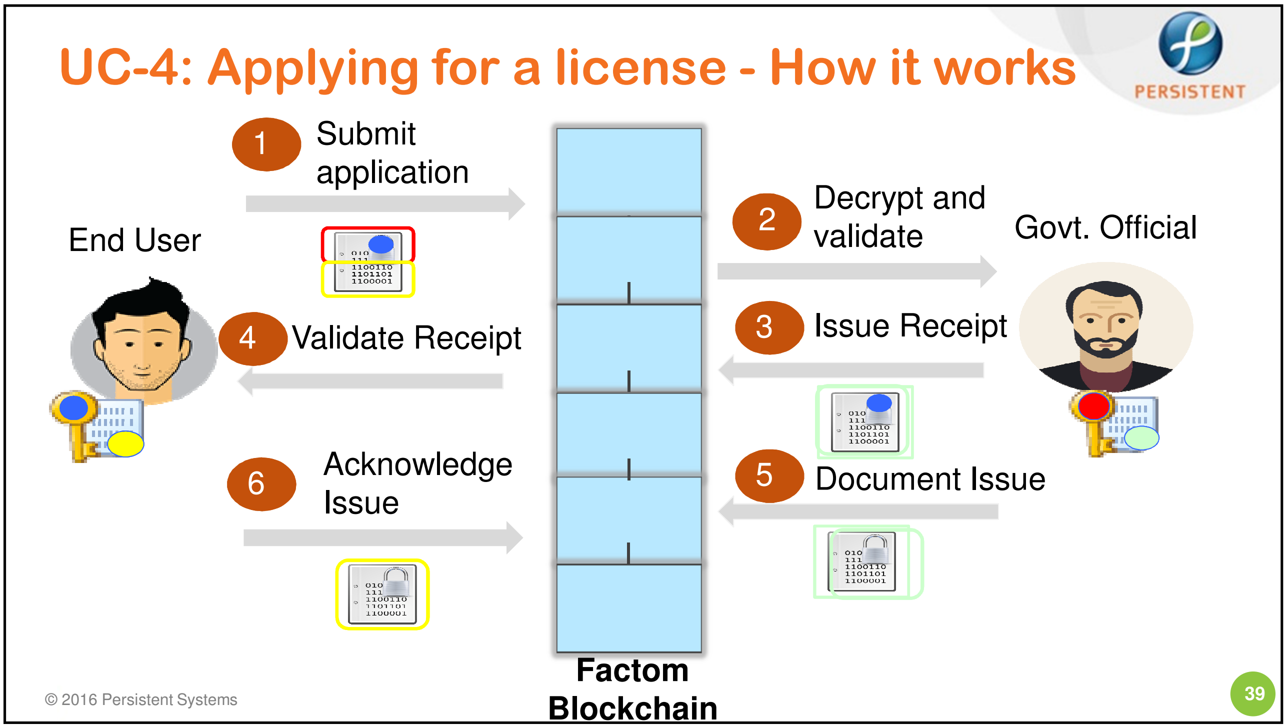
UC-4: E-Governance using Factom

- Blockchain based data publishing platform.
- Ideal for 3Ps applications
  - Proof-of-Existence, Proof-of-Process, Proof-of-Audit
- Helps users to build and use custom chains.
- Chain entries and collected into folders and periodic hashes are anchored into the Bitcoin Blockchain.
- Factom servers store intermediate data hashes and chain information.
- Uses Factoids as its internal cryptocurrency to pay the network.
- No mining – Factom based consensus for adding Entries to the **Blockchain**.

Demo

UC-4: E-Governance Use Case

- Availing Government services is a source of frustration in developing countries
  - No SLAs
  - Corrupt insiders soliciting bribes
  - Lack of overall governance.
- Blockchain can help by making the process auditable and transparent.



UC-4: Applying for a license - How it works

PERSISTENT

End User

1 Submit application

2 Decrypt and validate

Govt. Official

3 Issue Receipt

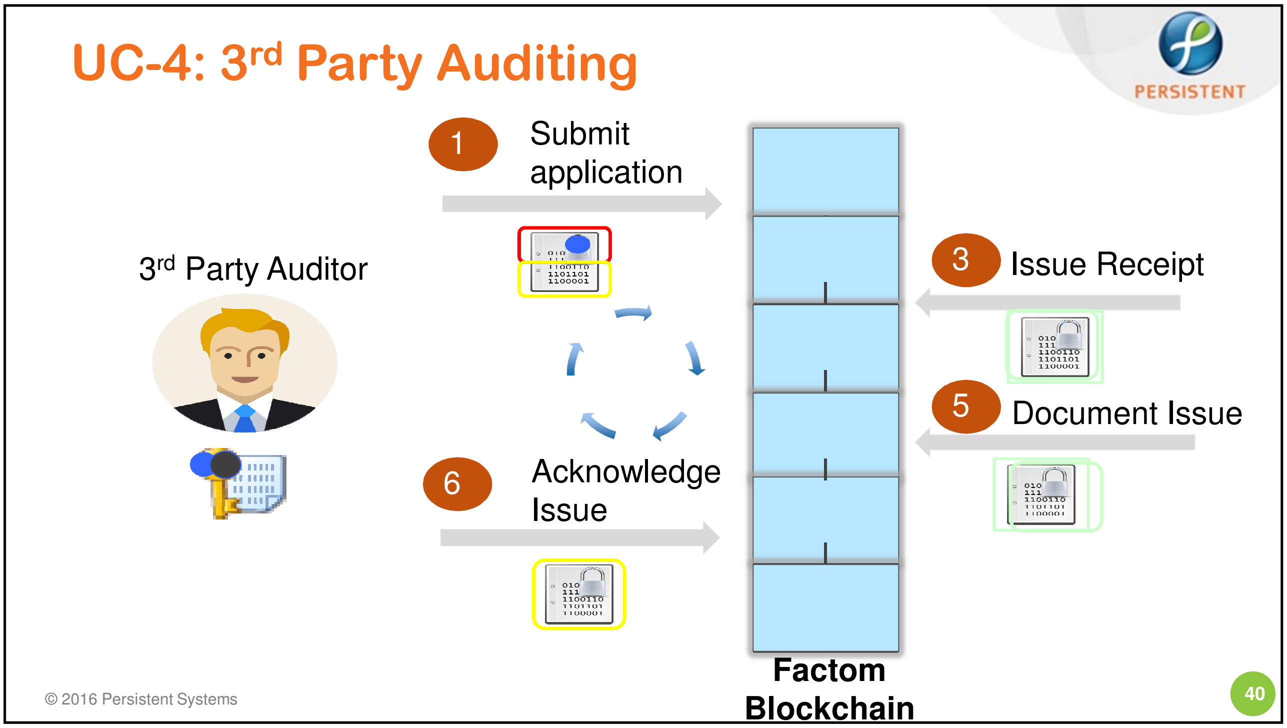
4 Validate Receipt

5 Document Issue

6 Acknowledge Issue

Factom Blockchain

39



UC-4: 3rd Party Auditing

PERSISTENT

3rd Party Auditor

1 Submit application

3 Issue Receipt

5 Document Issue

6 Acknowledge Issue

Factom Blockchain

40

UC-5: Rewards Alliance using IBM OBC

PERSISTENT

Demo

- IBM Open Blockchain allows for building a private permissioned custom blockchains.
- Has support for smart contracts called chaincode.
- Has a Registration Authority that allows for unique identification of all entities interacting with the blockchain.
- Supports private and confidential contracts.
- Allows for modularity in plugging in the desired consensus algorithm that can be run by all validating peers.

Thank You

sid_chatterjee@persistent.com