

Blockchain De-Mystified and Uses

Dr. Tet Yeap

School of Electrical Engineering and Computer Science

Presentation Outline



- Introduction
- Some Basics
- Simplified Blockchain
- Blockchain Categorization
 - Permissionless Blockchain
 - Permissioned Blockchain
- Blockchain Applications





Introduction



uOttawa

What is Blockchain?



- Blockchain is a decentralized software mechanism that enables a public distributed ledger system.
- It allows the tracking and recording of assets and transactions without the presence of a central trust authority such as a bank.
- Importantly, it relies on cryptography to make it difficult for hackers and other cyber criminals to change or steal data.
- It enables peer-to-peer exchange of data, assets and currencies through rules-based smart contracts in a more efficient, transparent and cost-effective manner



What is Blockchain?



- A blockchain is a series of data blocks, each containing information about events or transactions that have recently occurred
- Each block is securely **hashed** — meaning it is rendered into a digital representation and the hash is stored in the next block which makes it nearly tamper proof
- Each data block typically contains four pieces of information: a reference to the previous block, the list of included transactions including the transaction summary which is created by hashing all the transactions in the block, a time stamp, and optionally a cryptographic proof that ensures that the nodes stay true
- The blocks are strung together into a chain and broadcast across the network to various nodes. Each node independently validates the blocks and comes to a consensus about the block's validity before the block is added to the decentralized ledger.





Some Basics



uOttawa

Cryptographic Hash Function



- It is a one-way hash function that maps data of arbitrary size (called the "message") to a bit string of a fixed size (the "hash value", "hash", or "message digest")
- Hash (Data) = Message Digest
- Examples: MD5, RIPEMD, SHA-1, SHA-256

Properties of Cryptographic Hash Function



Five main properties:

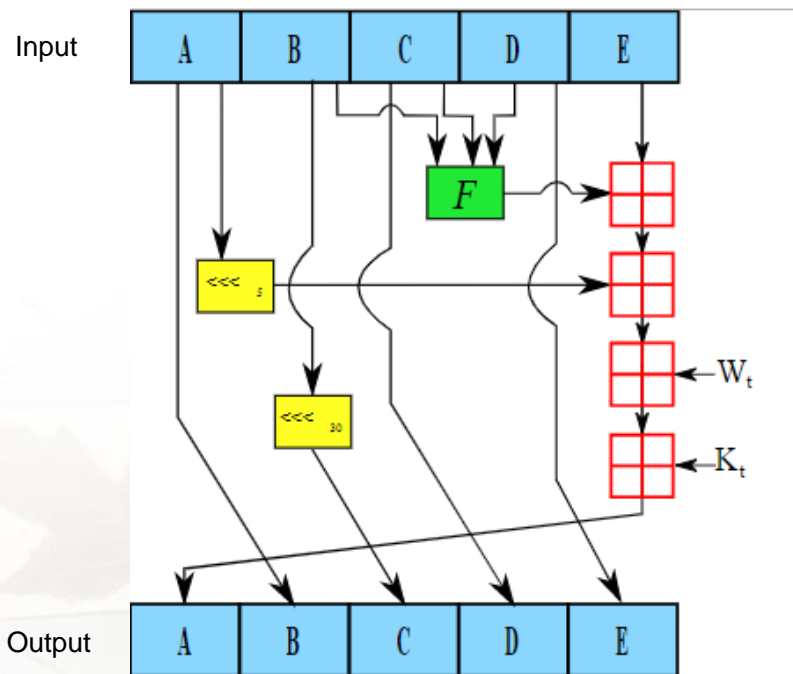
- It is deterministic
- It is quick to compute the hash value for any given message
- It is practically infeasible to generate a message that yields a given hash value
- It is infeasible to find two different messages with the same hash value
- A small change to a message should generate a new hash value uncorrelated with the old hash value



SHA-1 Cryptographic Hash Function



- The Secure Hash Algorithms (SHAs) are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)
- SHA-1 takes an input and produces a 160-bit of hash




A, B, C, D and E are 32-bit **words** of the state

F is a nonlinear function

$\lll n$ denotes left shift by n

W_t is the expanded word message of round t

K_t is the round constant of round t

 is the addition modulo of 2^{32}

Note: Diagram taken from Wikipedia

Cryptographic Nonce



- A cryptographic nonce is an arbitrary number that is only used once.
- A cryptographic nonce can be combined with data to produce different hash digests per nonce:
$$\text{Hash (Data + Nonce)} = \text{Message Digest}$$
- Only changing the nonce value provides a mechanism for obtaining different digest values while keeping the same data.
- This technique is utilized in the Proof of Work consensus model



Simplified Blockchain



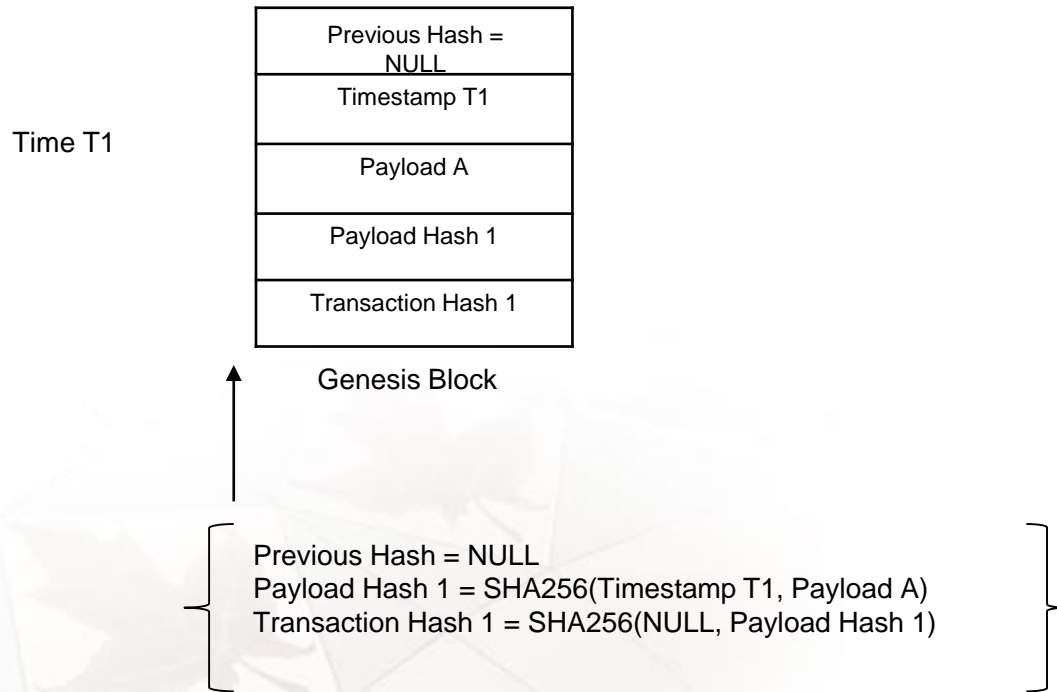
uOttawa

A Simplified Data Block Structure

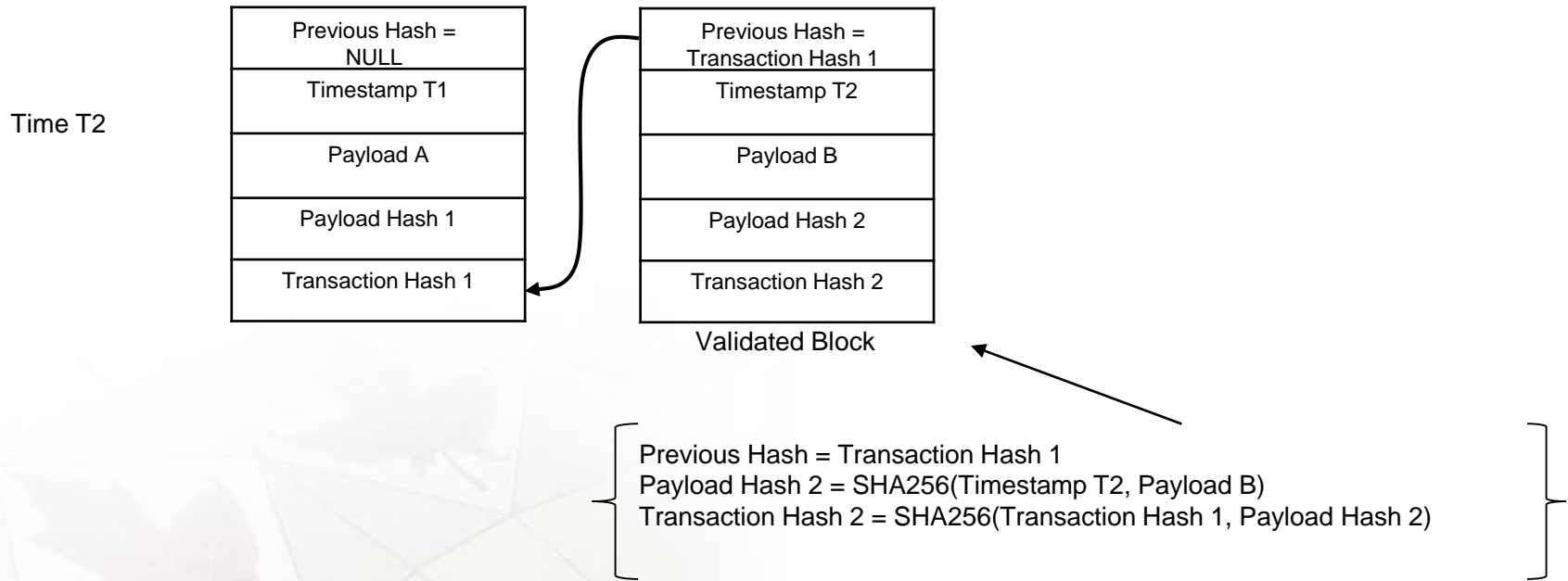


Previous Hash
Timestamp
Payload (Transaction List)
Payload Hash
Transaction Hash

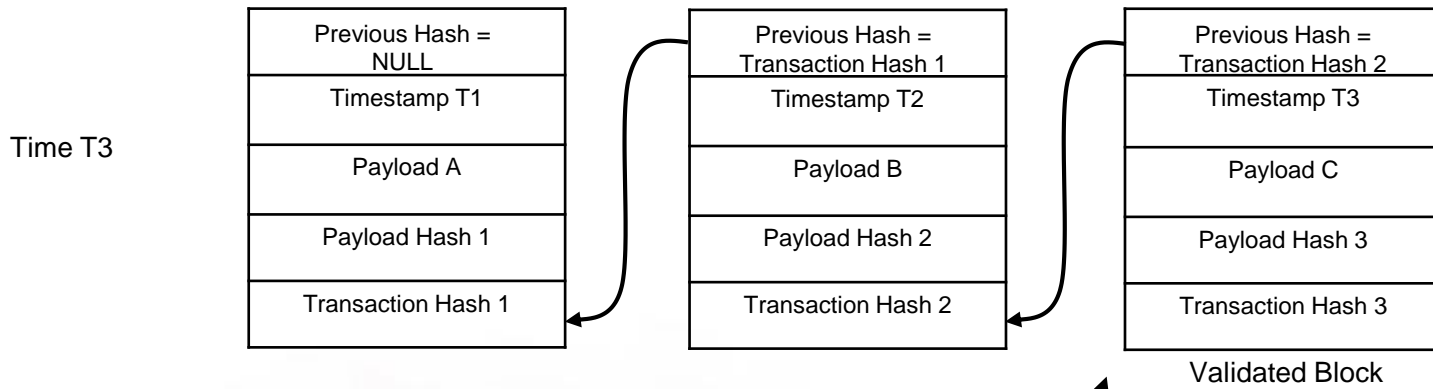
Blockchain Formation (Time T1)



Blockchain Formation (Time 2)



Blockchain Formation (Time T3)



Previous Hash = Transaction Hash 2
Payload Hash 3 = SHA256(Timestamp T3, Payload C)
Transaction Hash 3 = SHA256(Transaction Hash 2, Payload Hash 3)

Properties of Blockchain



- Immutable transaction
 - transaction can only be added
- Tamper-resistant
- Tamper-evident



Blockchain Categorization



uOttawa

Blockchain Categorization



- Blockchain networks can be categorized based on their permission model, which determines who can maintain them (e.g., publish blocks).
- There are two categories:
 - If anyone can publish a new block, it is *permissionless or public*.
 - If only particular users can publish blocks, it is *permissioned or private*.



Permissionless Blockchain



uOttawa

Permissionless or Public Blockchain



- Permissionless or public blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority
- Permissionless blockchain platforms are often open source software, freely available to anyone who wishes to download them. Since anyone has the right to publish blocks, this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain
- Since permissionless blockchain networks are open to all to participate, malicious users may attempt to publish blocks in a way that subverts the system
- To prevent this, permissionless blockchain networks often utilize a multiparty agreement or 'consensus' system that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system



Example of Permissionless Blockchain



- Bitcoin – A Distributed Open Ledger (cryptocurrency) operating in a P2P (Peer-to-Peer) platform
- Early permissionless blockchain platforms involve three overlapping groups: **users**, **nodes**, and **miners**
 - **users** participate in the platform by buying and selling coins by running open source code on their computer. This software broadcasts the **users' required transactions onto the network, to be incorporated into blocks by miners**
 - **miners** assemble transactions into blocks and broadcast those blocks to **nodes** across the P2P network, so the **nodes** can append the new block to their local copies
 - **miners** are rewarded for adding new blocks with newly minted cryptocurrencies, as well as any transaction fees **users** have offered.

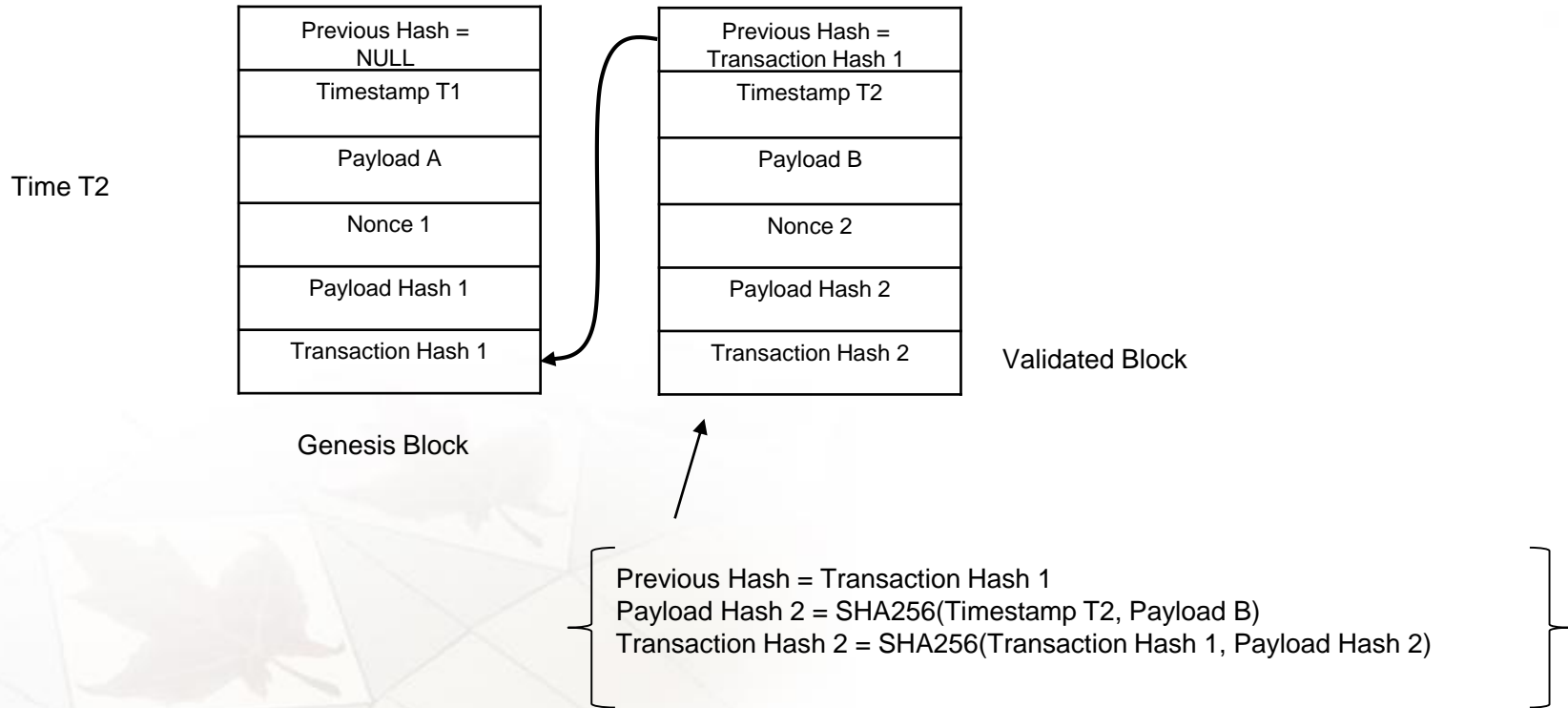


A Data Block Structure



Previous Hash
Timestamp
Payload (Transaction List)
Nonce
Payload Hash
Transaction Hash

Blockchain Formation (Time 2)



Proof of Work Consensus Model



- For permissionless blockchain networks there are generally many publishing nodes or miners competing at the same time to publish the next block. The miners usually do this to win cryptocurrency and/or transaction fees
- Use *consensus models* to enable a group of mutually distrusting miners to work together
- A miner publishes the next block by being the first to solve a computationally intensive puzzle. The solution to this puzzle is the “proof” they have performed work
- A common puzzle method is to require that the hash digest of transaction hash be less than a target value by essentially either increases or decreases the number of leading zeros required. Publishing nodes make many small changes to their transaction hash by applying cryptographic nonce technique



Example of Cryptographic Nonce



- Consider a puzzle where, using the SHA-256 algorithm, a computer must find a hash value meeting the following target criteria (known as the difficulty level):

SHA256("blockchain" + Nonce) = Hash Digest starting with "**000000**"

- Sample output:

SHA256("blockchain0") = 0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938 (not solved)

SHA256("blockchain1") = 0xdb0b9c1cb5e9c680dff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10 (not solved)

SHA256("blockchain10730895") = 0x**000000**a1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587 (solved)

- To solve this puzzle, it took 10,730,896 guesses

Note: Example taken from NISTIR 8202 Report, US Department of Commerce

Other Consensus Models for Permissionless Blockchain



- Proof of Stake Consensus Model
 - It is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it
 - Stake is often an amount of cryptocurrency that the blockchain network user has invested into the system. Once staked, the cryptocurrency is generally no longer able to be spent
- Delegated Proof of Stake
 - users vote for nodes to become publishing nodes – therefore creating blocks on their behalf. Blockchain network users' voting power is tied to their stake so the larger the stake, the more weight the vote has. Nodes who receive the most votes become publishing nodes and can validate and publish blocks





Permissioned Blockchain



uOttawa

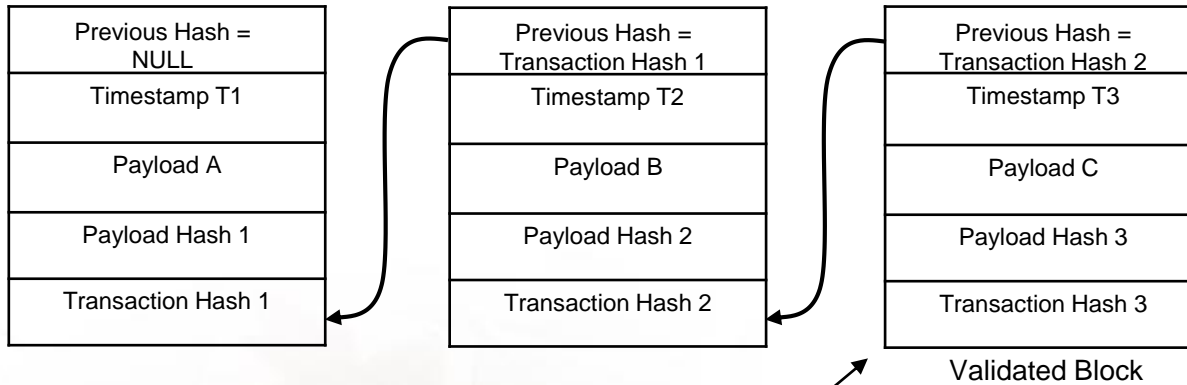
Permissioned or Private Blockchain



- Permissioned or private blockchain networks are ones where users publishing blocks must be authorized by some authority. They may be instantiated and maintained using open source or closed source software
- Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions
- Permissioned blockchain networks may allow anyone to read the blockchain or they may restrict read access to authorized individuals
- Permissioned blockchain also use consensus models for publishing blocks, but the methods are then usually faster and less computationally expensive since the establishment of one's identity is required to participate as a member of the blockchain network



Permissioned Blockchain



Previous Hash = Transaction Hash 2
Payload Hash 3 = SHA256(Timestamp T3, Payload C)
Transaction Hash 3 = SHA256(Transaction Hash 2, Payload Hash 3)



Consensus Models for Permissioned Blockchain



- Round Robin Consensus Model
 - ✓ With this model of consensus, nodes take turns in creating blocks
- Proof of Authority Consensus Model
 - ✓ Publishing nodes must have their identities proven and verifiable within the blockchain network. Publishing nodes can lose reputation by acting in a way that the users disagree with. Therefore, it is in the interest of a publishing node to maintain a high reputation
- Proof of Elapsed Time Consensus Model
 - ✓ Each publishing node requests a wait time from a secure hardware time source which generate a random wait time and return it to the publishing node software. Publishing nodes take the random time and become idle for that duration. Once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network, alerting the other nodes of the new block





Differences between Database and Blockchain



uOttawa

Comparisons



Traditional Database

- A traditional database is centralized
- Everyone needs to trust the administrator managing the database
- There's typically no immutability or provenance

Distributed Database

- Distributed databases do not alleviate the trust issue
- There are now more copies to worry about and more administrators

Blockchain

- Blockchain allows the concept of a distributed database to be deployed across an untrusted network
- Something a traditional database cannot handle
 - ✓ Immutable
 - ✓ Tamper-resistant
 - ✓ Tamper-evident

Note: Information taken from an IBM presentation on blockchain



Blockchain Applications



uOttawa

Potential Blockchain Applications



Blockchain technology solutions may be suitable if the activities or systems require features such as:

- Many participants
- Distributed participants
- Want or need for lack of trusted third party
- Workflow is transactional in nature
- A need for a decentralized naming service or ordered registry
- A need to reduce or eliminate manual efforts of reconciliation and dispute resolutions
- A need to enable real time monitoring of activity between regulators and regulated entities
- A need for full provenance of digital assets and a full transactional history to be shared amongst participants



Smart Contracts



- It refers to a blockchain based computer program that automatically brings about some specific action, such as carrying out transfers of, or executing other actions relating to, digital assets according to a set of pre-specified rules.
- It aims to capture in the software the semantics of potentially complex interactions and thus can be used to automate agreements between parties according to the set of instructions written into their code



Smart Contract Applications



- Financial Services

- Banking and Finance

- ✓Blockchain could be applied to enhance security, simplification and cost reduction, and transparency



Smart Contract Applications



- Financial Services

- Securities Brokerage and Trade settlement

- ✓Trade settlement processes typically require two to three days for payments and securities to change hands. Blockchain could eliminate or change the role of intermediaries, resulting in reduced commissions and other costs. Trades could be settled instantaneously



Smart Contract Applications



- Financial Services

- Insurance

- ✓Having trusted blockchain ledgers of various events and identities could eliminate the need for human triggers. A smart insurance contract would pay out against the insurable event without the policyholder having to make a claim or the insurer having to administer the claim. This will essentially remove the cost of claims processing and minimize fraud



Smart Contract Applications



- Non-financial Industries

- Entertainment industries

- ✓It can transform everything from proof of creation to ownership, transfers of digital assets, rights management, micropayments and creative collaboration



Smart Contract Applications



- Non-financial Industries

- Property ownership

- ✓Blockchain can be used not only for transactions, but as a registry and inventory system for any asset ranging from raw materials to intellectual property.

Smart Contract Applications



- Non-financial Industries

- Manufacturing and Inventory control

- ✓ Manufacturing value chains are complex, multi-tiered combinations of various types of organizations providing design, sourcing, manufacturing, delivery and service across multiple geographies. Blockchain quickly and inexpensively provides trust in the identity and legitimacy of any partner in any financial or trading relationship. This reduces manufacturing cost and time to reconcile transactions



Smart Contract Applications



- Non-financial Industries

- Healthcare

- ✓ Blockchains could address interoperability challenges in clinical, research as well as administrative areas. Digital transaction ledgers could be securely shared among a wide group of stakeholders, who could directly exchange data using a virtually impenetrable and immutable ledger.
 - ✓ Electronic health records (EHR) is a critical area of interoperability where blockchain would offer an array of benefits and capabilities

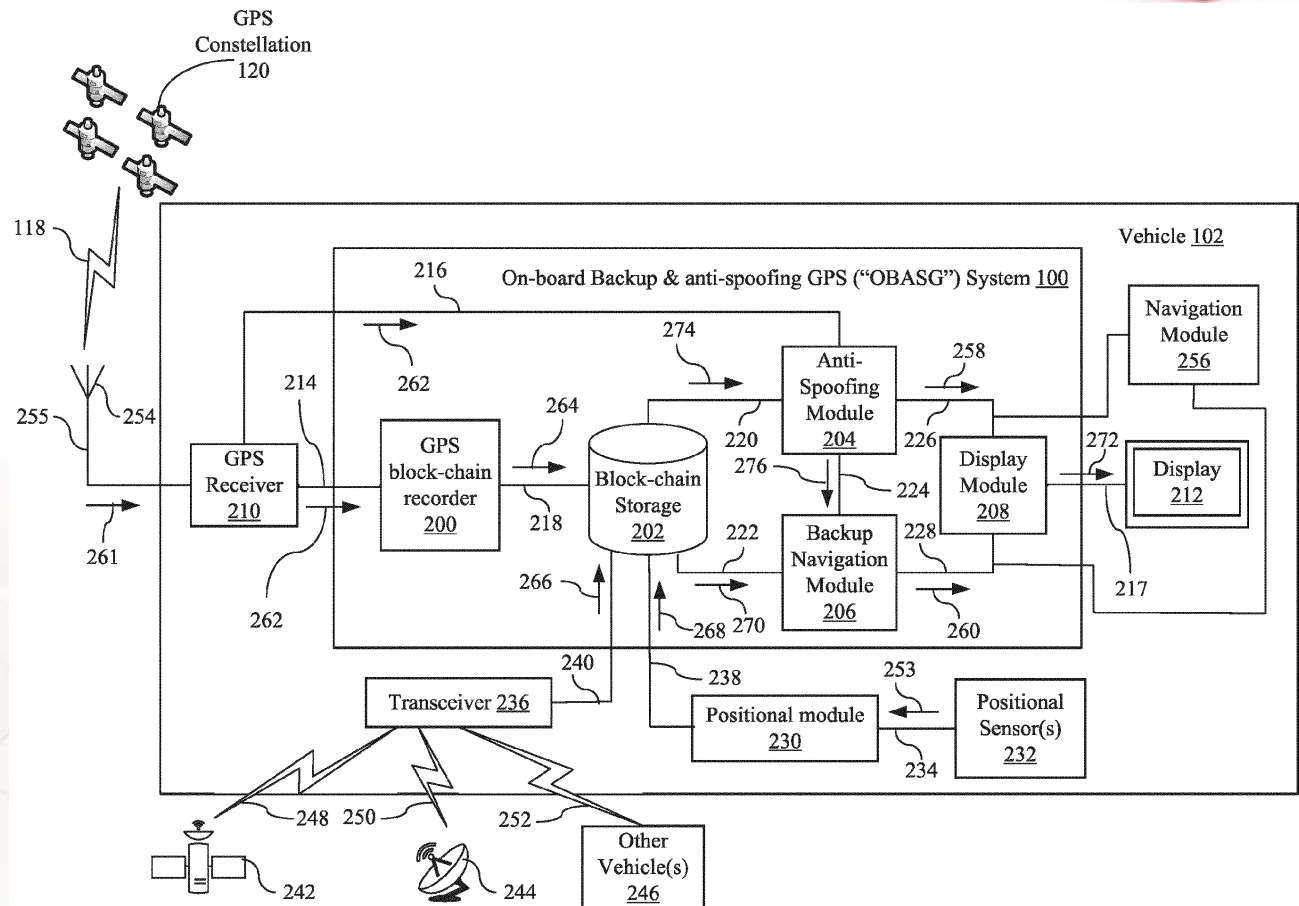


On-board backup and anti-spoofing GPS system by Boeing



An on-board backup and anti-spoofing GPS ("OBASG") system for navigating a vehicle through an environment with a GPS receiver is proposed by *Boeing Co.*

In general, the OBASG includes a **GPS block-chain recorder**, a **block-chain storage module**, an **anti-spoofing module**, and a **backup navigation module**.





Q & A?



uOttawa