Introduction to Blockchain Technology and Smart Contract

DR. Amit Kumar Vishwakarma
Blockchain Consultant

AJNIFM, Ministry of Finance, India

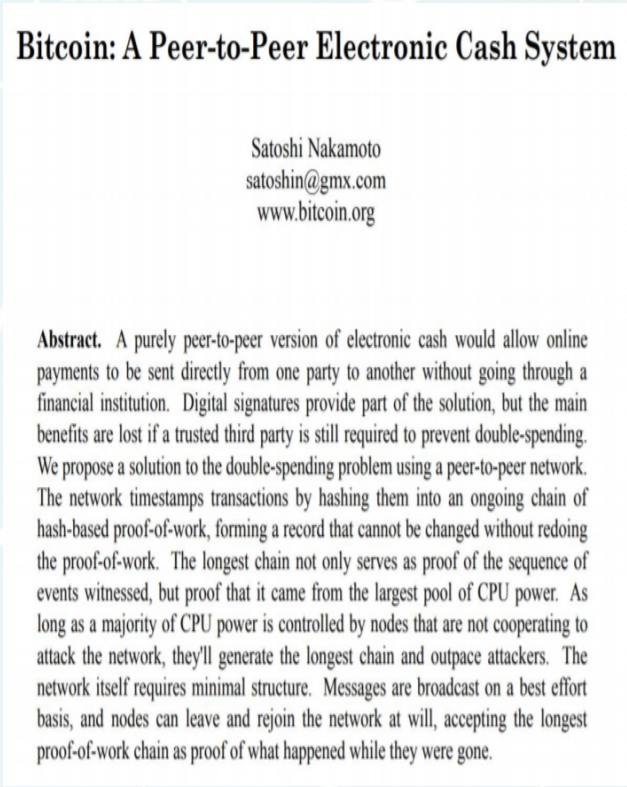
amitvec1014@gmail.com

March 17, 2023

Table of Content

Origin of Blockchain

- **August 2008**, domain name bitcoin.org was registered.
- **October 2008**, a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was published by the name Satoshi Nakamoto
- aka. DLT = Distributed Ledger Technology
- Developed for Bitcoin, the first distributed cryptocurrency
- **The Problem**, How to perform digital currency transactions between users directly, without an intermediary.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Immutable and Irreversible

- Blockchain is immutable - Blockchain data can't be changed
- Blocks can't be deleted
- As each block contains a hash value of the previous dependent block
- All the blocks are chained and linked
- Entries are immutable and irreversible.
- Data tamper proof
- If any node tries to modify a block, then the entire blockchain will be invalidated
- How does it works?

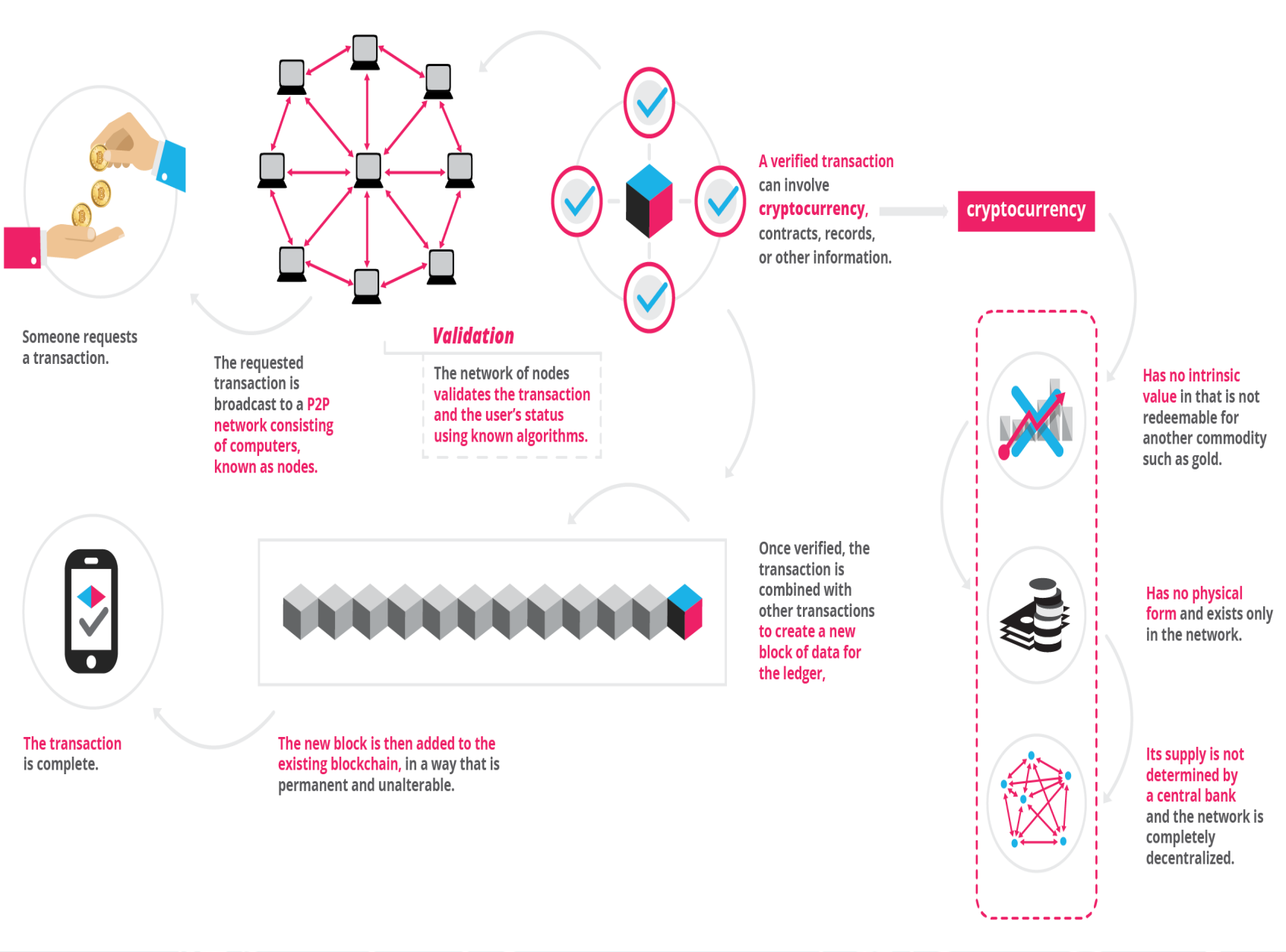


Figure: Blockchain based transaction

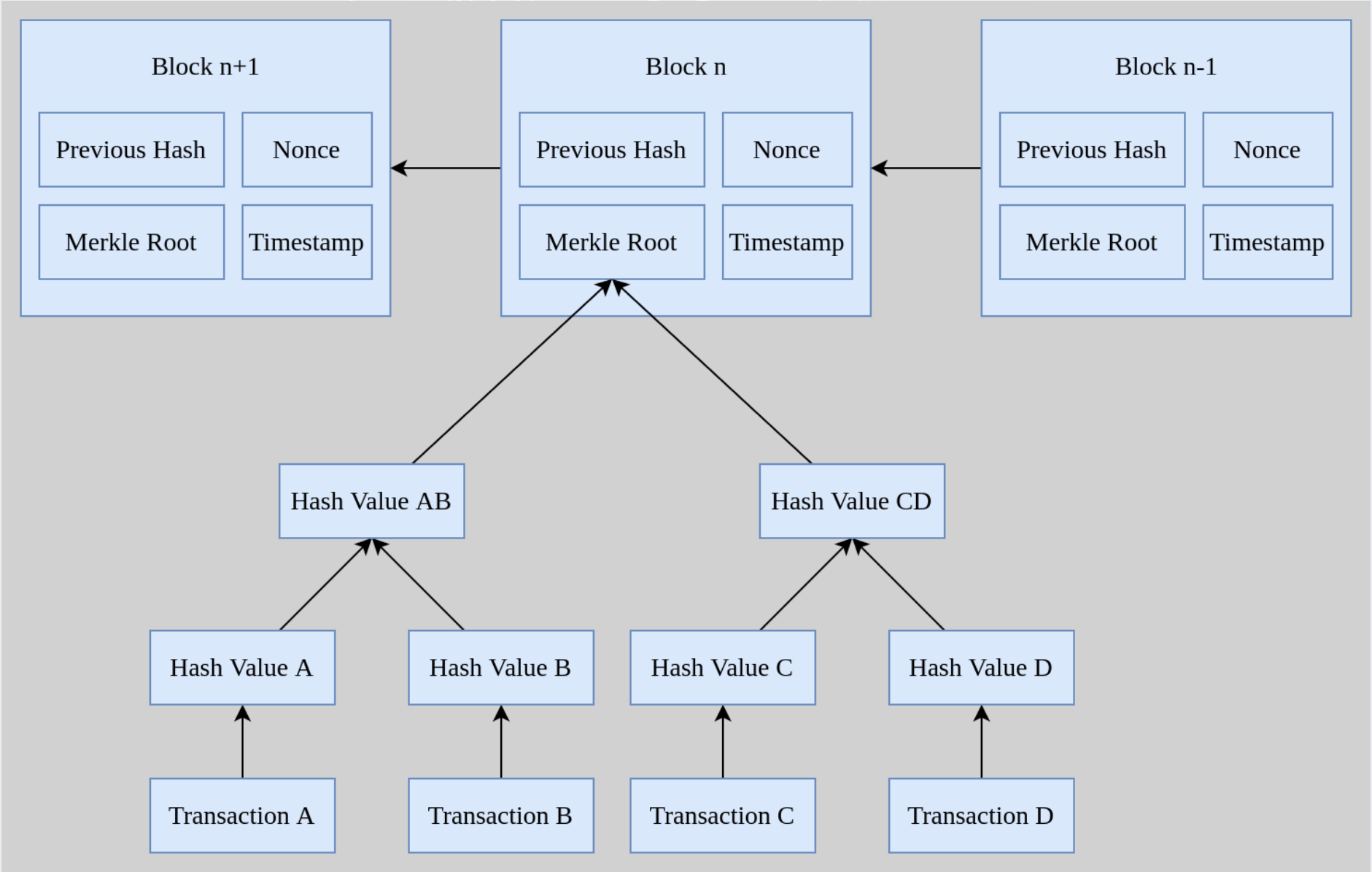


Figure: Blocks in blockchain

Hash

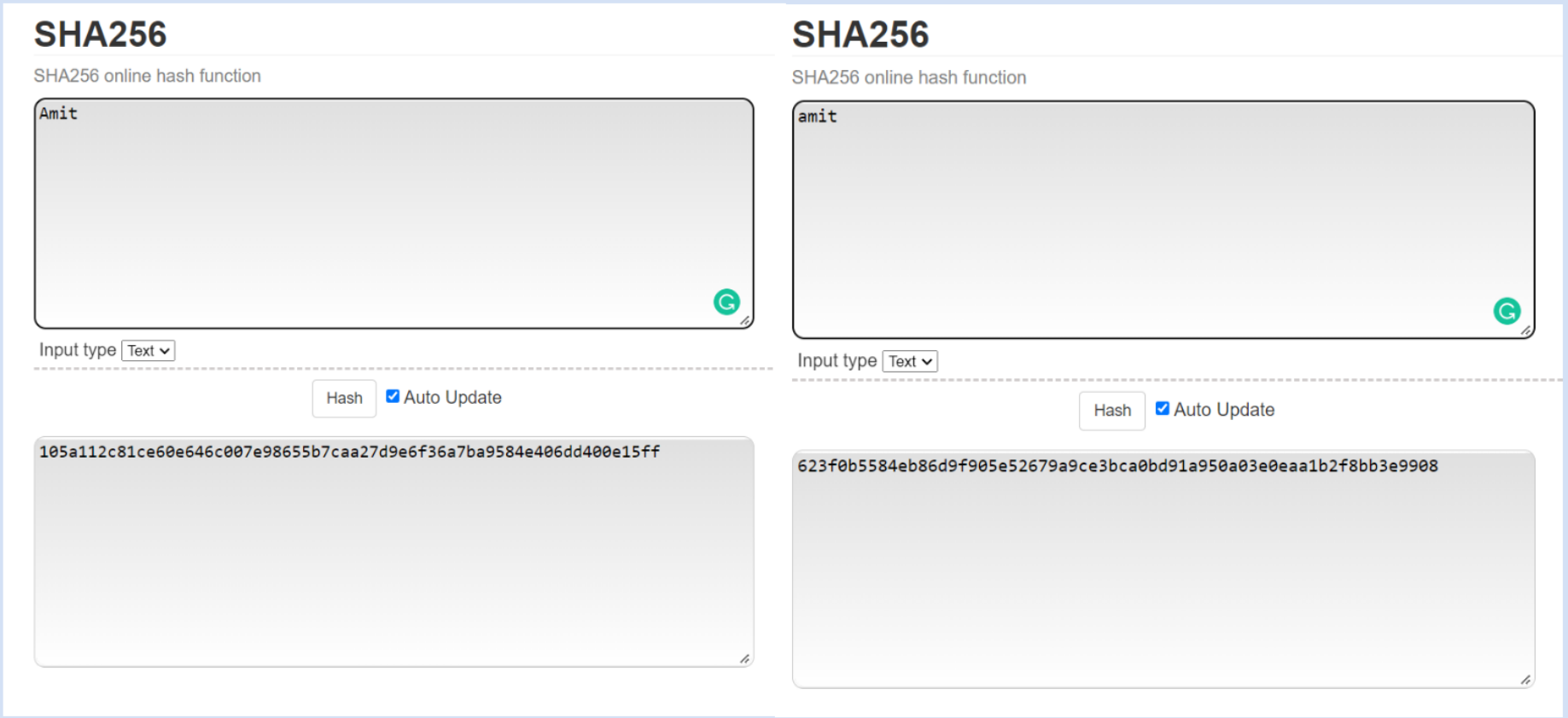


Figure: Hashing

Merkle Root

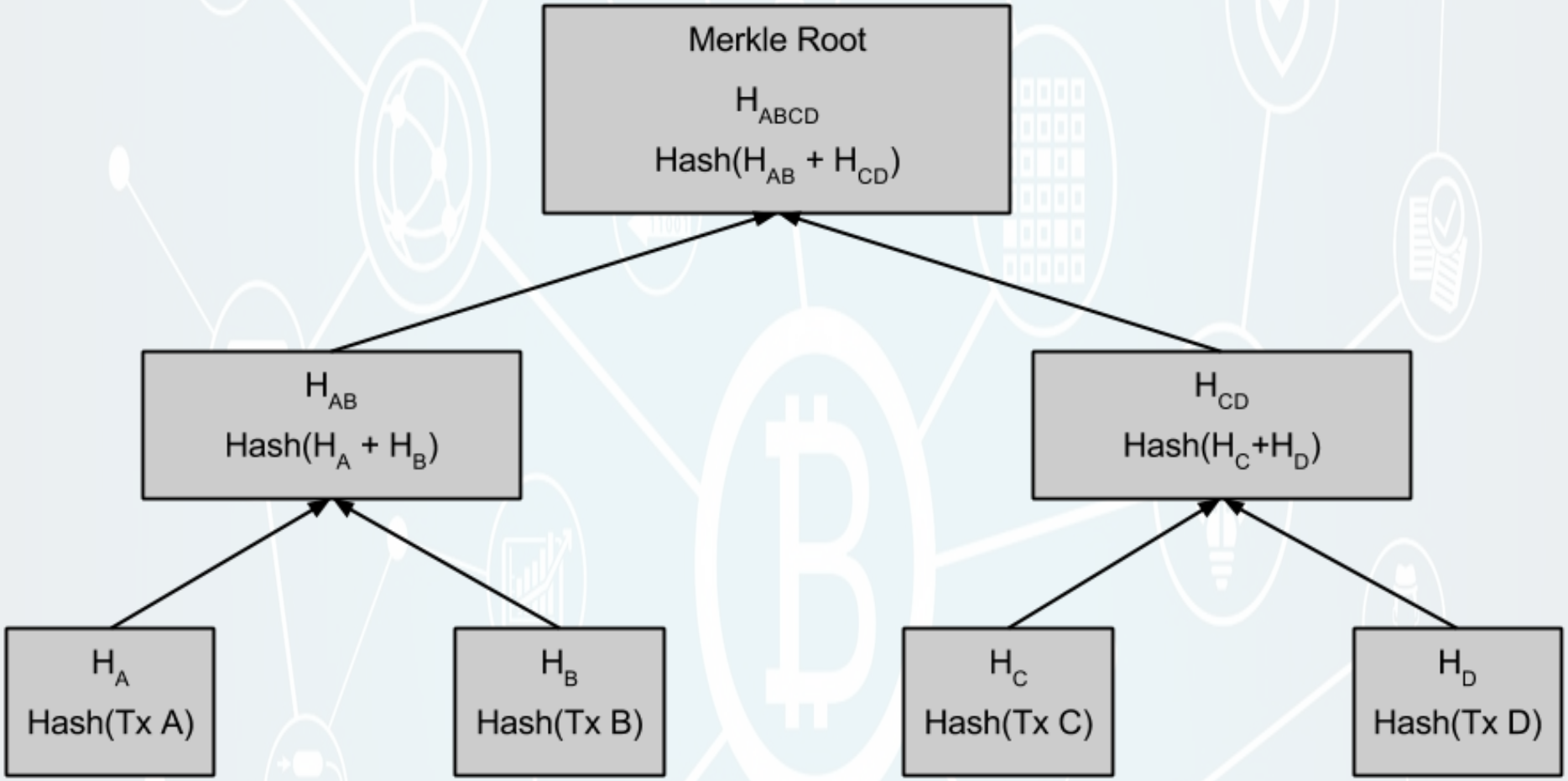


Figure: Merkle Tree

Block of Blockchain

Details

Hash	00000-7b7df	Depth	8
Capacity	169.35%	Size	1,775,731
Distance	14y 2m 9d 15h 46m 54s	Version	0×20008000
BTC	12,699.5330	Merkle Root	2e-83
Value	$309,575,881	Difficulty	43,551,722,213,590.37
Value Today	$309,711,005	Nonce	3,275,958,763
Average Value	5.4833907781 BTC	Bits	386,299,521
Median Value	0.02019931 BTC	Weight	3,993,379 WU
Input Value	12,699.85 BTC	Minted	6.25 BTC
Output Value	12,706.10 BTC	Reward	6.56983423 BTC
Transactions	2,316	Mined on	14 Mar 2023, 14:02:50
Witness Tx's	1,986	Height	780,753
Inputs	5,503	Confirmations	8
Outputs	7,786	Fee Range	0-2,155 sat/vByte
Fees	0.31983423 BTC	Average Fee	0.00013810
Fees Kb	0.0001801 BTC	Median Fee	0.00003667
Fees kWU	0.0000801 BTC	Miner	Unknown

Blockchain Process

- A transaction is transformed into a hash
- The hash of a whole block is created
- A nonce (Random String) is appended to the hash and hashed again
- The resulting hash is compared to the difficulty level required by a blockchain
- It is less than the difficulty level, other nodes on the network check and confirms the solution and update their instances of the blockchain
- If not, then the nonce is changed, and the trial-and-error process repeats
- The hash of the header becomes the new blocks identifying strings, and the addition is propagated through the network
- That block is now part of the ledger
- The miners responsible for this are rewarded (If there is a reward associated with mining)

Blockchain is a Trust Protocol

- A distributed public/private open/closed database where records are kept tamper-proof by virtue of its technical implementation alone
- Enables decentralized authority (A 3rd party intermediary authority is no longer required.)
- Provide privacy, transparency, and security
- Application in a wide range of areas

Various Implementations

Public & Closed	**Public & Open**
• Voting • Voting Records • Whistleblower	• Crypto Currencies • Betting • Video Games
Private & Closed	**Private & Open**
• National Defence • Law Enforcement • Millitary • Tax Returns	• Supply Chain • Government Financial Records • Corporate Earning Statements

Consensus Algorithm in Blockchain

- **Proof of Work (PoW) Algorithm:** PoW is a piece of data that is difficult to produce but easy for others to verify and satisfies certain requirements.
- Bitcoin network asks miners to prove computing efforts.
- Prop: Low Throughput, Higher latency, Large Power Consumption, Large Open Networks, Cryptocurrency applications.
- **Proof of Stake (PoS) Algorithm:** Asks miners to prove ownership of a certain amount of cryptocurrency.
- Prop: Similar to POW but Power Consumption Efficient, Complex implementation could be made faster.
- **Byzantine Fault-Tolerant Algorithms:** Database replication protocol used in closed blockchain with limited nodes.
- Prop: High Throughput and Lower Latency, Small Closed Networks, Enterprise Solutions.

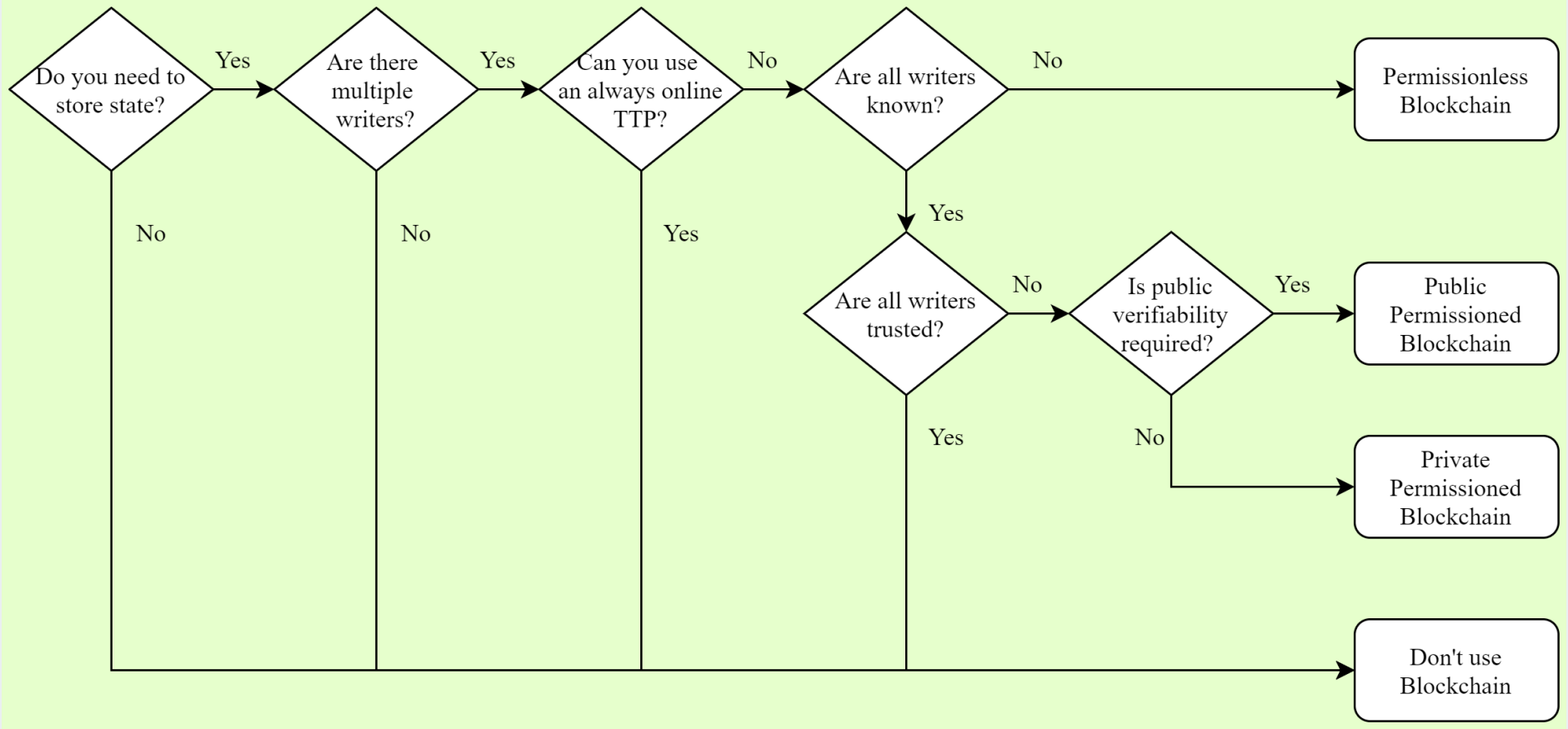


Figure: Do we really need blockchain?

Blockchain Evolution

Blockchain 2.0 (Ethereum 2014)

- Ethereum is a global, open-source platform for decentralized applications.
- On Ethereum, you can write code that controls digital value, runs exactly as programmed and is accessible anywhere in the world.

Ethereum

"Ethereum is the foundation for a new era of the internet:

1. An internet where money and payments are built-in
2. An internet where users can own their data, and your apps don't spy and steal from you
3. An internet where everyone has access to an open financial system
4. An internet built on neutral, open-access infrastructure, controlled by no company or person

Ethereum is programmable, which means that developers can use it to build new kinds of applications. "

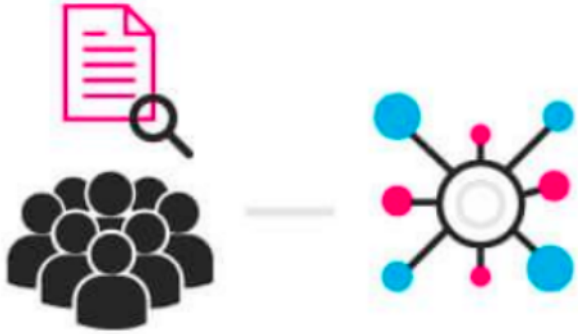
Smart Contract

- Introduced by Nick Szabo in 1994
- Help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman

What is Smart Contract?

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger

A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms



Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors positions

What is Smart Contract?

Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers

The terms and conditions of an agreement is written in code

What is Smart Contract?

Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers

The terms and conditions of an agreement is written in code

These agreements facilitate the exxchange of money, shares, property etc.

What is Smart Contract?

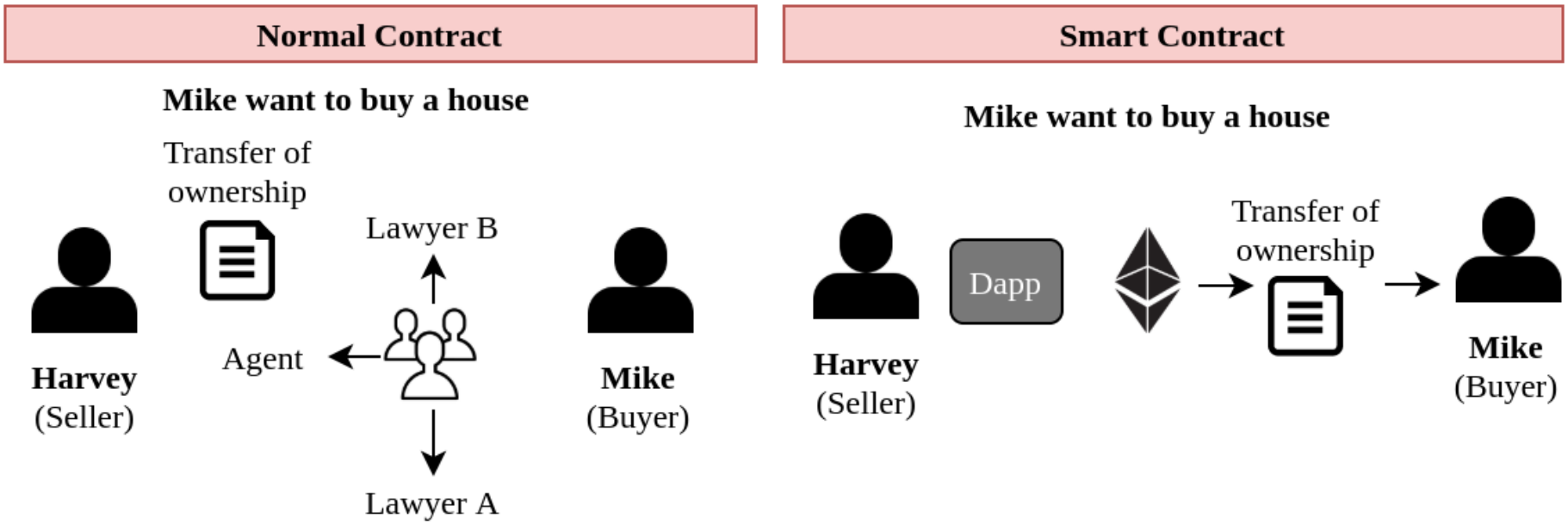
Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers

The terms and conditions of an agreement is written in code

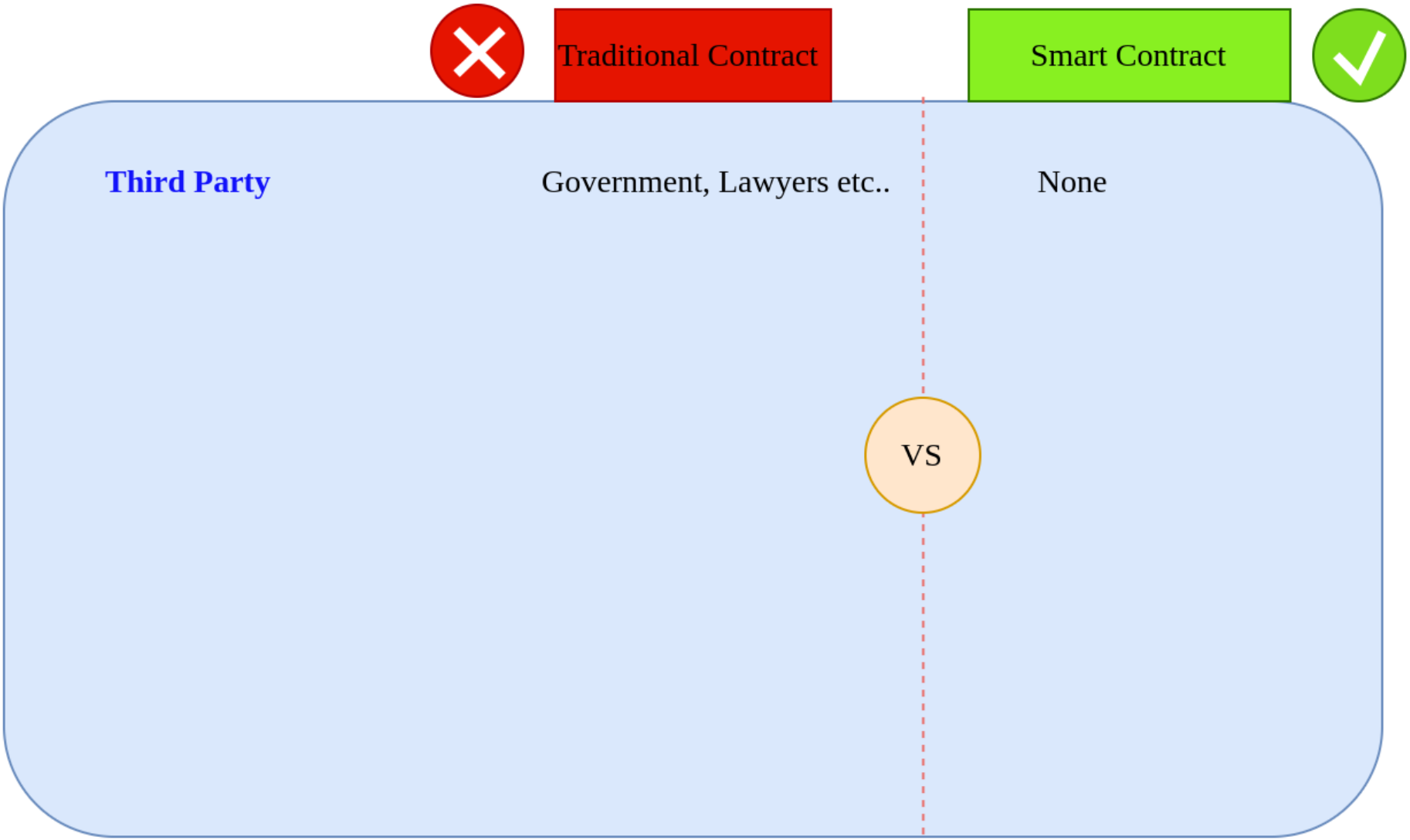
These agreements facilitate the exxchange of money, shares, property etc.

It executes in blockchains decentralized platform

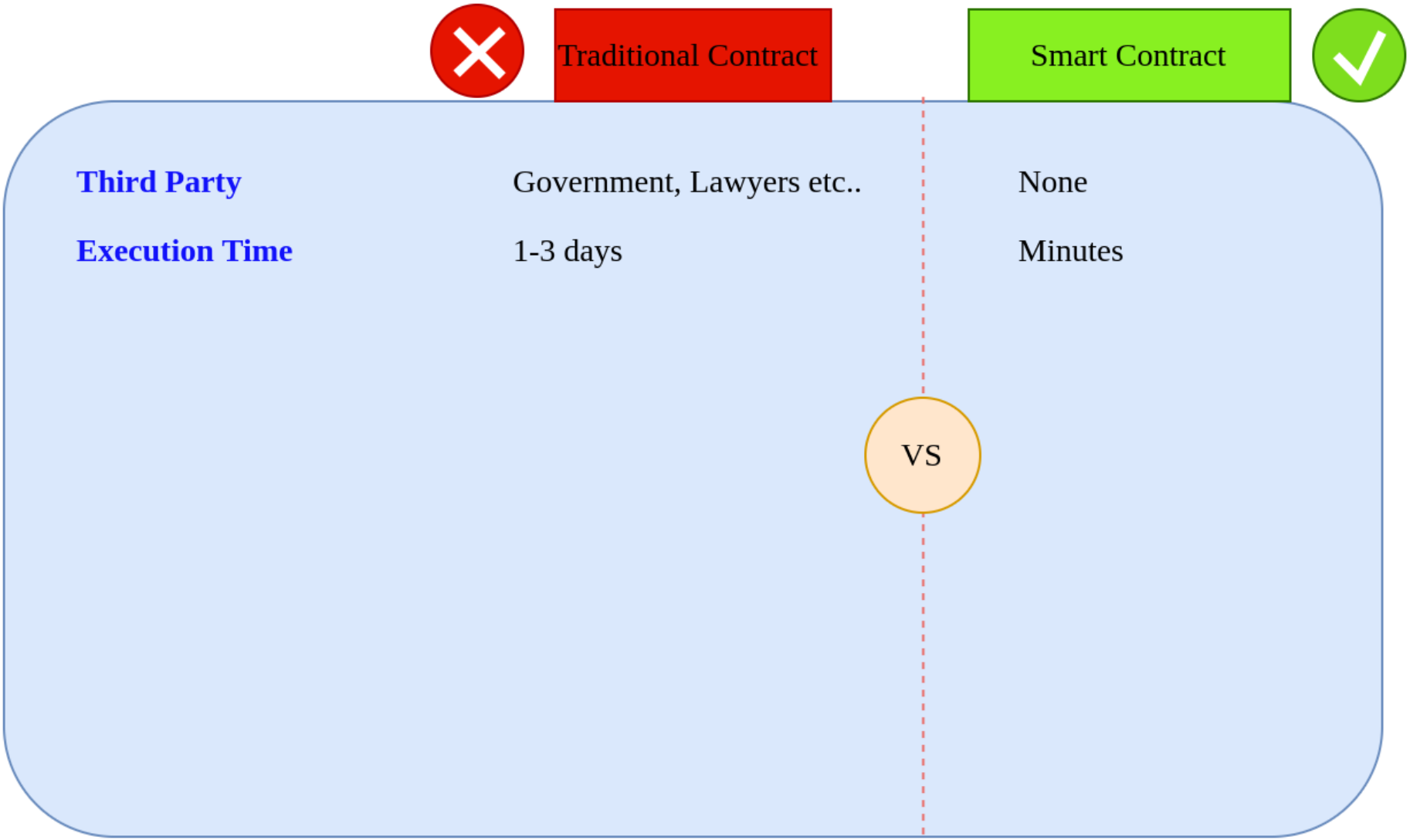
Why Smart Contract?



Why Smart Contract?



Why Smart Contract?



Why Smart Contract?

Traditional Contract

Smart Contract

Third Party	Government, Lawyers etc..	None
Execution Time	1-3 days	Minutes
Remittance	Manual Process	Automatic Process

VS

Why Smart Contract?

Traditional Contract

Smart Contract

Third Party	Government, Lawyers etc..	None
Execution Time	1-3 days	Minutes
Remittance	Manual Process	Automatic Process
Transparency	Unavailable	Available

VS

Why Smart Contract?

	Traditional Contract		Smart Contract
Third Party	Government, Lawyers etc..		None
Execution Time	1-3 days		Minutes
Remittance	Manual Process		Automatic Process
Transparency	Unavailable	VS	Available
Archiving	Difficult		Easy

Why Smart Contract?

	Traditional Contract		Smart Contract
Third Party	Government, Lawyers etc..		None
Execution Time	1-3 days		Minutes
Remittance	Manual Process		Automatic Process
Transparency	Unavailable	VS	Available
Archiving	Difficult		Easy
Security	Limited		Cryptographically Secure

Why Smart Contract?

	Traditional Contract		Smart Contract
Third Party	Government, Lawyers etc..		None
Execution Time	1-3 days		Minutes
Remittance	Manual Process		Automatic Process
Transparency	Unavailable	VS	Available
Archiving	Difficult		Easy
Security	Limited		Cryptographically Secure
Cost	Expensive		Cheap

Why Smart Contract?

	Traditional Contract		Smart Contract
Third Party	Government, Lawyers etc..		None
Execution Time	1-3 days		Minutes
Remittance	Manual Process		Automatic Process
Transparency	Unavailable	VS	Available
Archiving	Difficult		Easy
Security	Limited		Cryptographically Secure
Cost	Expensive		Cheap
Signature	Manual Process		Digital Signature

Ethereum smart contracts  need **gas** to run

Task	Gas Required	Cost (ETH)	Cost (USD)	Ops per ETH	Ops per USD	Ops per Block	Blocks to complete Op
Add or subtract two integers	3	0.00000009	0.00002655	11111111.11	37664.78343	1566666.667	0.0000006382978723
Add or subtract two integers 1 million times	3000000	0.09	26.55	11.11111111	0.03766478343	1.566666667	0.6382978723

Task	Gas Required	Cost (ETH)	Cost (USD)	Ops per ETH	Ops per USD	Ops per Block	Blocks to complete Op
Save a 256-bit word to storage	20000	0.0006	0.177	1666.666667	5.649717514	235	0.004255319149
Save 1 MB to storage (31250 256-bit words)	625000000	18.75	5531.25	0.05333333333	0.000180790960	0.00752	132.9787234
Save 1 GB to storage (1000 MB)	625000000000	18750	5531250	0.000053333333	0.000000180790	0.00000752	132978.7234

Smart Contract Application

Digital Identity

Access to your identity can play a vital part in safekeeping all of your sensitive information. With smart contracts, it's possible to allow third parties to access a certain part of your identification without fully revealing all of the information.

This allows the third party to validate your information, but you still retain full control over your identification.

Smart Contract Application

Securities

With smart contracts, managing securities can be improved and simplified. Usually, there are intermediaries involved in security custody chains. Therefore, there is always a vulnerability involved.

But smart contracts can reduce the operation risk of securities and make the workflow more digitized. Users can also use it for automatic payments, dividends, stock splits, and even liability management.

Smart Contract Application

Cross Border Payments

Making cross-border payments can be more simplified using smart contracts, mainly in tokenization of assets where the owner can define the attributes of the asset and then send that asset to other parties.

Also, cross-border payments need to adhere to many laws, which can restrict businesses. But with smart contracts, partners residing in different countries can work together without any financial issues.

Smart Contract Application

Loans

Smart contracts can help in facilitating loans. For example, it can connect the lender and borrower over a blockchain platform where the lender can lend the money to the borrower based on certain conditions.

It will track the conditions and follow the rules based on the outcome of the borrowers – whether the loan was paid off in due time or not.

Smart Contract Application

Financial Data Recording

Smart contracts can play a huge part in recording the financial data of a company. These offer a more proven way to record these data in a transparent and accurate environment.

Using smart contracts, it's possible to collect data uniformly throughout a company's business processes without needing any regular auditing.

Smart Contract Application

Government

As smart contracts have automated features, it can help the government to run operations without interference from third parties. Operations such as recording land titles can be done more efficiently and faster.

Also, as it's a public record, there is no option for anyone to alter it as they want. Another possible use case is electronic elections, where smart contracts can count the votes and automate the whole process.

Smart Contract Application

Supply Chain Management

Smart contracts can improve supply chain management greatly. If companies integrate smart contracts in all parts of the supply chain processes, it can help track items to record data in real-time.

It can also manage inventories and help to process all transactions and payments throughout the supply chain faster.

Smart Contract Application

Insurance

Smart contracts can automate the process of insurance claims. Insurers can use contracts to facilitate their insurance filing processes and save time.

Using blockchain, smart contracts can verify the documentation and data and process the insurance claims if it falls within the conditions. Everything is stored on the immutable ledger in blockchain, so no one can bypass the conditions or alter them.

Advantages of Smart Contract

- Autonomy: no need for trusted third party
- Trust: data stored in a shared ledger (cannot be lost)
- Backup: data duplication
- Speed: automating various processes

Challenges of Smart Contract

- Scalability
- Interoperability
- Regulatory challenges
- Governance
- Lack of digital literacy


Thank You