SUMOTEX
Permissionless Hybrid consensus blockchain network

Whitepaper V1
1st, August 2023
(This paper will be updated along time)

Introduction

Institutional finance, private equity, and real estate investment firms are an integral part of the global financial ecosystem. These firms play a critical role in allocating capital to businesses and projects, enabling economic growth and job creation. However, as we enter the era of Web3, these firms face significant limitations in terms of transparency, efficiency, and privacy. Web3 promises to overcome these limitations and usher in a new era of decentralised finance and investment.

Limitations of Institutional Finance, Private Equity, and Real Estate Investment Firms in Web2

Institutional finance, private equity, and real estate investment firms operate in a centralised and opaque system, which is prone to inefficiencies, corruption, and fraud. The lack of transparency and accountability in the financial system has resulted in several crises, such as the 2008 financial crisis, which have had far-reaching consequences for the global economy. In addition, the financial system is highly intermediated, with intermediaries such as banks and brokers taking a significant cut of the profits, resulting in high fees and costs for investors.

Private equity firms, in particular, have been criticised for their lack of transparency and accountability. Private equity firms are not required to disclose their investments, performance, or fees to the public, which makes it difficult for investors to evaluate their performance. This lack of transparency has led to concerns about conflicts of interest and potential mismanagement of funds.

Real estate investment firms, on the other hand, face significant challenges in terms of efficiency and accessibility. Real estate investment is a complex and highly localised market, which makes it difficult for investors to access and evaluate opportunities. In addition, the process of buying and selling real estate involves a significant amount of paperwork and intermediaries, which increases the cost and time required to complete transactions.

Web3: The Solution to the Limitations of Web2

Web3 promises to overcome the limitations of Web2 by enabling decentralized, transparent, and secure financial systems. Web3 is based on blockchain technology, which enables the creation of decentralized networks that operate without intermediaries. Blockchain technology provides a tamper-proof and transparent ledger that can be used to record transactions and verify ownership of assets.

Decentralisation and Transparency

Decentralisation and transparency are at the core of Web3. Decentralisation enables the creation of peer-to-peer networks that operate without intermediaries, thereby reducing the cost and time required to complete transactions. In addition, decentralisation enables greater transparency and accountability, as all transactions are recorded on a public ledger that can be accessed by anyone.

This transparency enables investors to evaluate the performance of investment firms and the underlying assets they invest in. In addition, it enables investors to access investment opportunities that were previously unavailable to them, such as investments in emerging markets or niche industries.

Security and Privacy

Web3 also promises greater security and privacy for investors. Blockchain technology enables the creation of secure and tamper-proof ledgers that can be used to record sensitive information, such as consumer data and investment performance. This enables investment firms to protect consumer data and privacy while providing investors with a transparent and auditable record of their investments.

Private Blockchains for Consumer Data and Privacy Protection

Private equity and real estate investment firms are particularly interested in using private blockchains to protect consumer data and privacy. Private blockchains are permissioned blockchains that enable a group of trusted entities to maintain and verify a ledger. This enables investment firms to maintain a high level of control over their data while ensuring that it is secure and tamper-proof.

Private blockchains also enable investment firms to share data securely and efficiently with other trusted entities, such as regulators and auditors. This can help to improve transparency and accountability while maintaining the privacy of sensitive information.

Limitation and inefficiencies

Traditional finance and institutional finance have been the backbone of the global financial system for decades, but they are not without their limitations and inefficiencies. Here are some of the most common limitations and inefficiencies of traditional and institutional finance:

Centralization: Traditional finance and institutional finance are highly centralised, with a small group of intermediaries controlling the flow of capital. This centralization results in higher costs and fees for investors, as intermediaries take a significant cut of the profits.

Lack of transparency: The financial system is often opaque, making it difficult for investors to evaluate the performance of investment firms and the underlying assets they invest in. This lack of transparency has led to concerns about conflicts of interest and potential mismanagement of funds.

Complexity: The financial system is complex and difficult to navigate, especially for retail investors. The complexity of the financial system can result in confusion, delays, and errors.

Intermediation: The financial system is highly intermediated, with intermediaries such as banks, brokers, and asset managers taking a significant cut of the profits. This intermediation can result in higher fees and costs for investors.

Lack of accessibility: The financial system is often inaccessible to small investors, as the minimum investment requirements are often too high. This lack of accessibility can result in a concentration of wealth among a small group of investors.

Lack of innovation: Traditional and institutional finance have been slow to adopt new technologies and innovations, resulting in a lack of progress and a failure to meet the changing needs of investors.

Risk management: The financial system has historically been focused on risk management, which has led to a risk-averse culture that is resistant to change. This risk aversion can result in missed opportunities and a failure to adapt to changing market conditions.

Overall, traditional finance and institutional finance have significant limitations and inefficiencies that have resulted in a lack of transparency, accessibility, and innovation. These limitations and inefficiencies have created a need for new approaches to finance, such as decentralised finance and Web3, which promise to address these issues and usher in a new era of transparent, accessible, and efficient finance.

Technical: Permissionless Hybrid Private Chain with DPOS

Our permissionless hybrid private blockchain introduces a new standard of cryptography token, we call it SRC20. SRC20 has all the benefits of ERC20 with additional encryption and decryption logic that enables what is known as a Hybrid blockchain.

SRC1

- Asymmetric Encryption
- Variable data level encryption
- Multi level security groups

Problem setting

In our model, there's a couple of key factors that ultimately make a hybrid blockchain hybrid. There will always be a set of users, grouping, and data fields that we need access to. The set of users represents the contract creator, the grouping represents the tier of the group for that contract itself and the data fields represent the data we want to encrypt or decrypt by the set of group users. We call this the graph of privacy, defined below:

Definition 1 (Graph of privacy). A privacy graph, G = = (U, D, E) consists of a set of Groups U, a set of data D, as well as a set of edges E, where an edge e is a pair (i, j) for i $\in$ U and j $\in$ D denoting group i has access to data field j. We write e $\in$ G to mean that e $\in$ E.

On a broader perspective, this level of encryption enables a desirable privacy blockchain. If some groups were not given access to the data field, the user should not be able to read the data field or publicly unavailable to be seen. This graph denotes the true distribution of privacy. Each user generates his own private key and signs that particular field of changes that enables no trusted party for using that key.

Data Obfuscation

The secondary importance of having a hybrid blockchain is that the hidden data should not be able to distinguish between ciphertexts of two hash values and not match their signature. The case when the token matches a ciphertext is handled by the token obfuscation. In the following definition, documents are numbered from 0 onwards and groups of users are 1 onwards.

Data Obfuscation Challenge

The data obfuscation challenge is between a challenger Ch and an adversary Adv on security parameter κ and public parameters params

- Ch computes params ⇐ CSetup(1^k) and provides them to Adv.
- Adv provides an access graph G with users numbered from 1 and documents numbered from 0 to Ch along with keys kj for every data field with j > 0.
- Ch generates k0 ⇐ MK.KeyGen(1^κ , params) for document 0. Then, for every user i, it generates uk_i ⇐ MK.KeyGen(1^κ) and for every edge (i, j) ∈ G, it provides MK.Delta(uk_i , k_j) to Adv.
- Challenge step: Adv chooses w^*_0 , $w^*{}_1$ ← {0, 1} n(κ) and provides w ∗ 0 , w∗ 1 to Ch. Ch chooses a random bit b and provides MK.Enc(k0, w^*_b) to Adv.
- Adaptive step: Adv makes the following queries to Ch adaptively. The ℓ-th query can be:
  - "Encrypt w_ℓ to data field 0: Ch returns MK.Enc(k_o, w_ℓ)
  - "Token for word w_ℓ for user i": Ch returns MK.Token(uk_i , w_ℓ
- Adv outputs b ′, its guess for b

Restriction on Adv: for all token queries w_ℓ for user i, if (i, 0) ∈ G, it must be that wℓ ∈ { / w^*_0 , w^*_1 }. Adv wins the game if b ′ = b. Let winAdv(κ) be the random variable indicating whether Adv wins the game for security parameter κ.

Definition. A multi-key search scheme is data hiding if, for all PPT adversaries Adv, for all sufficiently large$_\kappa$, Pr[winAdv(κ)] < 1/2 + negl(κ).

Here is how this definition models work on our intentions:

- For every Adv, it can provide keys for all data fields except for the challenge one models and the fact that an adversary could steal keys of the data field, but such action wouldn't allow Adv to learn information about the data field that he does not own.
- The restriction on the token queries of Adv is required because otherwise Adv could distinguish the ciphertexts based on the functionality of the scheme.
- Note that Adv can ask tokens for words that are part of the challenge (e.g., w0 or w1) for users that do not have a delta to document 0. This ensures that any user that does not have a delta to a document cannot search that document.
- We do not need to allow Adv to ask for encrypt queries to documents i for i > 0 because Adv has the corresponding secret keys and can encrypt by itself.

Source:(Multi-key searchable encryption: https://people.csail.mit.edu/nickolai/papers/popa-multikey-eprint.pdf)

Signature Obfuscation

Signature obfuscation requires that the adversary cannot learn the definition of who signed the transaction with limited grouping rules.

A u-free data field in a particular graph is a data field with no edge from user u in that graph. A u-free user in a particular graph is a user that has edges only to u-free data fields in that graph.

User 0 will be the challenge user, for which Adv will have to distinguish tokens. Thus, we will refer to 0-free users and 0-free data field as simply “free users” and “free data field”

As before, the reason Adv can pick keys is to signify that Adv can corrupt certain users or documents, or can even create nodes in the access graph.

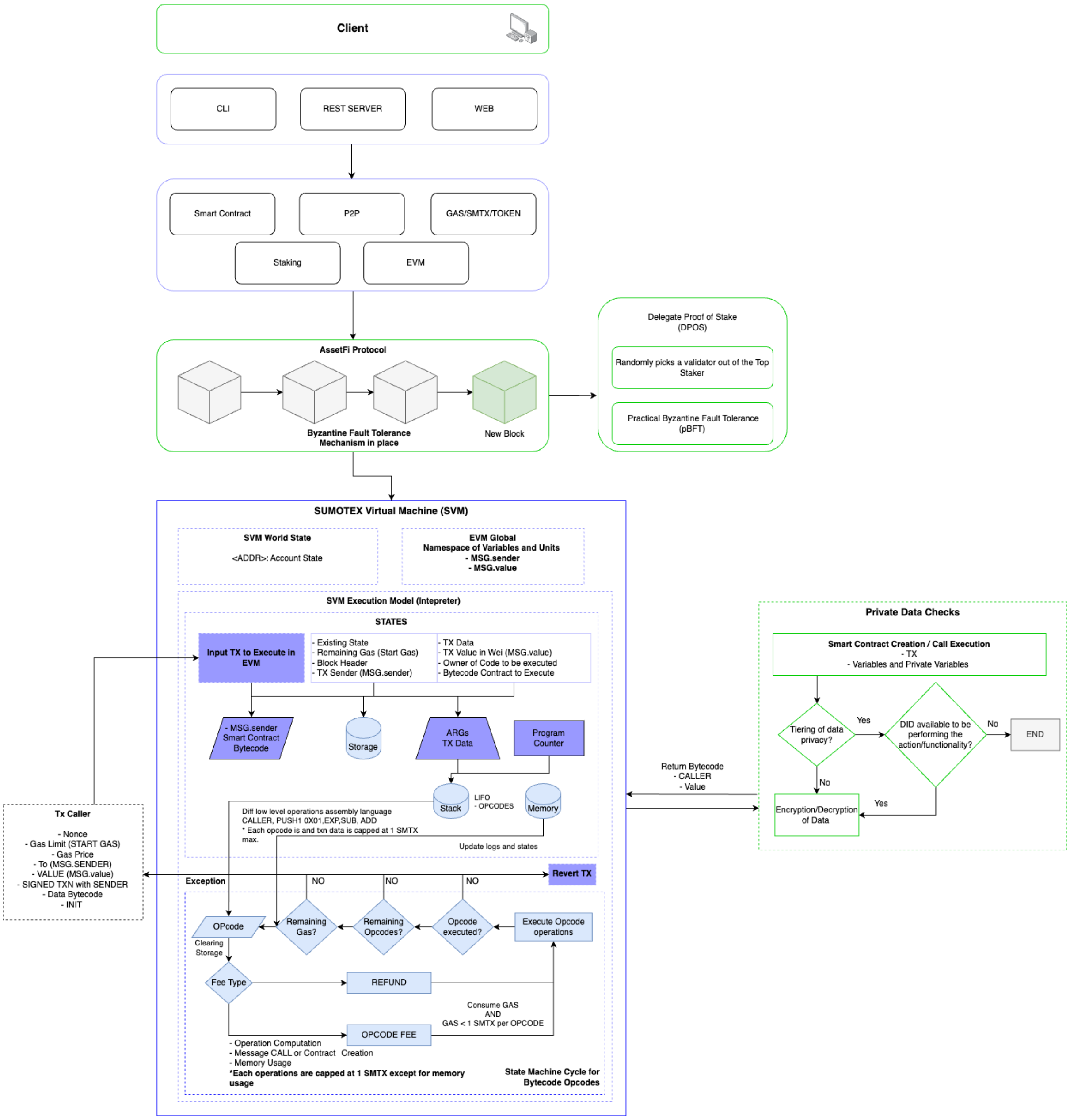
The constraints on the game are so that the adversary cannot distinguish the challenge words trivially, because the functionality of the scheme distinguishes them (either because there is a search match or the token is deterministic). Note that the definition (and in fact the scheme as well) allows an adversary to tell if two tokens are equal: in practice, if the same set of data field match a token, it is likely that the token is the same so we did not consider it important to hide this equality relation among tokens. A solution for hiding the token is to use composite groups and multiply a random element from the second group to the token, but we do not explore this further here.

To save the network from malicious transactions and double spending, the platform is equipped with Practical Byzantine Fault Tolerance (pBFT) and incorporates Master–Slave Architecture

Construction

We will utilise asymmetric pairing construction here as it is crucial for security. Through symmetric pairings, there’s an attack that can determine the search words. Given that one can distinguish by computing crossed pairings and thus do a dictionary search then a dictionary attack will happen. Asymmetric groups prohibit applying the pairing between elements.

Core Architecture Diagram


Client
CLI
REST SERVER
WEB
Smart Contract
P2P
GAS/SMTX/TOKEN
Staking
EVM
AssetFi Protocol
Byzantine Fault Tolerance Mechanism in place
New Block
Delegate Proof of Stake (DPOS)
Randomly picks a validator out of the Top Staker
Practical Byzantine Fault Tolerance (pBFT)
SUMOTEX Virtual Machine (SVM)
SVM World State
<ADDR>: Account State
EVM Global Namespace of Variables and Units
- MSG.sender
- MSG.value
SVM Execution Model (Intepreter)
STATES
Input TX to Execute in EVM
- Existing State
- Remaining Gas (Start Gas)
- Block Header
- TX Sender (MSG.sender)
- TX Data
- TX Value in Wei (MSG.value)
- Owner of Code to be executed
- Bytecode Contract to Execute
- MSG.sender Smart Contract Bytecode
Storage
ARGs TX Data
Program Counter
Stack
LIFO
- OPCODES
Memory
Diff low level operations assembly language
CALLER, PUSH1 0X01,EXP,SUB, ADD
* Each opcode is and txn data is capped at 1 SMTX max.
Update logs and states
Exception
NO
NO
NO
Revert TX
OPcode
Remaining Gas?
Remaining Opcodes?
Opcode executed?
Execute Opcode operations
Clearing Storage
Fee Type
REFUND
Consume GAS
AND
GAS < 1 SMTX per OPCODE
OPCODE FEE
- Operation Computation
- Message CALL or Contract Creation
- Memory Usage
*Each operations are capped at 1 SMTX except for memory usage
State Machine Cycle for Bytecode Opcodes
Tx Caller
- Nonce
- Gas Limit (START GAS)
- Gas Price
- To (MSG.SENDER)
- VALUE (MSG.value)
- SIGNED TXN with SENDER
- Data Bytecode
- INIT
Return Bytecode
- CALLER
- Value
Private Data Checks
Smart Contract Creation / Call Execution
- TX
- Variables and Private Variables
Tiering of data privacy?
Yes
DID available to be performing the action/functionality?
No
END
No
Yes
Encryption/Decryption of Data

Example Use Case

To create a private blockchain for their own bank.

As a bank, I want to be able to transact and create my own private contract easily while maintaining a certain level of decentralisation and transparency on data.
My requirement is that my data such as the transaction amount, address will be private while the transaction time has to be public. My secondary requirement is that the transaction will have to be visible towards a group of addresses that has been appointed as part of the organisation that launched the private contract. The address that is executing the transaction will be able to see the transaction between both parties that owns the transaction.

These transactions should be tiered and only a certain tier of users will be able to see them.

Example as below

Tier 0 - Contract Creator
Tier 1 - They are able to see all transactions in its raw format.
Tier 2 - They are able to see only which functionality was executed.
Tier 3 - They are only able to see the amount of the transactions without the functionality.

Departments

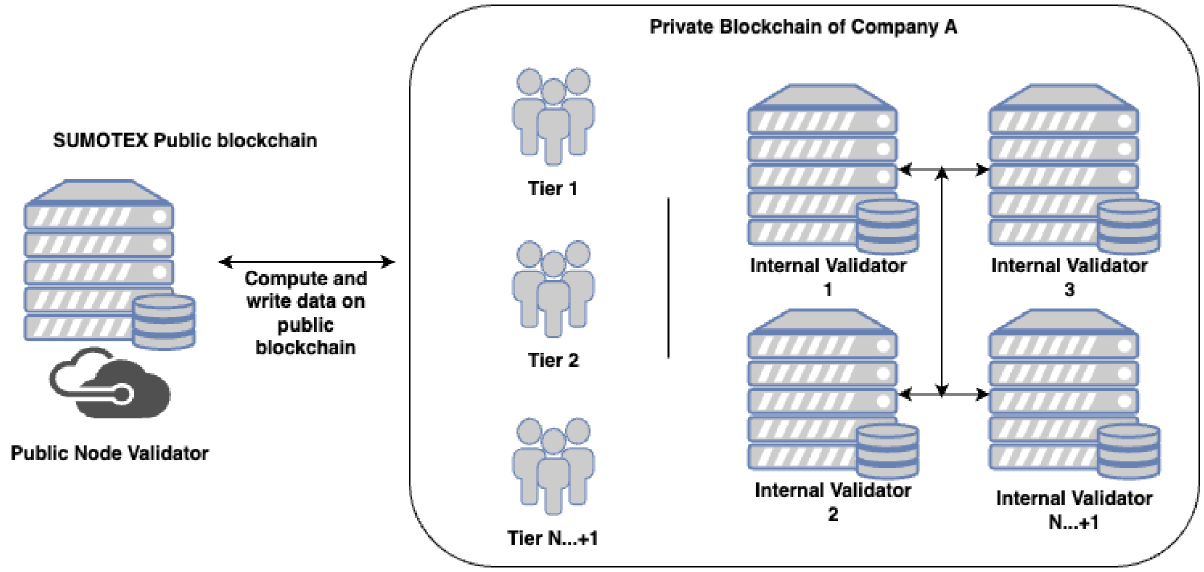
Level 1- Administrators.

Level 2 - Managers/ Head of Departments / Regulatories

Level 3 - Accountings/Administrators/Finance/Treasury

As you can see, the accessibility of data is being grouped as per above and it will then further enhance into n…n+1 where n represents number of privacy levels

Optional - Private Nodes hybrid to public node validators


SUMOTEX Public blockchain
Public Node Validator
Compute and write data on public blockchain
Private Blockchain of Company A
Tier 1
Tier 2
Tier N...+1
Internal Validator 1
Internal Validator 3
Internal Validator 2
Internal Validator N...+1

The above is for enterprises that require isolation of data and hosting on their own servers, acting as a subnet. It will be an option for users to be their own validator for proper privacy, while also maintaining proper public node governance.

Public Mainnet

The public mainnet can still benefit from the existence of private blockchains acting as subnets within its ecosystem. Here's how the public mainnet can derive advantages from the integration of private blockchains as subnets:

Scalability: Public mainnets often face scalability challenges due to the extensive computational requirements and network congestion caused by a large number of participants. By incorporating private blockchains as subnets, the burden on the mainnet can be alleviated. Private blockchains can handle a significant portion of transactions and data processing, offloading the strain on the public mainnet and improving overall scalability.

Privacy and Confidentiality: Public mainnets are inherently transparent, meaning that all transactions and data are visible to all participants. While this transparency is desirable for certain use cases, it may not be suitable for sensitive or confidential information. Private blockchains offer the advantage of enhanced privacy and confidentiality by restricting access to authorised participants. This enables the storage and management of confidential data without compromising the transparency and security of the public mainnet.

Performance and Speed: Public mainnets often experience network congestion and slower transaction processing times due to the decentralized and distributed nature of their networks. By incorporating private blockchains as subnets, transactions within the private network can be executed with higher performance and speed. This is particularly beneficial for enterprises and retail users who require faster transaction confirmation times or real-time processing capabilities.

Customization and Governance: Public mainnets typically operate under predefined consensus mechanisms and governance models. Private blockchains, on the other hand, can be customized to meet specific enterprise or industry requirements. By integrating private blockchains as subnets, organizations gain greater flexibility to tailor the blockchain infrastructure to their specific needs, such as adjusting consensus algorithms, access controls, or transaction rules. This enables enterprises to maintain a level of autonomy and control within their private blockchain subnets while benefiting from the security and decentralization of the public mainnet.

Interoperability and Cross-Chain Communication: Private blockchains acting as subnets can facilitate interoperability and cross-chain communication within the broader public mainnet ecosystem. By establishing bridges or interoperability protocols, private blockchains can seamlessly exchange data, assets, or tokens with the public mainnet. This enables enterprises and retail users to leverage the benefits of both private and public blockchains, expanding the scope of their applications and interactions within the larger blockchain network.

In summary, the public mainnet can derive several benefits from incorporating private blockchains as subnets within its ecosystem, including improved scalability, enhanced privacy and confidentiality, faster transaction processing, customization and governance flexibility, and interoperability with other chains. This integration allows for a more robust and versatile blockchain infrastructure, catering to a wide range of enterprise and retail use cases while leveraging the security and decentralization of the public mainnet.

Private blockchain: Use case

Supply Chain Management: Enterprises can leverage the prowess of a private blockchain network to establish an immutable and distributed ledger, ensuring traceability and verifiability of goods within the supply chain. Through the deployment of smart contracts, self-executing protocols can be enforced, enabling transparent and auditable transactions. Retail users gain access to this blockchain, harnessing the power of cryptographic hashes and consensus mechanisms to seamlessly verify the provenance and integrity of products, utilizing the decentralized and tamper-resistant records stored on the blockchain.

Enterprises involved in supply chain management can utilize private blockchains as subnets to enhance the transparency and security of their operations. They can track and verify the movement of goods, share relevant data with authorized participants, and ensure the integrity of their supply chain while leveraging the scalability and interoperability of the public blockchain.

Financial Transactions: By implementing a private blockchain network, enterprises can revolutionize their financial landscape, creating a secure and efficient infrastructure for transactional activities. This decentralized ledger acts as an incorruptible repository, leveraging consensus algorithms and cryptographic principles to validate and record financial transactions. The introduction of smart contracts enables the automation of processes such as payment settlements, loan approvals, and trade settlements, providing unparalleled speed, cost-efficiency, and immutability. Retail users benefit from swift and cost-effective cross-border payments, streamlined remittances, and heightened security, thanks to cryptographic keys and decentralized consensus mechanisms.

Banks and other financial institutions can incorporate private blockchains as subnets to improve the efficiency and speed of transactions. They can create private networks for interbank transfers, remittances, and settlements, allowing for faster and more secure transactions while still benefiting from the public blockchain's interoperability and decentralized nature.

Identity Management: Private blockchains present an ideal solution for robust identity management, empowering enterprises to establish a distributed and verifiable repository for digital identities. Through the use of cryptographic signatures, public-private key pairs, and decentralized storage, enterprises can ensure the integrity and privacy of user credentials. Retail users can benefit from self-sovereign identities, leveraging cryptographic proofs and zero-knowledge protocols to maintain control over their personal data, granting selective access and verifiability to online services that rely on identity verification.

Healthcare providers can utilize private blockchains as subnets to securely store and manage patient health records. By integrating with the public blockchain, they can ensure data integrity, control access to sensitive information, and streamline interoperability between different healthcare providers while adhering to privacy regulations.

.

Intellectual Property Protection: The implementation of private blockchains revolutionizes intellectual property rights management, leveraging cryptographic hashes, timestamps, and decentralized consensus. Enterprises can establish an immutable and tamper-proof ledger for recording copyright registrations, patents, and trademarks. By utilizing the blockchain's transparency and consensus mechanisms, enterprises can secure the proof-of-existence and ownership of intellectual property assets. Retail users can rely on blockchain-based platforms to assert and protect their creations, utilizing cryptographic proofs and decentralized storage to establish the irrefutable ownership and authenticity of their intellectual property.

Companies dealing with intellectual property rights and legal firms can leverage private blockchains as subnets to create a decentralized registry for tracking and managing patents, copyrights, and trademarks. By integrating with the public blockchain, they can enhance the transparency, authentication, and traceability of intellectual property while protecting confidential details.

Energy Sector: Energy companies can employ private blockchains as subnets to enable peer-to-peer energy trading, metering, and billing. They can create a secure and transparent environment for participants to exchange energy resources, monitor consumption, and settle transactions, benefiting from the scalability and customization options of private blockchains within the public blockchain ecosystem.

Real Estate Transactions: Private blockchains bring radical transformation to real estate transactions, providing a transparent and auditable registry of property ownership, transfers, and contracts. Enterprises can establish a decentralized network, employing consensus algorithms and cryptographic hashes to ensure the integrity and immutability of property records. Smart contracts automate processes like property transfers, escrow arrangements, and title registrations, leveraging blockchain's capabilities to streamline and expedite transactional workflows. Retail users benefit from secure and expedited property transactions, reduced reliance on intermediaries, and increased confidence in the integrity of property records.

Healthcare Data Management: Private blockchains revolutionize healthcare data management, ensuring privacy, security, and interoperability. Enterprises can establish a private blockchain network where sensitive medical records are securely stored and shared, utilizing cryptographic encryption and decentralized access controls. Consensus algorithms and blockchain-based interoperability protocols enable seamless data exchange between healthcare providers, insurance companies, and patients, while maintaining data integrity and patient consent management. Retail users gain control over their health data, leveraging cryptographic keys and decentralized storage to selectively grant access to healthcare providers, researchers, or wearable devices, ensuring privacy and data sovereignty.

Voting Systems: Private blockchains serve as the foundation for secure and transparent voting systems, enhancing the integrity and inclusivity of democratic processes. Enterprises can build a private blockchain network, utilizing cryptographic signatures, decentralized consensus, and transparent ballot records to ensure the tamper-proof recording and counting of votes. Smart contracts enforce predefined voting rules, enabling automated and verifiable elections. Retail users partake in a decentralized voting experience, leveraging cryptographic proofs and consensus algorithms to verify the integrity and transparency of the voting process, reinvigorating trust and confidence in democratic governance.

Retail and E-commerce: Retailers and e-commerce platforms can integrate private blockchains as subnets to enhance supply chain traceability, combat counterfeiting, and improve customer trust. By securely recording product information, transaction details, and shipment data, they can provide transparent and authenticated product histories while leveraging the public blockchain's interoperability for cross-border transactions.

These blockchain-infused use cases showcase the extraordinary potential of private blockchains, employing cryptographic principles, decentralized storage, and consensus algorithms to redefine transparency, security, and efficiency across diverse sectors, empowering both enterprises and retail users to unlock unprecedented opportunities and seamless experiences.

Conclusion:

In the realm of blockchain technology, the convergence of public and private blockchains as a unified ecosystem represents a seismic shift towards a future of boundless possibilities. Our vision encompasses a world where the limitations that have hindered the full potential of blockchain are shattered, replaced by an amalgamation that transcends the boundaries of scalability, privacy, performance, customization, and interoperability. Through the integration of private blockchains as subnets within public blockchain frameworks, we are on the cusp of revolutionizing industries across the spectrum. From supply chain management and financial institutions to healthcare, intellectual property, energy, retail, and beyond, our vision is to empower enterprises with a blockchain infrastructure that redefines what is achievable.

Picture a supply chain where transparency and security reign supreme, eradicating fraud and inefficiencies. Imagine a financial landscape where transactions occur with lightning-fast speed, empowering businesses and individuals to thrive in a digital economy. Envision a healthcare system where patient data is safeguarded with utmost privacy and seamlessly shared for enhanced treatment outcomes. Envisage an intellectual property ecosystem where innovation flourishes, protected by an unyielding shield of authenticity. Envision an energy sector where peer-to-peer trading fosters sustainable practices and equitable distribution.

Our vision extends further still, embracing retail and e-commerce landscapes that flourish on the bedrock of trust, enabling consumers to make informed choices with unwavering confidence. These are just glimpses of the boundless potential that emerges from the fusion of public and private blockchains, where limitations dissolve, and unprecedented opportunities arise.

Together, we are forging a path towards a future where the decentralized and transparent nature of public blockchains intertwines seamlessly with the privacy, customization, and performance of private blockchains. This is a future where enterprises can thrive, innovation can flourish, and individuals can experience a new level of empowerment.

The future of blockchain—welcome to limitless possibilities with Sumotex.