WST Token White Paper

Table of Contents

1. Introductory 1

1.1 Project Description 1

1.2 Development Background 1

1.3 WST's Core Mission 2

2. Privacy Challenges in the Payment Process 3

2.1 Privacy in Traditional Payment Systems 3

2.2 Privacy Issues in Blockchain Payment Systems 3

2.3 Growing Demand for Privacy Protection 3

2.4 Risk of user privacy disclosure 4

2.5 WST Privacy Solution 4

3. WST's core protocol mechanism 5

3.1 Agreements Overview 5

3.2 Encryption Technology Assurance 5

3.3 Privacy protection mechanism 5

3.4 Trade Validation Mechanism 6

3.5 Efficient and scalable payment process 6

3.6 Decentralized Operations 7

4. User identity protection and anonymous transaction process 8

4.1 The Need for User Identity Protection 8

4.2 Decentralized management of user identities 8

4.3 Anonymous transaction flow design 9

4.4 Protection of Privacy in the Transaction Process 9

4.5 The Law and Compliance of Privacy Protection 10

4.6 Privacy protection of the user experience 10

5. Zero-knowledge proofs and mixed-currency mechanisms 11

5.1 Zero Knowledge Proofing Technology Overview 11

5.2 Application Scenarios for Proof of Zero Knowledge 11

5.3 Principles and Operation of the Mixed Currency Mechanism 11

5.4 Synergy between zero-knowledge proofs and mixed-currency mechanisms 12

5.5 Challenges and solutions in practical applications 13

6. Cross-Chain Payments and Privacy Integration 13

6.1 Demand and Challenges of Cross-Chain Payments 13

6.2 WST's Cross-Chain Payment Solution 14

6.3 Practical Realization of Cross-Chain Privacy Protection 15
7. WST Token Roles and Economic Modeling 15
7.1 WST Token's central role in the agreement: 15
7.2 Token Aggregate and Distribution Modeling: 16
8. Application Scenarios 17
8.1 Private Donation 17
8.2 Payroll Confidentiality 18
8.3 Cross-border Payments 18
8.4 Future Scenario Expansion 19
9. Security audits and anti-fraud mechanisms 19
9.1 Security Audit 20
9.2 Anti-fraud mechanism 20
10. Community Governance and Agreed Upgrade Mechanism 21
10.1 decentralized governance 21
10.2 Agreement Upgrade Mechanism 21
Appendix: Disclaimer 22

1. Introductory

1.1 Project Description

WST is a kind of on-chain payment protocol token designed to protect the privacy of user transactions. With the rapid development of digital payments and the widespread application of blockchain technology, privacy issues have gradually become a major challenge for users and enterprises when making payments and transactions.WST is designed to fill the privacy loopholes in the existing payment system, and to realize an anonymous, decentralized, and seamless payment experience by means of advanced encryption technology and innovative protocol mechanisms.

WST's core objective is to provide an efficient, secure and reliable payment solution for users who need to protect the privacy of their transactions. Whether it's for everyday transactions or highly sensitive financial activities, WST provides strong privacy protection, thus enhancing users' trust in digital payment systems.

1.2 Development Background

With the increasing maturity of blockchain technology, more and more enterprises and users are turning to blockchain payment systems. However, most existing blockchain payment systems have shortcomings in privacy protection. Traditional blockchain systems, such as Bitcoin and Ether, provide public transaction records and high transparency, but this also makes every transaction easy to track and analyze, which in turn poses a threat to user privacy.

The lack of privacy protection in existing payment protocols, especially the risks associated with highly sensitive transactions (e.g., payroll, private finance, etc.), has led to concerns about security and privacy, and WST was created to address these issues, not only by solving the existing payment system's disregard for privacy, but also by improving the efficiency and security of the overall payment system, thus revolutionizing the digital payment space. It not only addresses the privacy concerns of existing payment systems, but also strives to improve the efficiency and security of the overall payment system, thus revolutionizing the digital payment field.

1.3 WST's Core Mission

WST's mission is to build a decentralized payment system that focuses on user privacy and applies privacy-protecting technologies (e.g., zero-knowledge certificates, mixed-currency mechanisms, etc.) to everyday transactions and enterprise-level payments. We aim to achieve this goal through the following means:

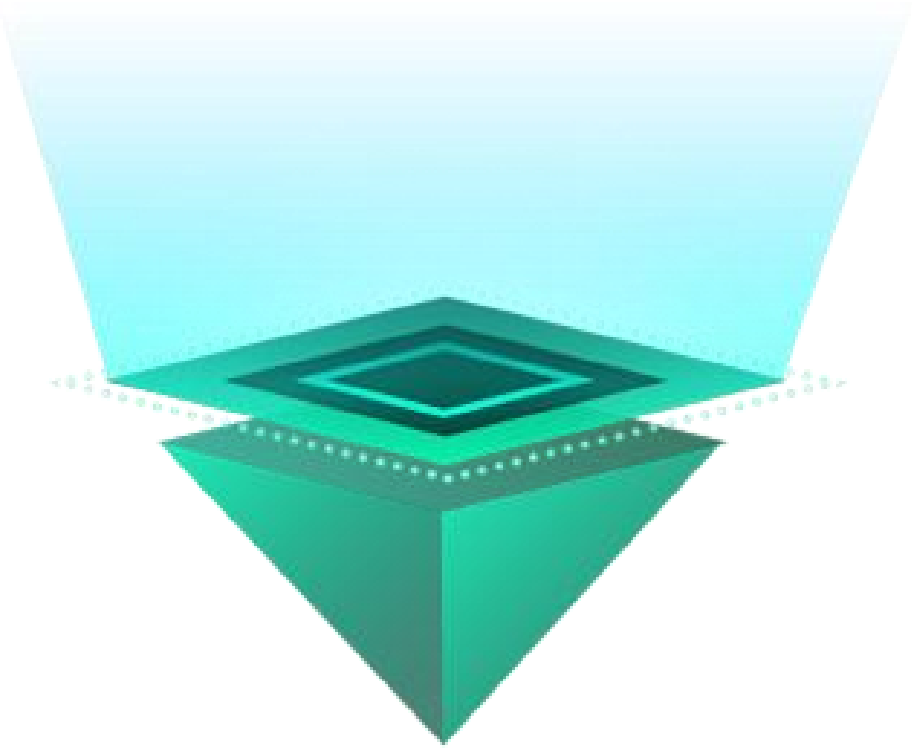
Encryption Technology: Provides strong encryption protection to ensure the privacy of all transaction data and prevent any sensitive information from being leaked during the transaction process.

Identity isolation: Decentralized technology ensures that the privacy of the user's identity is not exposed, so that even the platform operator cannot know the user's specific identity information.

Cross-chain interoperability: Supports cross-chain payments between different blockchains and maintains privacy in the process.

Anonymous transactions: Utilizing technologies such as mixed-currency mechanisms and zero-knowledge proofs, completely anonymous transaction flows are realized, preventing transaction tracking.

The birth of WST marks the beginning of a new stage in the application of privacy protection tokens in the field of digital payment, and provides users with a more secure payment option. In the future, WST will not only be a payment tool, but will become an indispensable privacy protection solution in users' daily life.



2. Privacy Challenges in the Payment Process

2.1 Privacy in Traditional Payment Systems

With the global popularization of digital payments, traditional payment systems have gradually replaced cash payments and become the foundation of modern economic operations. While these payment systems (e.g., credit cards, debit cards, and e-payment platforms) have played an important role in enhancing the convenience of payment and accelerating the flow of transactions, they still face many challenges in terms of user privacy protection.

In traditional payment systems, user transaction data is usually stored and processed by a centralized organization (e.g., a bank or payment platform). These data include sensitive information such as user's identity, purchase history, payment amount, timestamps, etc., which can reveal user's behavioral patterns and economic status and may be used for data analysis, behavioral tracking, or misuse. In addition, data storage and management in these systems are often centralized, which increases the risk of hacking and data leakage.

2.2 Privacy Issues in Blockchain Payment Systems

With the rise of blockchain technology, many digital payment systems have shifted to a decentralized model so that users can make peer-to-peer payments directly without relying on a centralized organization. However, despite the decentralized and tamper-proof nature that blockchain technology offers, it still has some issues with privacy protection.

In the case of Bitcoin and Ether, for example, while these blockchains guarantee transparency and decentralization of transactions, all transaction records are public and accessible. Each transaction is permanently recorded on the blockchain and is associated with the addresses of the sender and receiver. Although these addresses do not themselves contain specific personal information, as transactions accumulate, they can be identified and associated, leading to the exposure of a user's identity. This may pose a threat to user privacy in certain circumstances.

2.3 Growing Demand for Privacy Protection

With the increasing global demand for privacy protection, users' need for transactional privacy is gradually increasing. Data privacy policies of governments and enterprises are also becoming more stringent, such as the EU's GDPR (General

Data Protection Regulation) and California's CCPA (California Consumer Privacy Act), etc. These laws and regulations require enterprises to provide more privacy protection when handling user data.

Against this backdrop, traditional payment systems and existing blockchain systems are unable to meet the growing demand for privacy. Therefore, in order to adapt to these changes, it is particularly important to create a payment protocol that protects privacy while maintaining transaction transparency and efficiency.

2.4 Risk of user privacy disclosure

The risk of privacy breaches comes not only from the payment system itself, but also from the intervention of external attackers. For example, when data in a payment system is not encrypted or stored on a centralized server, it becomes an easy target for hackers. If this data is stolen or compromised, it can lead to identity theft, financial loss and even greater social security risks.

In addition, data tracking during the payment process brings new privacy challenges. For example, some platforms may use a user's transaction history to analyze his or her spending behavior and sell that information to third-party advertisers or engage in other unethical data exploitation. These practices not only violate users' privacy, but also reduce trust in digital payment systems.

2.5 WST Privacy Solution

In the face of these privacy challenges, the WST Agreement will address them in the following ways:

Anonymous Transactions: Utilizes advanced cryptography and mixed-currency mechanisms to ensure that the sender and receiver of each transaction cannot be traced, even on the public blockchain.

Proof of Zero Knowledge: Introducing Proof of Zero Knowledge technology allows users to prove their ownership of certain information or assets without having to disclose the specifics of the transaction or the amount of the transaction, thus further enhancing privacy protection.

Decentralized Identity Authentication: Through the decentralized identity authentication mechanism, it avoids centralized storage of user's identity information and reduces the risk of identity theft.

These technological innovations of WST will effectively fill the privacy gap in the existing payment system and provide users with a higher level of privacy protection.

3. WST's core protocol mechanism

3.1 Agreements Overview

WST (Privacy Protection Asset Protocol) aims to solve the privacy problem in the existing payment system and provide a secure and privacy-protected payment solution through advanced blockchain technology. Its core protocol mechanism combines the key elements of privacy protection, transaction authentication, decentralized operation and cross-chain interoperability to create an efficient and tamper-proof payment platform.

The design of the WST protocol follows a simple yet powerful principle: **to protect user privacy while ensuring the transparency and efficiency of the payment process**. The protocol's operating mechanism is based on encryption technology, and combines innovative technologies such as zero-knowledge proof and mixed-currency mechanisms to realize a comprehensive privacy protection solution.

3.2 Encryption Technology Assurance

In the WST protocol, all transactions are encrypted and recorded on the blockchain. The protocol uses advanced cryptographic algorithms such as **Elliptic Curve Cryptography (ECC) and Symmetric Cryptography** to ensure that the transaction data cannot be snooped by unauthorized third parties.

Transaction Encryption: All transaction content (including amount, sender, receiver, etc.) is encrypted and only authorized receivers can decrypt and obtain transaction details.

Encrypted Data Transmission: During the transaction process, all data will be encrypted and transmitted to prevent data from being stolen or tampered with during the transmission process.

Such an encryption mechanism ensures privacy and security during the transaction process, effectively preventing external data theft or analysis.

3.3 Privacy protection mechanism

The WST protocol's privacy protection mechanism is based on **Zero-Knowledge Proof (ZKP) and a mixed-currency mechanism**, two technologies that take privacy protection during transactions to a whole new level.

Proof of Zero Knowledge: Proof of Zero Knowledge technology allows a user to prove the truth of a fact to another party without revealing the specifics of the

transaction. This means that when a user conducts a transaction, he or she can prove the validity of the transaction without revealing any sensitive information, such as the amount of money or identity. For example, when making a payment, the user does not have to disclose the amount or identity of the payment, but simply provide sufficient evidence of the ability or legitimacy of the payment.

This technology is critical to improving transaction privacy, especially in protecting user identity and monetary information.

Coin Mixing: WST introduces coin mixing to further enhance the privacy of transactions. During the coin-mixing process, a user's payment funds are mixed with other users' funds, making each transaction difficult to track or identify. This mechanism prevents third parties from analyzing transaction records on the blockchain to track a user's payment behavior, thus effectively protecting the user's anonymity.

3.4 Trade Validation Mechanism

To ensure the legitimacy of transactions and prevent malicious behavior, WST Protocol uses an advanced transaction validation mechanism. In each transaction, WST Protocol performs the following steps of validation:

Transaction Signature: Each transaction needs to be signed by the sender using a private key to verify the legitimacy of the transaction. This signature process not only ensures that the transaction was initiated by the actual sender, but also that the content of the transaction has not been tampered with during transmission.

Smart Contract Validation: All transactions are validated by smart contracts that determine whether a transaction is compliant based on predefined conditions. For example, smart contracts will check that the user has sufficient funds or that the conditions of the transaction have been met.

This transaction verification mechanism not only protects the legitimacy of payments, but also effectively prevents double payments, fraudulent behavior and system errors.

3.5 Efficient and scalable payment process

The design of the WST protocol takes into account the scalability of the blockchain and ensures that the protocol can cope with large-scale transaction processing.WST uses an advanced hierarchical structure that divides the different operations of the blockchain to improve the overall processing efficiency:

Blockchain Layered Processing: The WST protocol divides transactions into different layers for processing, which can effectively reduce the burden of transactions on the blockchain and increase the processing speed of the system.

Transaction Batch Processing: To enhance transaction speed, WST supports combining multiple transactions into one batch for processing, which reduces transaction confirmation time and increases system throughput.

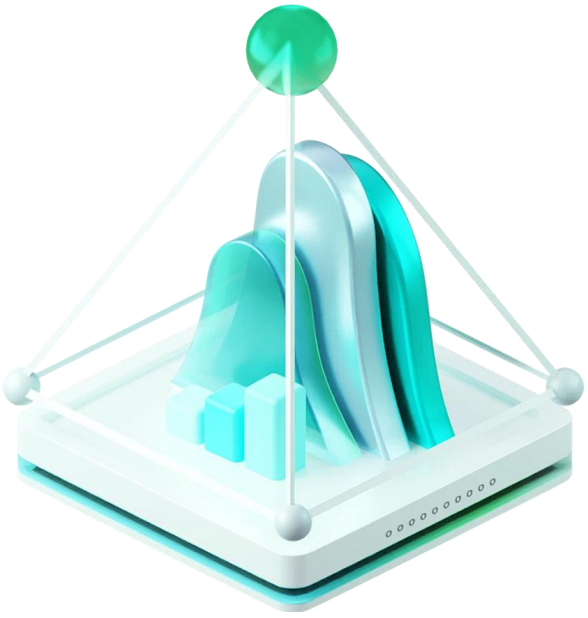
This efficient design not only supports the simultaneous operation of a large number of users, but also ensures that the system remains stable even under high transaction volumes.

3.6 Decentralized Operations

The WST protocol adopts a decentralized architecture to avoid the risk of a single control point. WST realizes a decentralized payment mechanism through the collaborative operation of multiple nodes in a distributed network. Under such a structure, neither the payment process nor the transaction verification relies on a single organization or a hub server, thus effectively reducing the security risks associated with a centralized system.

Decentralized nodes: Each node plays the role of a verifier in the network and works together to maintain the blockchain record. These nodes work in concert through consensus algorithms to ensure the transparency and security of transactions.

No intermediary operation: WST agreement does not rely on any third-party intermediary organization, which can effectively reduce the cost and delay caused by intermediary operation and allow users to enjoy higher transaction efficiency.



4. User identity protection and anonymous transaction process

4.1 The Need for User Identity Protection

In the current digital payment environment, a user's identity information is often exposed during transactions, which poses a great risk to the user's privacy and security. Especially in sensitive scenarios such as cross-border payments, privacy donations, and payroll payments, leakage of identity information can lead to identity theft, financial fraud, and commercial espionage. Therefore, protecting users' identity information and ensuring anonymity in the transaction process are key requirements for digital payment systems.

The WST protocol takes this need into account and makes user identity protection one of its core design principles. Through innovative privacy protection technology, WST is able to effectively segregate users' personal information and ensure the anonymity of transactions.

4.2 Decentralized management of user identities

The WST protocol uses a decentralized authentication mechanism to protect user identity information. Unlike traditional centralized authentication methods, WST avoids storing sensitive user information centrally in a single server, thus reducing the risk of data leakage.

Decentralized Identity (DID): WST adopts Decentralized Identity (DID) technology, which means that each user has an independent and secure identity in the WST ecosystem without relying on any centralized identity verification authority. The user's identity information is not stored in a centralized server, but distributed across multiple blockchain nodes, so that even if some nodes are attacked, the user's identity cannot be easily cracked.

Private key control: The subscriber controls his identity and transaction operations through the private key to ensure that only the person who owns the private key can carry out the corresponding operations. This private key control ensures that the subscriber has full control over his identity and prevents identity theft or tampering.

4.3 Anonymous transaction flow design

One of the core goals of the WST protocol is to achieve a **completely anonymous** transaction process, i.e., users make payments without their identity and transaction details being traceable or revealed by third parties. This goal is achieved through the following technologies and processes:

Anonymous Payment Address: In WST, the user's payment address is not directly related to the real identity. Users can generate one or more anonymous payment addresses and use a different address for each transaction, which avoids the binding of the transaction address to the user's identity.

Transaction obfuscation technology: WST uses a coin-mixing mechanism to further enhance the anonymity of transactions. When a transaction occurs, the funds sent are mixed with funds from other users, so that even the transaction history on the blockchain cannot directly associate the transaction with a particular user. The mixing process makes each transaction untraceable and ensures the anonymity of the funds.

Zero Knowledge Proof (ZKP): In WST, ZKP technology allows users to prove the legitimacy of their payment behavior without revealing specific transaction information. Users do not need to disclose the transaction amount, source or recipient information, but only need to provide sufficient evidence to prove that the transaction is legitimate. In this way, even if the transaction takes place on a public blockchain, the user's sensitive information will not be exposed.

4.4 Protection of Privacy in the Transaction Process

The WST transaction process is designed to emphasize privacy protection. The following is the specific procedure for protecting privacy during the WST transaction process:

Transaction initiation: When a user chooses to initiate a transaction, an anonymous payment address is first generated and the amount of the payment is selected. This process is done without revealing the user's real identity or payment details.

Transaction Encryption and Coin Mixing: Transaction information is encrypted and funds sent are mixed with other users' funds through a coin mixing mechanism. This makes it impossible to identify the exact source or purpose of the funds, even if the transaction history is queried.

Zero-knowledge authentication: During the transaction process, zero-knowledge proof technology verifies the legitimacy of the transaction and

ensures that the contents of the transaction are not compromised. Even the authentication node on the blockchain has no way of knowing the exact amount of the transaction or the identities of the sender and receiver.

Transaction Settlement: After a successful transaction, funds will be settled according to the blockchain consensus mechanism and transaction records will be generated on the blockchain. These records will not contain any sensitive information and will maintain the transparency and verifiability of the transaction process.

4.5 The Law and Compliance of Privacy Protection

The WST protocol is designed with full consideration of the requirements of privacy protection laws and regulations in different countries and regions. In some privacy-sensitive areas, the design of WST ensures compliance with global privacy protection regulations such as **GDPR** (European Union General Data Protection Regulation), **CCPA** (California Consumer Privacy Act), etc. Decentralized authentication and zero-knowledge proof technology in WST not only ensures the privacy rights of the users, but also realizes an efficient transaction process under the compliance framework.

4.6 Privacy protection of the user experience

The privacy-protecting design of the WST protocol not only safeguards users' data, but also ensures a smooth user experience. by streamlining the authentication and payment process, WST allows users to easily complete anonymous payments without being bothered by complicated operations or additional privacy protection measures.

When making a transaction, users only need to focus on the payment amount and recipient information, and other privacy protection processes will be carried out automatically, so that users do not need to worry about the disclosure of their sensitive information.

5. Zero-knowledge proofs and mixed-currency mechanisms

5.1 Zero Knowledge Proofing Technology Overview

Zero-Knowledge Proof (ZKP) is a cryptographic technique that allows one party (the prover) to prove a statement to another party (the verifier) to be true without revealing any specific information about the statement. In other words, the verifier can prove that he or she knows certain information or fulfills certain conditions without revealing the specifics of that information or condition in the process. This technology has great potential for privacy protection, especially in the area of blockchain and digital payments.

In the WST protocol, zero-knowledge proofs are widely used in transaction verification to ensure the legitimacy and validity of the transaction, while hiding the specific details of the transaction to further protect the user's privacy. This application allows the user's identity and transaction amount to be hidden, and only shows whether the transaction is legal or not.

5.2 Application Scenarios for Proof of Zero Knowledge

In WST, zero-knowledge proofs are mainly used in the following scenarios:

Transaction Validation: When a user initiates a transaction, the WST protocol proves the legitimacy of the transaction through zero-knowledge proof. For example, it proves that the sender has sufficient funds to complete the transaction without revealing their account balance or the exact amount of the transaction.

Authentication and Privacy Protection: WST uses zero-knowledge proofs to realize user authentication. Users can prove that they are the owner of a certain identity without the need to provide actual identity documents. This approach effectively protects user privacy and avoids the exposure of sensitive information.

Anonymity and Compliance: WST maintains the anonymity of its users while needing to comply with laws and regulations. With zero-knowledge proof, transactions can achieve regulatory compliance without revealing the user's specific identity or amount of money.

5.3 Principles and Operation of the Mixed Currency Mechanism

A mixed-currency mechanism is a technique that mixes transactions from multiple users in order to make the source and purpose of the transaction untraceable. In this way, even if a transaction leaves a trace on the public blockchain, it is impossible to determine which funds belong to which specific user. Mixed-currency technology effectively protects user privacy and prevents the flow of funds from being tracked or snooped.

The operation of the mixed-currency mechanism in the WST protocol is divided into the following steps:

Pooling: Funds from multiple users are pooled into a common address, creating a mixed pool. Each fund is randomly reallocated and its amount, source and recipient information is hidden, making each transaction less traceable.

Hybridization: The system performs hybridization of funds pooled in a hybrid pool, where the sources and destinations of these funds are mixed, encrypted and redistributed. In this way, transaction records queried from the blockchain no longer correspond to specific user identities or transaction details.

Random Allocation: Funds will be randomly allocated to different user addresses after the mixing is completed in the mixing pool, and these new addresses are also not associated with the user's real identity.

Transaction Completion: Funds after mixing coins are transferred as specified by the user and the transaction is recorded in the blockchain. In the end, the transaction maintains its legality and transparency, but the true source and flow of funds is completely hidden.

5.4 Synergy between zero-knowledge proofs and mixed-currency mechanisms

Zero-knowledge proof and mixed-currency mechanism complement each other in the WST protocol, and the combination of the two makes WST realize efficient privacy protection. In WST, Zero Knowledge Proof is responsible for ensuring the legality and compliance of each transaction, while Mixed Currency guarantees the anonymity of the transaction by hiding the transaction funds.

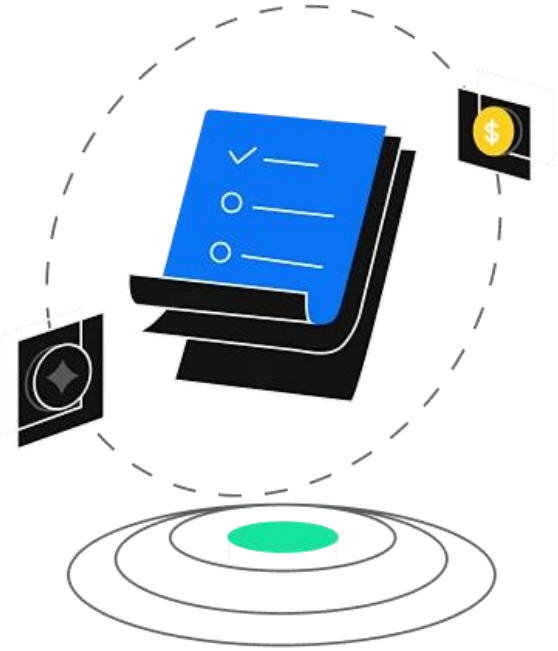
Enhanced anonymity: The specific source and recipient of a transaction are effectively hidden through the mixed-currency mechanism, while zero-knowledge proof of authenticity and legitimacy ensures that the transparency requirements of blockchain are met while maintaining privacy.

Guaranteeing the legitimacy of transactions: Even if the amount and identity of the transaction are hidden, zero-knowledge proof technology can guarantee that the

transaction will not violate the rules of the agreement, which is critical to preventing illegal activities such as money laundering.

5.5 Challenges and solutions in practical applications

Despite the obvious advantages of zero-knowledge certificates and mixed-currency mechanisms in terms of privacy protection, they still face some challenges in practical application. For example, how to balance privacy protection and transaction efficiency, and how to realize compatibility with regulatory compliance. In order to solve these problems, WST adopts an efficient encryption algorithm and consensus mechanism to ensure that privacy protection will not have too great an impact on the transaction speed, and realize compatibility with regulatory norms through innovative technical means.



6. Cross-Chain Payments and Privacy Integration

6.1 Demand and Challenges of Cross-Chain Payments

With the rapid development of blockchain technology, more and more blockchain platforms and cryptocurrencies are being created, which makes

cross-chain payments a demand that cannot be ignored. Users want to be able to transfer funds between different blockchains without being restricted by a single blockchain. However, cross-chain payments face several challenges, especially in terms of privacy and security.

Traditional blockchain payment systems are generally limited to transactions within the same blockchain and cannot easily realize the flow of funds between different blockchains. Although some interoperability solutions (e.g., cross-chain bridges, atomic swaps, etc.) have emerged, these solutions usually have certain privacy risks and security vulnerabilities, especially when funds are exposed to the public blockchain during cross-chain transactions, the user's privacy may be compromised.

Therefore, how to realize safe, fast and efficient cross-chain payment under the premise of protecting user privacy has become an urgent problem in the blockchain payment system.

6.2 WST's Cross-Chain Payment Solution

WST protocol adopts advanced cross-chain technology to support seamless payment between different blockchain platforms, and provides an efficient and transparent cross-chain payment process while protecting user privacy.WST's cross-chain payment solution is mainly realized through the following technologies:

Cross-Chain Bridges: The WST protocol utilizes cross-chain bridges to exchange assets between different blockchains. Cross-Chain Bridges enable the movement of assets between different blockchains and maintain the privacy of the assets during the transaction process.WST's Cross-Chain Bridges use cryptography to lock funds on one blockchain and generate corresponding tokens on another blockchain, ensuring the security and privacy of the funds.

Atomic Swaps: The WST protocol also supports Atomic Swaps, which are cross-chain transactions that do not require a trusted third party. Atomic swaps ensure that transactions on two different blockchains are either fully completed or do not occur at all, thus avoiding risk for either party. In WST, these swaps use cryptography to hide the specific details of the transaction, ensuring anonymity and security.

Privacy-protected cross-chain protocols: WST's cross-chain payment privacy protection measures include encryption and anonymization of all data in cross-chain transactions using Zero-Knowledge Proof (ZKP) and mixed-currency mechanisms. In this way, the amount, source, destination, and associated user identifiers of a

transaction remain private from surveillance and tracking, even when the money flows across different blockchains.

6.3 Practical Realization of Cross-Chain Privacy Protection

In WST, the privacy protection design for cross-chain payments incorporates various advanced technologies to ensure that users' privacy will not be compromised when making payments across different blockchains. Specifically, WST realizes cross-chain payment privacy protection in the following ways:

Zero-knowledge proof in cross-chain payments: Zero-knowledge proof technology is not only used in single-chain transactions, but also plays a key role in cross-chain payments. In cross-chain transactions, Proof of Zero Knowledge can prove that a transaction is legitimate without revealing the exact amount, source or recipient of the transaction. This ensures privacy regardless of the blockchain from which the funds originate.

Cross-chain application of mixed-currency mechanism: WST's mixed-currency mechanism is also applied to cross-chain payments. By mixing the funds in a transaction with the funds of other users, WST can effectively hide the specific source and destination of the funds, and even in cross-chain transactions, the path of the funds cannot be traced and analyzed. In this way, even when transactions are conducted across multiple blockchains, privacy is still fully protected.

Encryption Privacy Protection Protocol: The WST protocol uses high strength encryption technology to protect transaction data. During cross-chain payments, all data (e.g., transaction information, user identity, payment amount, etc.) is encrypted to ensure that even if the transaction takes place on a public blockchain, this sensitive information will not be known to the outside world.

7. WST Token Roles and Economic Modeling

WST is a native functional token designed to support the operation and governance of the entire privacy-oriented payment network. Its role is not only limited to payment purposes, but also extends to every aspect of the protocol's operation, from fee settlement, to node incentives, to decentralized governance, WST plays an indispensable and fundamental role.

7.1 WST Token's central role in the agreement:

Payment Fuel (Gas): WST tokens are used as fuel in the payment network to pay for the processing fees required for each transaction, especially when enabling privacy features such as mixed coins, zero knowledge certificates, etc., with corresponding fees based on resource usage.

Protocol Pledge: Participating nodes are required to pledge a certain amount of WST as economic collateral in order to perform operations such as transaction packaging, privacy task processing or cross-chain conversion, ensuring the integrity and stability of network participants.

Governance Participation: WST token holders have the right to participate in proposals, voting, protocol upgrades, and major decisions, and are the cornerstone of decentralized governance.

Ecological incentives: the protocol uses some of the tokens to reward behaviors that contribute to the network, such as node maintenance, protocol testing, vulnerability rewards, and private application development.

7.2 Token Aggregate and Distribution Modeling:

The total supply of WST tokens is 1 billion and no additional tokens will be issued in the future to ensure scarcity and long-term value stability. The preliminary allocation model is designed as follows:

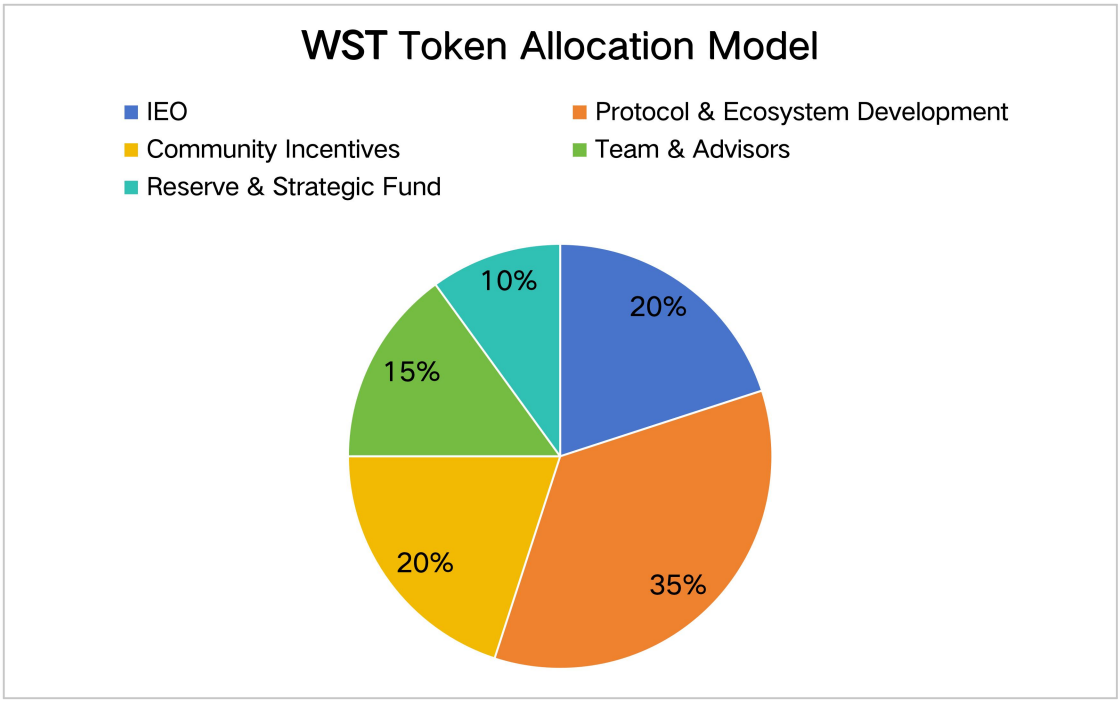
IEO Public Offering (20%): Allocated for initial exchange offerings to enhance token liquidity and encourage early market participation.

Protocol and Ecosystem Development (35%): Dedicated to the development of core privacy protocols, module optimization, cross-chain integration, and application expansion. This portion also supports strategic partnerships and ecosystem resource allocation.

Community Incentives (20%): Distributed to contributors involved in privacy payments, node operations, and governance, aiming to strengthen decentralization and maintain community engagement.

Team and Advisors (15%): Reserved for rewarding the long-term contributions of the core team and technical advisors. A multi-phase vesting schedule with linear release ensures sustainable project growth.

Reserve and Strategic Fund (10%): Designated for future risk management, strategic opportunities, or key protocol milestones. Usage is subject to approval via community governance, with clear release conditions and strict eligibility criteria for participants.



8. Application Scenarios

As a payment protocol token designed for privacy protection, WST Token has a wide range of application potentials, especially in areas with high privacy requirements. Due to its strong privacy protection mechanism, WST can effectively solve several pain points in the existing payment systems, especially in the scenarios of privacy donation, payroll confidentiality, and cross-border payment, which provide innovative solutions. In this section, we will introduce these application scenarios and how to fully utilize the features of WST tokens.

8.1 Private Donation

As charitable donations grow globally, donors are increasingly demanding privacy for their donations. In traditional donation systems, the identity of the donor and the amount of the donation may be recorded and made public, which may be a concern for some donors who have very high privacy requirements. WST token is designed to address this need by using zero-knowledge proofs and a mixed-currency mechanism to ensure that every donation remains anonymous while guaranteeing the validity and security of the transaction.

When donating with WST tokens, donors can conduct transactions completely anonymously, not only protecting their identity, but also ensuring the privacy of the donation amount. The simplicity and anonymity of the donation process makes more

users willing to participate in this charitable endeavor and encourages more people to support transparent and privacy-protected donation methods.

The WST Token's privacy donation solution is not only available to individual donors, but can also be used by large organizations, NGOs, charities, etc. These organizations can safeguard donors' privacy through the WST agreement, while also ensuring transparency in the donation process, thus enhancing donors' trust in the donation process.

8.2 Payroll Confidentiality

Payroll is one of the most common forms of payment between enterprises and their employees. However, with the expansion of enterprise scale and the acceleration of globalization, the privacy issue in payroll is becoming more and more prominent. Information about the amount and method of payroll payment is often easily exposed, which threatens the privacy of employees, and WST tokens provide an innovative solution to protect the privacy of payroll through encrypted payment and anonymous transaction technology.

Businesses can utilize WST agreements for payroll payments, and employees can receive completely anonymous payroll transfers, which protects their privacy and avoids leakage of payroll amounts. By using WST tokens, employees can ensure that their paychecks are not tracked or exposed by unauthorized third parties, thus avoiding unnecessary leakage of personal information or other privacy risks.

In addition, the WST agreement can also support cross-border payroll, enabling employees in different countries to receive their paychecks in a privacy-protected manner, addressing the privacy risks associated with cross-border payroll payments. This feature is not only important for multinational enterprises, but also provides convenience and protection for freelancers and outsourced workers working across borders.

8.3 Cross-border Payments

Cross-border payments have always been one of the most challenging areas of global business transactions. Traditional cross-border payment systems are often plagued by high fees, long processing times, and intermediary monitoring of transactions. In addition, privacy issues in cross-border payments are often overlooked. Against this backdrop, WST tokens offer an innovative solution for cross-border payments.

The WST protocol enables interoperability between different blockchains by supporting cross-chain payment technology and enables fast, low-cost cross-border payments while safeguarding privacy. Using WST tokens for cross-border payments not only effectively reduces transaction fees, but also speeds up transactions, ensuring that they are completed in minutes rather than days as with traditional financial systems.

In addition, the privacy protection technology in the WST protocol ensures that every cross-border transaction can be conducted without revealing transaction details, which not only protects the privacy of both parties, but also avoids possible external surveillance and data leakage risks. Whether you are a multinational company, an international freelancer or an individual user, you can enjoy a payment experience that emphasizes both privacy and efficiency when using WST for multinational payments.

8.4 Future Scenario Expansion

With the growing demand for blockchain technology and privacy protection, WST tokens have a wide range of applications in the future. In addition to the already mentioned privacy donations, payroll and cross-border payments, WST can be further expanded to various areas that require a high degree of privacy protection. For example, WST tokens can be used in legal compliance to protect sensitive payments made by corporations and individuals in legal matters; they can also play a role in the healthcare sector to protect patients' private information and payment data; and they can even be further applied to the entertainment and cultural industries to provide users with a more secure digital payment experience.

The application scenarios for WST tokens are not only in the payment field, but also include various digital asset exchanges that require privacy protection, smart contract execution, decentralized finance (DeFi), and other scenarios. These applications will help expand the market demand for WST tokens and lay a solid foundation for their future development.

9. Security audits and anti-fraud mechanisms

With the popularity of digital payments, the security of the payment system becomes crucial, especially when sensitive financial transactions are involved.WST tokens are designed with security in mind and a series of measures have been taken to ensure the safety of the protocol and user funds.The security audit and anti-fraud

mechanism in the WST protocol will provide protection for all participants and reduce potential risks.

9.1 Security Audit

The WST protocol undergoes regular independent third-party security audits, which are a critical part of ensuring system security and protocol stability. Through a thorough examination of the protocol code, security audits help identify any potential vulnerabilities or inconsistencies and provide recommendations for remediation. These audit reports will be made available to the community to increase transparency and thus enhance user trust.

In addition, the WST team also actively conducts internal security tests, including penetration tests and simulated attacks, to identify potential weaknesses in the protocol. The results of these tests will be used as the basis for subsequent improvements to ensure that the security of the protocol is continuously enhanced.

9.2 Anti-fraud mechanism

With the popularity of digital payments, fraud is becoming increasingly rampant, especially for users unfamiliar with cryptocurrency and blockchain technologies. To this end, the WST protocol is designed with a multi-layered anti-fraud mechanism to prevent all forms of fraud, including phishing attacks, identity impersonation, and illegal payments.

WST uses advanced identity verification technologies and multi-factor authentication mechanisms to ensure that every transaction comes from a legitimate and authorized user. In addition to these basic identity verification measures, WST also implements a transaction behavior analysis system that can detect unusual transaction patterns and warn users or block suspicious transactions in a timely manner.

In addition, WST combines encryption technology with smart contracts to protect the integrity of transactions through pre-set conditions and rules. All transactions are recorded and encrypted for storage, so that if an anomaly is found, it can be traced and scrutinized to avoid loss of funds.

10. Community Governance and Agreed Upgrade Mechanism

The decentralized governance mechanism of the WST protocol is a key feature that ensures that token holders and community members have direct influence over the development of the protocol. This mechanism not only guarantees the transparency and democracy of the protocol, but also effectively promotes innovation and improvement.

10.1 decentralized governance

The governance of the WST Agreement is based on a token holder voting mechanism, whereby token holders have the right to vote on proposals for the Agreement. All major decisions related to protocol upgrades, feature adjustments, and funding allocations will be decided by community vote. This governance structure ensures that each participant's voice is heard and that they are able to participate fairly in the development of the agreement.

In addition, the WST team plans to establish a governance committee to review all submitted proposals. The committee, comprised of experts from different fields, will evaluate the feasibility and potential risks of the proposals. Only vetted proposals will proceed to the voting stage, which will improve the quality and efficiency of the governance process.

10.2 Agreement Upgrade Mechanism

Another key component of the WST protocol is the protocol's upgrade mechanism. As technology evolves and requirements change, the agreement needs to be continuously adjusted and optimized. the WST Agreement has a dedicated upgrade process in place to ensure that the agreement remains adaptable in an evolving environment.

Upgrades to the protocol will be implemented through community proposals and voting, a process that will be transparent and open to all token holders. In order to ensure the smooth implementation of the upgrade, WST has set up a dedicated testing network where all upgrades and changes will be tried out first to identify potential problems and vulnerabilities and to ensure that the upgraded protocol will not adversely affect existing users.

Appendix: Disclaimer

This White Paper is for reference only and is intended to introduce the core functions, application scenarios and development direction of WST Tokens, which have not yet entered the offering and official operation stage, and all contents are future plans and assumptions, and do not constitute any form of commitment or guarantee.

Investors and users should exercise caution and fully understand the risks involved when participating in WST-related activities. The project development team is not responsible for any investment losses and does not guarantee the future market value, liquidity or returns of the tokens. All investment and participation should be based on personal judgment and at the participant's own risk.

In addition, the issuance of WST Tokens and the operation of its related services may be subject to the laws, regulations and policies of the countries or regions in which they are located, and all participants should comply with local laws and regulations. If any legal issues are encountered in the future, the Project Development Team will make adjustments in accordance with the law and reserve the right to do so.