Spermbank App: Substrate Protocol for Encrypted Receipt Management

Abstract

This whitepaper presents a novel approach to digital receipt management using blockchain technology. The protocol embeds encrypted, verifiable receipts directly within payment transactions, eliminating the need for centralized receipt management systems. By leveraging Substrate's blockchain framework, the system ensures atomic transactions that combine payments with receipt data, providing a secure and decentralized solution for proof-of-purchase verification. The protocol is particularly valuable for peer-to-peer transactions and informal economies, where traditional receipt systems are impractical or unavailable. This paper details the technical implementation, including the encryption process, transaction structure, and key management system, while addressing practical limitations and considerations for implementation.

1. Executive Summary

In today's digital commerce landscape, the receipt remains an overlooked yet critical component of financial transactions. While payment systems have evolved dramatically, receipt management continues to rely on paper, email, or proprietary digital systems that create unnecessary friction and dependency on third parties. Spermbank addresses this gap by introducing a novel approach to receipt management: embedding encrypted, verifiable receipts directly within the transaction.

Spermbank is a Substrate-based protocol that standardizes and secures digital receipts through blockchain technology. By leveraging Substrate's flexible framework, the protocol enables atomic transactions that combine payments with encrypted receipt data, ensuring both actions succeed or fail together. This approach transforms any mobile device into a secure point-of-sale system without requiring centralized infrastructure.

The protocol's key innovation lies in its ability to maintain privacy while leveraging public blockchain transparency. Each receipt is encrypted using recipient-specific keys, ensuring that only authorized parties—typically the buyer and merchant—can access the transaction details. This creates a secure, verifiable record of purchase that remains private despite being stored on a public blockchain.

Spermbank is particularly valuable for merchants operating in informal economies or outside traditional payment infrastructure. By embedding receipts directly within payments, the protocol eliminates the need for separate receipt management systems or third-party integrations. Any financial application can read and present proof-of-purchase without requiring coordination with external services or shared backend systems.

Currently configured for the Paseo Testnet AssetHub network, the protocol can be readily adapted to support USDT-based transactions on the Polkadot AssetHub or other production networks, demonstrating its flexibility and potential for broader adoption.

2. Introduction

The receipt, as a formal acknowledgment of financial exchange, forms the foundation of modern commerce. Yet, despite its importance, receipt management remains fragmented and inefficient. In both digital and physical

environments, receipts are predominantly paper-based or tied to proprietary systems, creating significant challenges for consumers, businesses, and regulatory bodies.

Traditional digital receipt systems typically depend on centralized providers, SMS/email-based delivery, or tight integration with merchant systems. These approaches introduce several limitations: they create vendor lock-in, raise privacy concerns, and require ongoing dependency on third-party infrastructure. In peer-to-peer or informal market settings, where formal backend systems are absent, receipt delivery becomes particularly challenging to verify or trust.

Spermbank addresses these limitations through a simple yet powerful concept: embedding the receipt directly into the payment transaction. By attaching an encrypted, signed record of the transaction alongside the monetary transfer, authorized parties can independently retrieve, verify, and decrypt the proof of purchase. This eliminates the need for manual integrations, or external verification systems.

The protocol leverages Substrate's blockchain framework, known for its flexibility and cost-effective transaction model, to create a public, immutable trail of purchase metadata while maintaining privacy. Unlike traditional systems, this receipt layer operates independently of payment processors, focusing solely on the transaction participants.

3. Use Cases

Spermbank's innovative approach to receipt management addresses several critical use cases in modern commerce, particularly in scenarios where traditional receipt systems fall short.

3.1 Peer-to-Peer Sales and Informal Transactions

In today's economy, a significant portion of commerce occurs in informal settings—local marketplaces, garage sales, or direct person-to-person exchanges. In these environments, issuing formal receipts is often impractical or completely overlooked, creating challenges for both buyers and merchants. Traditional receipt systems, which typically require business registration, point-of-sale equipment, or integration with payment processors, are ill-suited for these scenarios.

Spermbank transforms this landscape by enabling any mobile device to function as a secure, self-custodial receipt generator. When a merchant clat a weekend market receives a mobile payment, Spermbank automatically encrypts and attaches a receipt to the transaction. The buyer receives private, verifiable proof-of-purchase without requiring printers or intermediary services. This capability is particularly valuable in emerging markets or informal economies where traditional business infrastructure is limited.

3.2 Regulatory and Tax Audit Trails

For independent contractors, freelancers, and small businesses, maintaining accurate financial records is crucial for regulatory compliance and tax reporting. Traditional approaches often involve manual processes—screenshots, manual exports, or reliance on external platforms—creating significant friction during audits or tax filings. These methods are not only time-consuming but also prone to errors and may not meet regulatory requirements.

Spermbank addresses these challenges by integrating receipt generation directly into the payment process. When a contractor receives payment for services, the transaction automatically includes a signed receipt containing detailed information about the services rendered, buyer details, and transaction metadata. At tax time, the contractor can efficiently filter, decrypt, and export the required data for disclosure, eliminating the need for complex account integrations or specialized reporting tools.

This approach provides a privacy-first solution for maintaining audit-ready records. Unlike traditional systems that require sharing financial data with third-party platforms, Spermbank enables businesses to maintain complete control over their transaction records while ensuring compliance with regulatory requirements. The system's ability to generate standardized, verifiable receipts makes it particularly valuable for businesses operating in regulated industries or those subject to frequent audits.

4. System Architecture

Spermbank's architecture is designed to operate entirely from a mobile device, eliminating the need for external servers or cloud platforms. This self-contained approach ensures maximum privacy and reliability while minimizing infrastructure requirements. The system consists of three interconnected layers that work together to provide a seamless receipt management experience.

4.1 Client Layer

At the foundation of Spermbank lies the client layer, built using React Native and Expo to provide a robust cross-platform mobile application. This layer serves as the primary interface between users and the receipt management system, handling all aspects of receipt creation, encryption, and blockchain interaction.

The client layer is composed of several specialized components, each responsible for a specific aspect of the system's functionality. The ReceiptManager handles the creation and encryption of receipts, ensuring that all necessary information is properly formatted and secured. The KeyManager maintains the system's encryption keys, storing them securely in the device's protected storage. The BlockchainManager interfaces with Substrate nodes, managing the submission and verification of transactions. The QRManager facilitates the exchange of information between devices through QR codes, while the TransactionManager maintains the local history of transactions and their associated receipts.

4.2 Receipt Creation Process

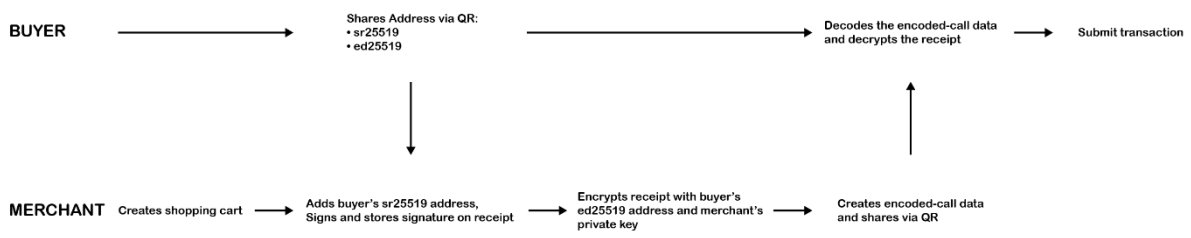
The receipt creation process begins with the buyer sharing their Ed25519 and Sr25519 addresses with the merchant. The merchant then uses these addresses for both receipt creation and encryption. This approach ensures that:

- The merchant can create a receipt specifically for the buyer

- The receipt can be encrypted using the buyer's public key

- The transaction can be properly signed and verified

- The buyer and merchant can decrypt and verify the receipt using their private keys



This sequence diagram illustrates the receipt creation process, showing the interaction between merchant and buyer devices, address exchange via QR codes, and the steps involved in creating and encrypting the receipt.

Once the addresses are exchanged, the merchant creates a receipt containing all relevant transaction details. This receipt is then signed with the merchant's private key, providing cryptographic proof of its authenticity. The signed receipt is encrypted using asymmetric encryption, ensuring that both the buyer and merchant can access its contents. Finally, the encrypted receipt is attached to the encoded-call data, which is shared with the buyer. The buyer can then decode and decrypt the transaction to ensure its authenticity, creating an atomic operation that combines payment and receipt in a single blockchain transaction.

5. Technical Implementation

Spermbank's technical implementation combines advanced cryptographic techniques with blockchain technology to create a secure and efficient receipt management system. The system's architecture is built around two core components: encryption and transaction structure.

5.1 Encryption Process

The encryption process forms the foundation of Spermbank's security model, employing asymmetric encryption to ensure that receipt data remains private while maintaining verifiability. This approach allows both the buyer and merchant to access the receipt data while keeping it secure from unauthorized parties.

The process begins with the buyer sharing their Ed25519 and Sr25519 addresses with the merchant. The merchant then uses these addresses to create and encrypt the receipt. The receipt is signed with the merchant's private key, providing cryptographic proof of its authenticity. The signed receipt is then encrypted using asymmetric encryption, ensuring that both the buyer and merchant can access its contents.

This approach guarantees both the integrity and confidentiality of the receipt data, as it can only be decrypted by the intended parties. The use of asymmetric encryption eliminates the need for complex key exchange protocols while maintaining strong security guarantees.

5.2 Transaction Structure

The transaction structure is designed to maintain the atomicity of payment and receipt operations, ensuring that both components succeed or fail together. This is achieved through a carefully designed structure that combines payment and receipt data in a single blockchain transaction.

Atomic Transaction Structure

Call 0	Call Index	0000		
	Call Module	Balances		
	Call Name	Transfer Keep Alive		
	Params	Dest	ID	0x000
		Value	10000	
Call 1	Call Index	0001		
	Call Module	System		
	Call Name	Remark		

	Params	Remark	{
			"encrypted_receipt": "base64_encoded_ciphertext",
			"aes_iv": "base64_encoded_iv",
			"recipients": [
			{
			"ephemeral_public_key": "base64_encoded_key",
			"encrypted_key": "base64_encoded_key",
			"nonce": "base64_encoded_nonce"
			}
			]
			}	

This diagram illustrates the atomic transaction structure, showing how payment and receipt components are bundled together using Substrate's utility.batchAll method. It demonstrates the relationship between different transaction elements and their role in maintaining atomicity.

The payment component includes essential transaction details such as the transfer amount, asset and recipient address. The receipt component contains the encrypted receipt data, merchant signature, metadata. These components are bundled together using Substrate's utility.batchAll method, creating an atomic transaction that cannot be partially completed.

This atomic structure is crucial for maintaining the integrity of the receipt system. It ensures that every payment is accompanied by its corresponding receipt, and that the receipt cannot be modified or tampered with after the transaction is completed. The structure also enables efficient verification of transactions, as both payment and receipt data can be validated in a single operation.

6. Blockchain Interaction

Spermbank's interaction with the blockchain is designed to ensure efficient and secure transaction processing while maintaining the integrity of receipt data. The system leverages Substrate's powerful features to create a robust and reliable receipt management solution.

6.1 Extrinsic Structure

The blockchain interaction is built around Substrate's extrinsic system, which provides a flexible and efficient way to process transactions. Each transaction in Spermbank combines two essential components: a payment transfer and receipt storage. The payment transfer is handled through the balances.transfer_keep_alive call, while the receipt data is stored using the system.remark call. These components are bundled together using the utility.batchAll method, ensuring atomic execution of both operations.

The transaction flow begins with the creation of a transaction containing both payment and receipt data. The merchant signs this embedded receipt, providing cryptographic proof of its authenticity. The transaction is then submitted to the network, where it undergoes validation and confirmation. Once confirmed, the receipt is permanently stored on the blockchain, creating an immutable record of the transaction.

Transaction verification is a crucial aspect of the system, ensuring that each transaction meets specific criteria. The system verifies that the payment amount matches the receipt, the receipt is properly encrypted, and the merchant's signature is valid. This comprehensive verification process guarantees the integrity of each transaction and its associated receipt.

6.2 Storage Limits

Receipt size limits are established to ensure optimal performance while maintaining practical usability. Through testing, the system has successfully handled receipts containing up to 200 items, demonstrating robust scalability. However, a recommended limit of 100 items per receipt is recommended as this far exceeds typical market transaction sizes while maintaining data limits. For transactions requiring more than 100 items, splitting the payment into multiple transactions is recommended, each with its own receipt.

6.3 Transaction Fees

Transaction fees are weight-based, meaning the fee is directly proportional to the size of the receipt being stored. This due to the computational and storage resources required by the transaction. Fees typically range

between 0.001 and 0.05 units (PAS on Paseo Testnet), with larger receipts incurring higher fees due to increased storage and processing requirements.

7. Limitations and Considerations

Receipt size is limited by blockchain storage requirements, which affects both transaction fees and performance. The system is designed to handle typical receipt data efficiently, but users should be aware that extremely large receipts may require special handling or optimization. The current implementation focuses on maintaining a balance between detail and efficiency.

Transaction history management presents another consideration. The system relies on both the Subscan API and Polkadot API for transaction history and verification, as neither API alone provides complete and real-time access to the receipt map. For businesses requiring comprehensive receipt management, it is recommended to implement a custom indexer or API service that can:

- Maintain a complete and up-to-date receipt map
- Provide real-time transaction monitoring
- Enable efficient searching and filtering of receipts
- Ensure reliable access to historical data
- Support business-specific reporting and analytics needs

This approach would eliminate the current limitations of relying on third-party APIs and provide businesses with the reliable receipt management system they require.

Network dependencies are an inherent aspect of the system. The protocol requires an internet connection for blockchain interactions and depends on the availability of various APIs. Users should be aware that network issues or API rate limits may affect system performance or availability.

7.1 Standardization Needs

The protocol requires standardization in several areas to ensure interoperability and reliability. These standards are essential for the system's long-term success and adoption.

Receipt format standardization is crucial for ensuring that receipts can be reliably processed and verified across different implementations. This includes establishing standard JSON structures, defining required fields, and specifying optional fields. These standards help guarantee consistency and allow proper interpretation by different systems.

Encryption standards are another important consideration. The system requires standardized approaches to key exchange, encryption, and signature verification. These standards ensure that receipts can be securely created and verified across different implementations, maintaining the system's security and privacy features.

Blockchain interaction standards are necessary for ensuring consistent transaction processing and verification. This includes standardizing transaction formats, storage approaches, and verification methods. These standards help ensure that the system can operate reliably across different blockchain networks and implementations.

7.2 Legal & Compliance

The protocol is designed to support common business needs while acknowledging the importance of legal and compliance considerations. This section outlines the system's features and limitations in this context.

Receipt features include several elements that support business operations. The system includes merchant details, items, prices, and tax information in receipts, providing a comprehensive record of transactions. Immutability is maintained through blockchain storage and signatures, ensuring that receipts cannot be modified after creation. The system supports returns and refunds with proper documentation and provides verifiable proof of transactions. Expense tracking is supported through the system's transaction history features.

Business considerations include important caveats that users should be aware of. While the protocol provides features that support common business requirements, businesses should consult with their tax and legal advisors to ensure compliance with specific regulatory requirements. The system does not provide specific legal compliance guarantees, and users are responsible for ensuring that their use of the system meets applicable legal and regulatory requirements.

8. Open Source Development

Spermbank is released as open-source software, providing users with the freedom to use, modify, and adapt the system to their specific needs. This open approach encourages innovation and collaboration while ensuring transparency in the system's implementation.

The protocol can be used in various ways, depending on the user's requirements and technical capabilities. Users can implement the system as-is for basic receipt management needs or modify specific components to better suit their use cases. The modular architecture allows for integration of individual components into other projects, enabling developers to leverage specific features without adopting the entire system. The open-source nature of the project also encourages community participation in identifying and fixing bugs, contributing to the system's ongoing improvement.

The system's modular architecture is designed to support this flexibility. The component system is highly adaptable, allowing for customization of features and functionality. The design is extensible, enabling developers to add new capabilities or modify existing ones to meet specific requirements. This approach ensures that the system can evolve to meet changing needs while maintaining its core functionality and security features.

9. Conclusion

Spermbank demonstrates the feasibility of building a fully decentralized receipt system that maintains privacy and security while leveraging the transparency of public blockchains. The protocol's innovative approach to receipt management addresses long-standing challenges in digital commerce, providing a solution that is both practical and forward-looking.

While the protocol uses public APIs for blockchain interactions, it maintains direct peer-to-peer receipt exchange without requiring centralized receipt management systems. This approach combines the benefits of blockchain technology with the efficiency of direct communication between transaction participants.

The protocol's architecture ensures that receipts are immutable and verifiable, providing a reliable record of transactions that cannot be altered or tampered with. The system maintains privacy and security through sophisticated encryption and key management, ensuring that sensitive transaction data remains protected. The decentralized, peer-to-peer nature of the system eliminates the need for intermediaries, reducing costs and complexity. The efficient and cost-effective design makes the system accessible to a wide range of users, from individual consumers to businesses of various sizes.

This approach provides a solid foundation for future development and adaptation to various use cases and requirements. As the system evolves, it has the potential to transform how receipts are managed in digital commerce, creating a more efficient, secure, and user-friendly experience for all participants.