Technical Datasheet: Secure and Anonymous Blockchain Algorithm with Public and Private Keys

---

1. Introduction

The algorithm presented here is based on a secure blockchain ensuring user anonymity, transaction security, and data integrity. It uses public and private keys to guarantee transaction security and user identification while maintaining anonymity.

---

2. Payment System Structure

2.1. Public and Private Keys

- **Public Key**: Used to receive funds and can be shared with other users. It acts as a public address where others can send money without knowing the user's identity, as it contains no personal information. It is equivalent to a bank account number.
- **Private Key**: Used to sign transactions and prove ownership of funds. It must remain secret, as anyone with access to the private key can spend the funds associated with the corresponding public key. The private key authenticates the user and authorizes transactions.

2.2. Anonymous Payments

Transactions are carried out using a public key generated specifically for each transaction. This method prevents direct identification of the sender and receiver. The user keeps their private key confidential, ensuring only authorized individuals can initiate payments from this address.

---

3. Transaction Anonymization

3.1. Fragmentation and Verification

Transactions are divided into multiple anonymous fragments validated independently. Each fragment is signed with a unique private key, but only the public address is visible on the blockchain, ensuring that no external actor can link a transaction to a specific user.

3.2. Zero-Knowledge Proofs (ZKPs)

The algorithm uses zero-knowledge proofs to validate transactions without revealing sensitive information. For instance, users can prove they have sufficient funds to make a payment without disclosing their exact balance or other personal data.

3.3. Ring Signatures and Coin Mixing

- **Ring Signatures**: Multiple users collectively create a signature, making it impossible to identify the real sender among them.
- **Coin Mixing**: A process where multiple transactions are combined to mix funds, making it difficult to trace the origin or destination of payments.

4. Security and Integrity

4.1. Cryptographic Hashing

Every transaction is hashed using functions like SHA-256, ensuring data security and immutability. Even a single character change in the transaction alters the hash, invalidating the transaction.

4.2. Double-Spending Prevention

The algorithm employs a decentralized validation system to prevent double-spending, where users attempt to spend the same funds twice. This is ensured by independent miners verifying the validity of each transaction.

4.3. Independent Validation by Miners

Miners independently validate transaction fragments and only have access to portions of the data. This prevents malicious miners from reconstructing a complete, valid transaction.

5. Recovering Funds in a Wallet

5.1. Withdrawal Process

To recover funds in a wallet, the user follows these steps:

1. **Access Wallet**: Using their private key, the user accesses the wallet to manage transactions.
2. **Receive Funds**: Funds are sent to the user’s public address, generated from their public key.
3. **Make Withdrawals**: Users can transfer funds to another address or convert them to fiat currency via an exchange platform.

5.2. Public and Private Key Functionality

When receiving funds, users can generate a new address for each transaction, ensuring old addresses cannot be linked. This method of generating unique addresses per transaction maintains user anonymity.

6. Algorithm Use Cases

6.1. Anonymous Payments

Users can make payments anonymously without revealing personal information or transaction history.

6.2. Anonymous Voting Systems

The system can facilitate secure, anonymous voting where voter identities are protected while votes are transparently and verifiably counted.

6.3. Sensitive Data Exchange

Institutions like hospitals or banks can use the system to securely and anonymously exchange sensitive data, preserving user confidentiality while ensuring the validity of exchanges.

6.4. Supply Chain Traceability

The system ensures product traceability in a supply chain, guaranteeing transparency without compromising the privacy of involved actors.

---

7. Conclusion

This blockchain algorithm, leveraging public and private keys, creates a secure, anonymous, and transparent payment system. It ensures both transaction integrity and user confidentiality. By combining decentralized validation, zero-knowledge proofs, and ring signatures, the algorithm offers a robust solution for various applications, from anonymous payments to sensitive data management.

Conte Théo, born 01/10/2001 in Grenoble, France