Algorand™

ALGORAND REKEYING:

Enabling the Security, Flexibility, and Operational Efficiency of Private Spending Keys

Public Address and Private Spending Key combos are used to protect accounts in blockchain. Public Address are publicly known and used for identification of an account, where Private Spending Keys are for security purposes and used for authentication and encryption of the Public Address. Today, the Public Address and Private Spending Key combo cannot be broken - they always come in distinct pairs.

The system of using keys in cryptography for protecting accounts has existed since the beginning of blockchain. But it has become inefficient and not always secure. When a compromised Private Spending Keys needs to be changed, an entirely new account with Public Address and Private Spending Key need to be opened - and assets within that account have to be moved from the old Public Address to a new address representing a new account creating inefficiency and onerous operational overhead.

Regularly changing the Public Address and Private Spending key also creates downstream implications. For instance, each time a user wants to initiate a transaction from a new public address, they must provide the new public address to others for identification purposes. This leads to interruptions of automated recurring transactions with peers or institutions and additional back office work for those institutions, peers, and vendors to keep track of the changing public address. Custody providers, as an example, encounter significant operational issues today as they often move customer funds from one public address to another in an effort to keep the spending keys cold.

UNIQUE FUNCTIONALITY

Rekeying, a feature of Algorand, solves for the existing Public Address and Private Spending key friction by allowing users to change their Private Spending key without the need to change their Public Address. Rekeying enables more fl xibility, Public Address continuity of use and permanent identifier with less overhead when changes to the Private Spending key occurs. This is achieved by having the:

- **Flexibility** in their ability to change the Private Spending Key anytime without needing to change the Public Address
- **Continuity** that provides the ability to continue using one's Public Address and keeping the assets in the same Public Address
- **Operational Efficiency** to maintain existing Public Address as identifiers or other people and custody providers that continuously transact with that Public Address, lowering operational burdens

KEY ATTRIBUTES & BENEFITS TO YOUR BUSINESS

Built into Algorand's Layer-1 Protocol that is:

- Decentralized
- Secure
- Scalable

Taking advantage of the Network's:

- Flexibility in Changing Private Spending Keys
- Preserving Account Permanence
- Account Novation, Governance and Control over Accounts
- Enables low operational overhead
- Secure accounts with hardware wallet, a multi-sig account, or smart contract based key
- Ensure "contract address," where the "smart contract" becomes the authorized signer

KEY BENEFITS

Algorand's Rekeying is unique and different because no other blockchain offers a way to change Private Spending Keys so easily, where it is:

- A fast and seamless way to preserve account permanence
- Secure existing accounts with a new Private Spending Key at anytime, including with a hardware wallet, a multi-sig account, or smart contract based key
- Novation with the ability to reassign ownership of a contract
    - This is often done in the form of reassigning ownership of a contract and often done in a larger settlement context.
    - With blockchain, accounts can now have ownership re-assigned trustlessly and in the context of atomic transfers/settlement.

MOST EXCITING USE-CASES

Many digital transactions need a secure, seamless way to transfer currency, and digital wallets or digital accounts require a Public Address as the account address and Private Spending Key as the account secure key to unlock that account. Rekeying enables key unique functionalities wherever a digital wallet or account is enabled with Algorand's blockchain feature that unlocks many possibilities for greater security, fast private key changes, low operational overhead for custody providers and much more.

1. Novation with the ability to reassign ownership of a contract. Rekeying the secret to a single Private Spending Key, a multi-sig key, or a stateless smart contract (contract account).
2. Custody Providers (that includes banks, exchanges, savings associations, registered broker-dealers, and futures commission merchants) can benefit from Rekeying by:
    a. Keeping their user's Private Spending Keys cold at all times while only needing to manage one Public Address key
    b. Eliminate the chain of old Public Address keys from having to move funds after using the Private Spending Keys. Eliminate complex off-chain solutions created to maintain a single Public Address key but give more control over the Private Spending Key.
    c. Enable standardized key rotation schedules depending on security posture (i.e. a company can institute a monthly key rotation if desired).
3. Onboarding large user bases for projects that are moving to Algorand from another blockchain or more traditional technology, making it easier to get users set-up and ensuring as little friction as possible is passed to them during the transition. Rekeying allows organizations to create and set-up accounts for their users ahead of time and trustlessly reassign them when needed
4. Any high security scenario in which the Private Spending Key must be kept cold, but a transaction is needed from the account.

About Algorand Inc.

Algorand Inc. built the world's first open source, permissionless, pure proof-of-stake blockchain protocol for the next generation of financial products. This blockchain, the Algorand protocol, is the brainchild of Turing Award-winning cryptographer Silvio Micali. A technology company dedicated to removing friction from financial exchange, Algorand Inc. is powering the DeFi evolution by enabling the creation and exchange of value, building new financial tools and services, bringing assets on-chain and providing responsible privacy models.

To learn more and work with the Algorand team, contact us at **algorand.com/contact**