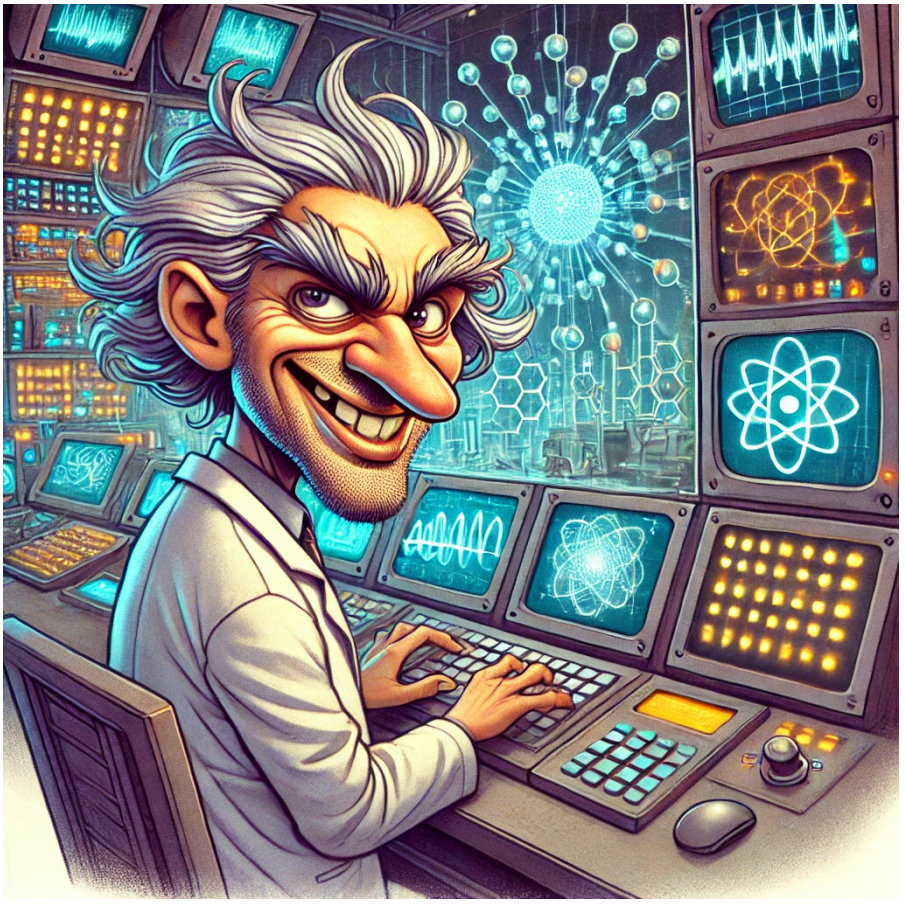
Layer 1 Solution with AI and Blockchain

How to use?

Quantum-Resistant Design: Our Top Priority

Regarding quantum computing, there might be trolls boldly claiming something like:
“With our quantum computers, **we can instantly obliterate all addresses using the widely adopted ECDSA encryption, such as in Bitcoin and Ethereum. By obtaining the periodic information of the elliptic curve ($y^2 = x^3 + 7$) modulo ($2^{256} – 2^{32} – 977$), we’ll bring blockchain to its knees!**“



Even if such 2^{256}-compatible quantum computers (using quantum gate systems) were operational as early as the late 2030s, blockchain’s inherent flexibility ensures it will never succumb to such threats.

At SORA, we've verified that a superior, forward-looking design is already feasible on the current main network. It allows us to mitigate the issue by simply discarding addresses linked to ECDSA. This means countermeasures are already in place today, and we can address future challenges with confidence.

Furthermore, we have implemented a system capable of supporting up to 256 types of cryptographic keys. This design allows for seamless key upgrades in line with changing times, ensuring a robust and adaptable security framework.

SORA Quantum Resistance Blockchain Core

The SORA-QAI Blockchain Core inherits from the wallets of typical blockchain projects, so you can use it in the same way.

After downloading, extract the executable file (SorachanCoin-Core.exe) from the archive. Note that there is no installer provided. In cryptocurrency (crypto-assets/virtual currency), upgrading the wallet is usually done by simply overwriting the executable file. Therefore, an installer would be inconvenient if you only need the executable file.

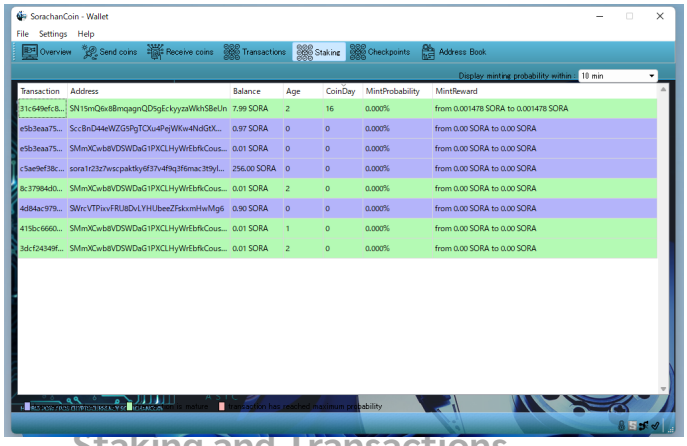
Next, place the executable file (SorachanCoin-Core.exe) in a location of your choice and launch it. Please allow it through SmartScreen.

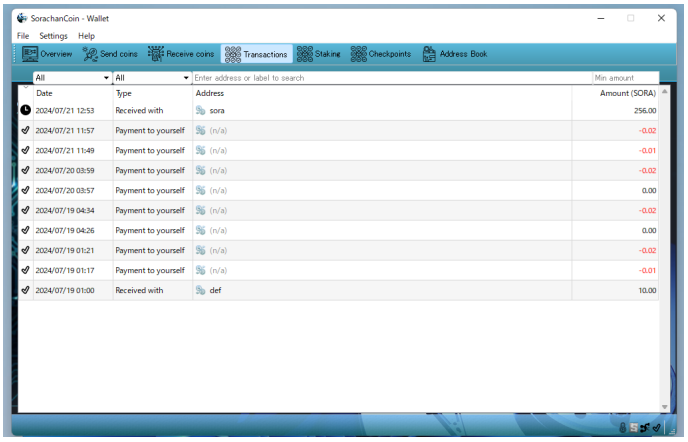
A dialog will prompt you to set the data folder, where you can specify the location for the blockchain and the wallet. Then, wait for the blockchain to synchronize.

SORA-QAI offers a rich array of features, such as “Quantum AI-resistant Schnorr aggregated signatures (5000 keys)” and “Blockchain anonymous encrypted communication,” due to our enthusiasm for key development. We hope you will find these features useful.

Overview

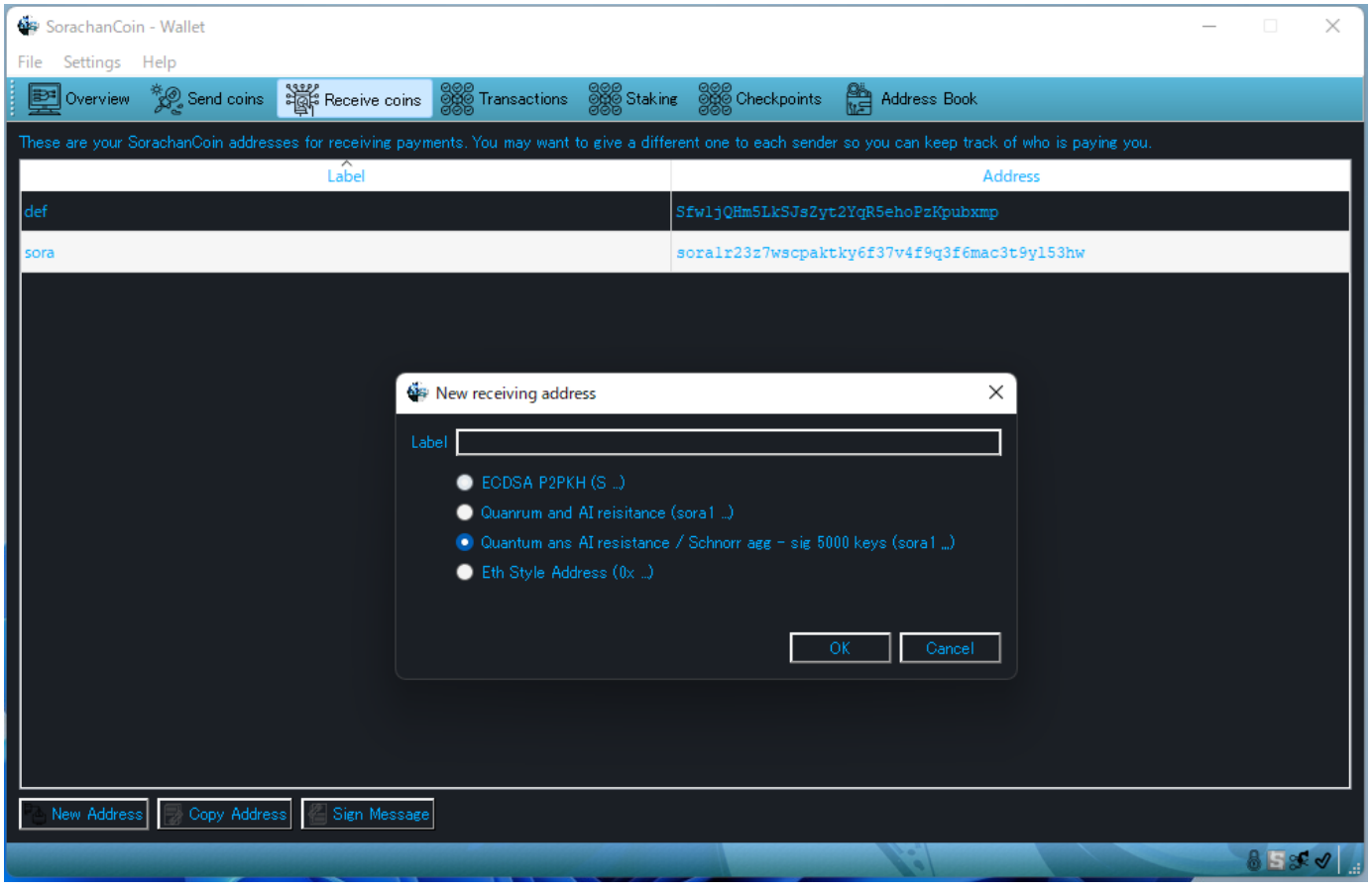
The overview highlights that the staking balance and balance categories are divided into “ECDSA only” and “Quantum AI-resistant Schnorr aggregated signatures (5000 keys).” It allows you to see at a glance the categories managed by SORA.





Staking and Transactions

This operates in a “decentralized” manner, leveraging the nature of the blockchain.

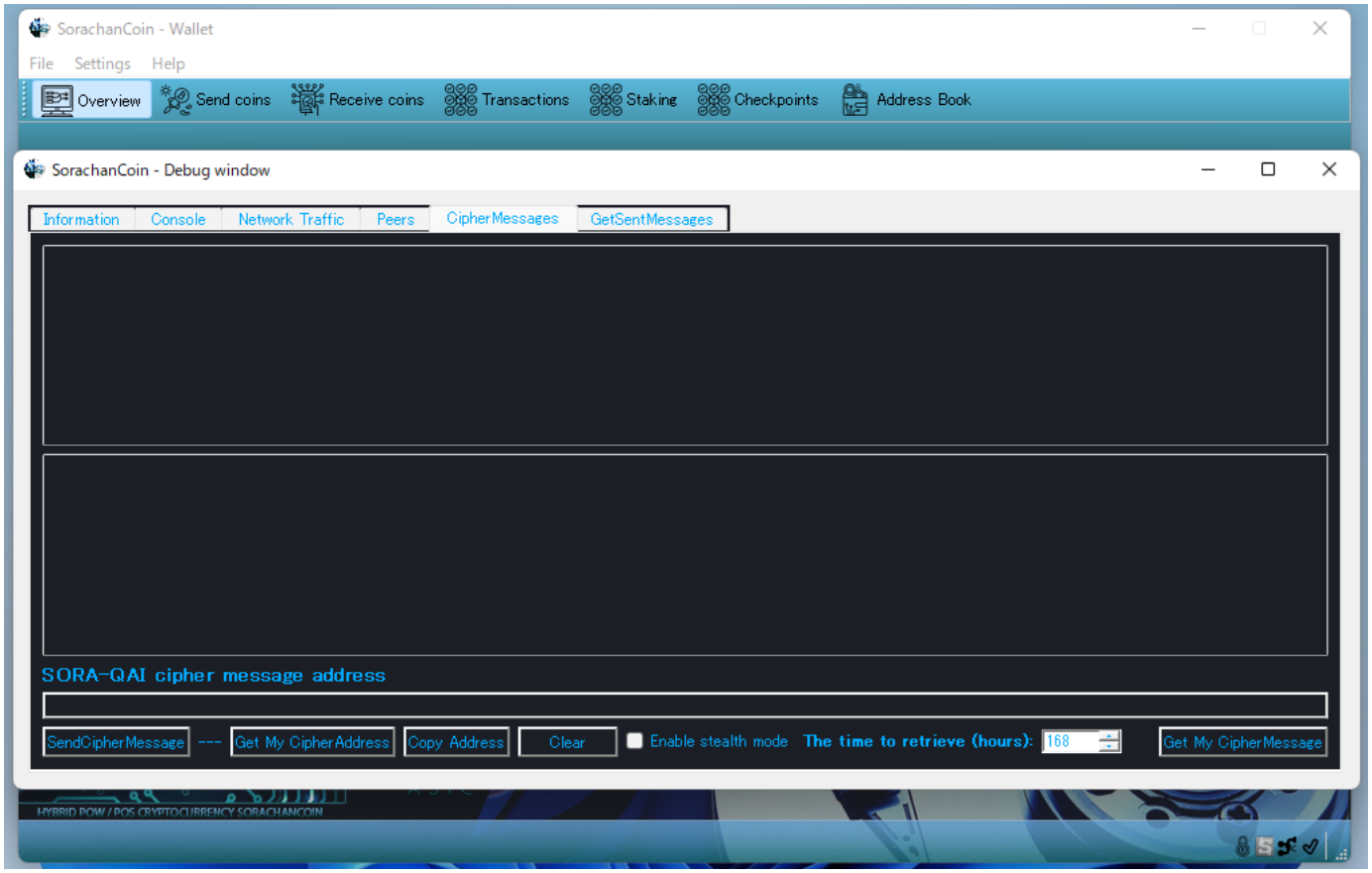


Introduction of New Features in SORA-QAI

When obtaining a new address, you will choose from 4 types:

- **An address for ECDSA: e.g (S ...)**
- **An address for Quantum AI-resistant: e.g. (sora1 ...)**
- **An address for Quantum AI-resistant Schnorr aggregated signatures (5000 keys): e.g. (sora1 ...)**
- **Ethereum-style address: e.g. (sora1 ...)**

If you generate without checking any options, it will be for ECDSA. The rest are determined by the presence or absence of checks. Note that the Ethereum-style address is still under development. It will sync with Ethereum's private key to obtain the same public key, which will be used to operate SORA.



Debug Menu

Open the debug menu to “Obtain your cryptographic address,” where you can get the address of the public key to receive encrypted messages. This special address starts with cipher1 and is for encrypted messages only. By separating it from the SORA receiving address, you can avoid accidental usage.

Sending and Receiving

The button on the left is for sending, and the button on the right is for receiving. Messages are sent to the address at the top. If you set the recipient address to a third party, it becomes a dialogue via encrypted messages. If you set it to yourself, it becomes an encrypted memo that only you can read.

There is also a “Stealth Mode” checkbox. When sending in this mode, your public key address is not displayed to the recipient, making you anonymous. Since the blockchain does not recognize the concept of IP addresses, it is impossible to trace the anonymous recipient. In the image, received messages with a from field of “—” were sent in this “Stealth Mode.” Normally, the from field contains the sender’s address.

When you receive a message, it is displayed at the top as shown in the image. You can change the search time with the spin box next to it. The default is 168 hours, covering 7 days.

Writing and Sending Encrypted Messages

Write your encrypted message in the large text box below. It supports Japanese and line breaks, with a maximum of about 2,000 characters. After sending, wait for it to be recorded on the blockchain. There is a feature that automatically checks until it is recorded, and you will be notified once it is complete.

This feature leverages the decentralized nature of the blockchain, ensuring that no one, not even us, can intercept the messages. Rest assured.

Viewing Sent Encrypted Messages

The adjacent feature allows you to view encrypted messages you have sent in the past. Enter the recipient's address and press the button on the right in the same way.