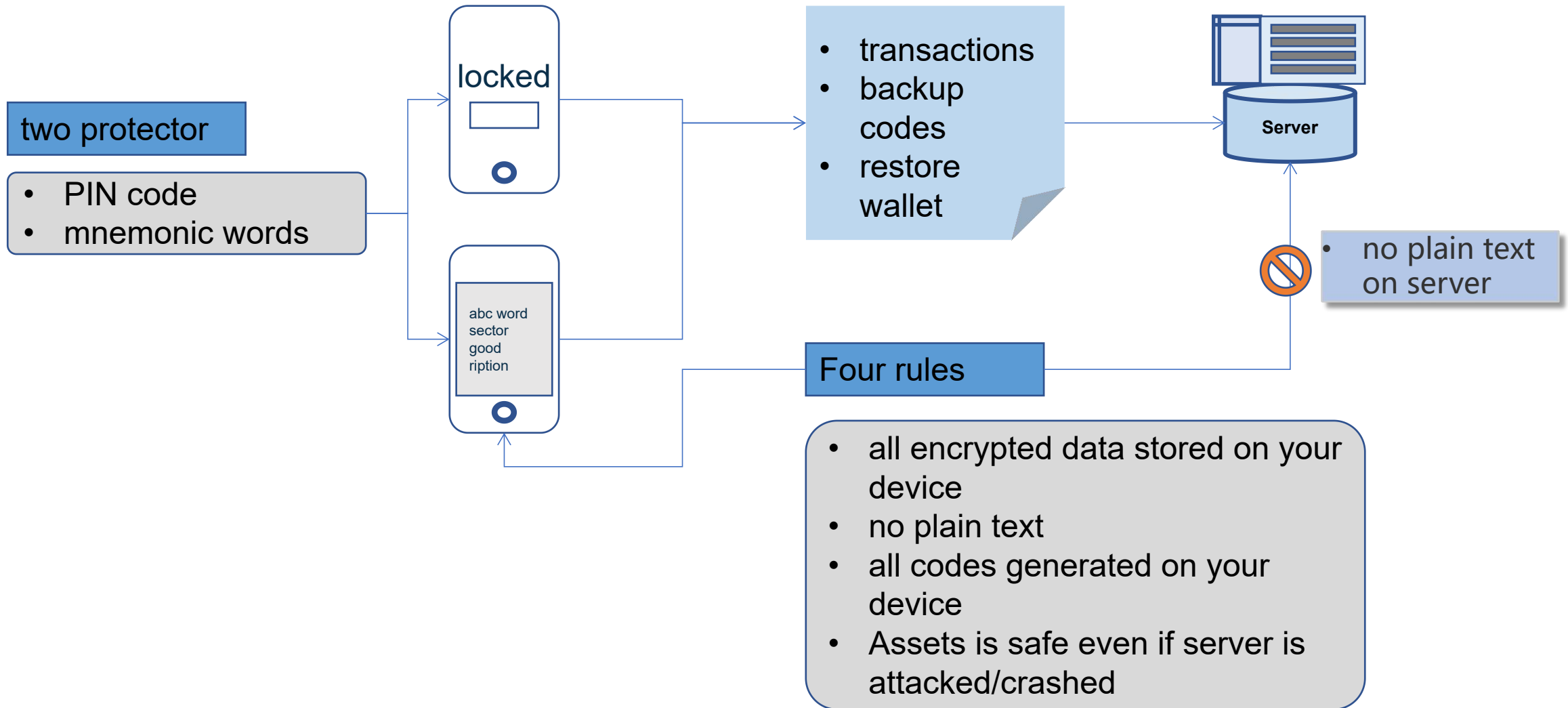


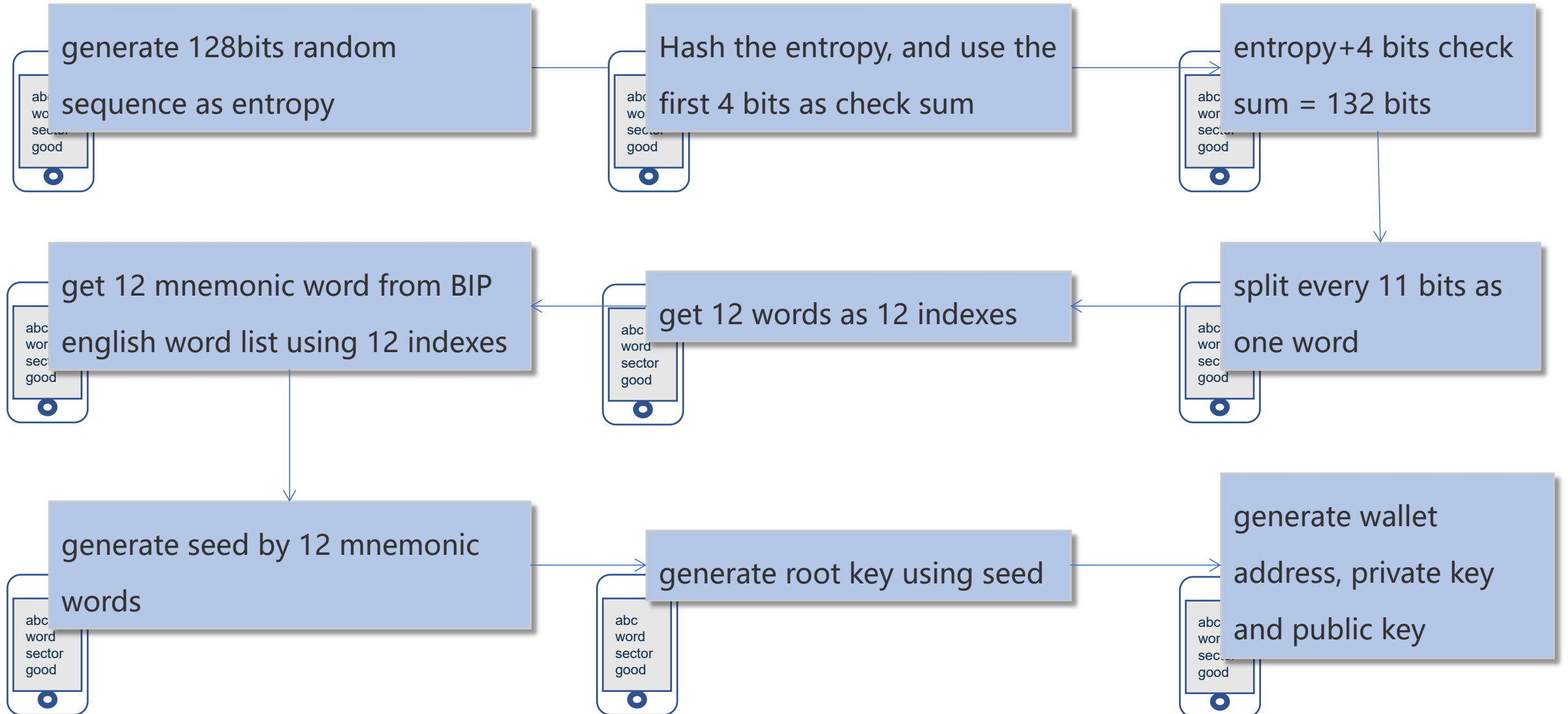
The Security of Decentralized Mobile OmniWallet

OmniLayer
Kevin Zhang
2019.5

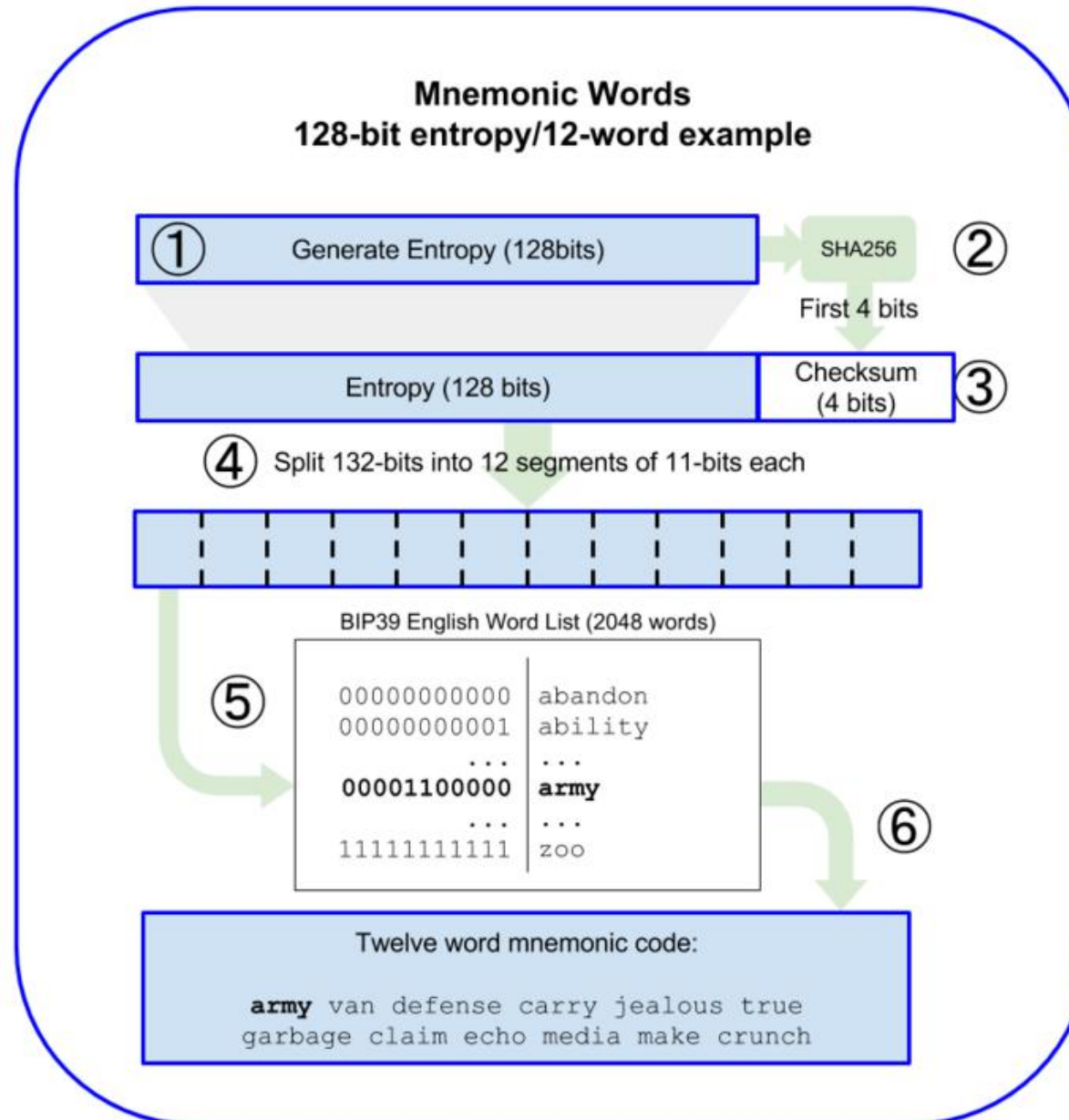
Decentralized Security Architecture for Mobile OmniWallet



Process for generating 12 mnemonic words, wallet address and private key



12mnemonic code generation



```
graph LR; A[start wallet] --> B[register account]; B --> C[input nick name and pin code]; C --> D[encrypt PIN code in MD5, and store it in local and server]; D --> E[generate mnemonic words]; E --> F[backup mnemonic words]; F --> G[create a default address(store the address on server, while the private key will be generated dynamically when transaction occurs)]; G --> H[begin to use the wallet]; H --> I[next page];
```

The flowchart illustrates the process of creating a wallet. It begins with 'start wallet', followed by 'register account', 'input nick name and pin code', and 'encrypt PIN code in MD5, and store it in local and server'. A 'Server' icon is shown next to the encryption step. The process then moves to 'generate mnemonic words', which is linked to a list of 'use of mnemonic words:'. This list includes: 'As user ID(MD5 encrypted, stored at local and server)', 'Display in backup page(AES encrypted in local)', and 'generate root seed, then address and private key'. The next step is 'backup mnemonic words', which is linked to a list of 'use of PIN code when:'. This list includes: 'Unlock App', 'Restore account as an extra check', 'Verify transferring tokens', 'Backup mnemonic codes', 'Sign transaction where PIN code is used as salt to encrypt private key.', and 'generate root seed as salt(to be done)'. The process then moves to 'create a default address(store the address on server, while the private key will be generated dynamically when transaction occurs)', which is linked to a 'Server' icon. The final step is 'begin to use the wallet', which is linked to a 'next page' box. A 'Server' icon is also shown next to the 'begin to use the wallet' step.

start wallet

register account

input nick name and pin code

encrypt PIN code in MD5, and store it in local and server

Server

generate mnemonic words

use of mnemonic words:

- As user ID(MD5 encrypted, stored at local and server)
- Display in backup page(AES encrypted in local)
- generate root seed, then address and private key

backup mnemonic words

use of PIN code when:

- Unlock App
- Restore account as an extra check
- Verify transferring tokens
- Backup mnemonic codes
- Sign transaction where PIN code is used as salt to encrypt private key.
- generate root seed as salt(to be done)

create a default address(store the address on server, while the private key will be generated dynamically when transaction occurs)

Server

begin to use the wallet


next page



register account

input nick name
and pin code

encrypt PIN code in MD5, and
store it in local and server



Server



- use of mnemonic words:
- As user ID(MD5 encrypted, stored at local and server)
- Display in backup page(AES encrypted in local)
- generate root seed, then address and private key


- As user ID(MD5 encrypted, stored at local and server)
- Display in backup page(AES encrypted in local)
- generate root seed, then address and private key

generate
mnemonic
words

- use of PIN code when:
 - Unlock App
 - Restore account as an extra check
 - Verify transferring tokens
 - Backup mnemonic codes
 - Sign transaction where PIN code is used as salt to encrypt private key.
 - generate root seed as salt(to be done)

- Unlock App
- Restore account as an extra check
- Verify transferring tokens
- Backup mnemonic codes
- Sign transaction where PIN code is used as salt to encrypt private key.
- generate root seed as salt(to be done)

create a default address(store the address on server, while the private key will be generated dynamically when transaction occurs)



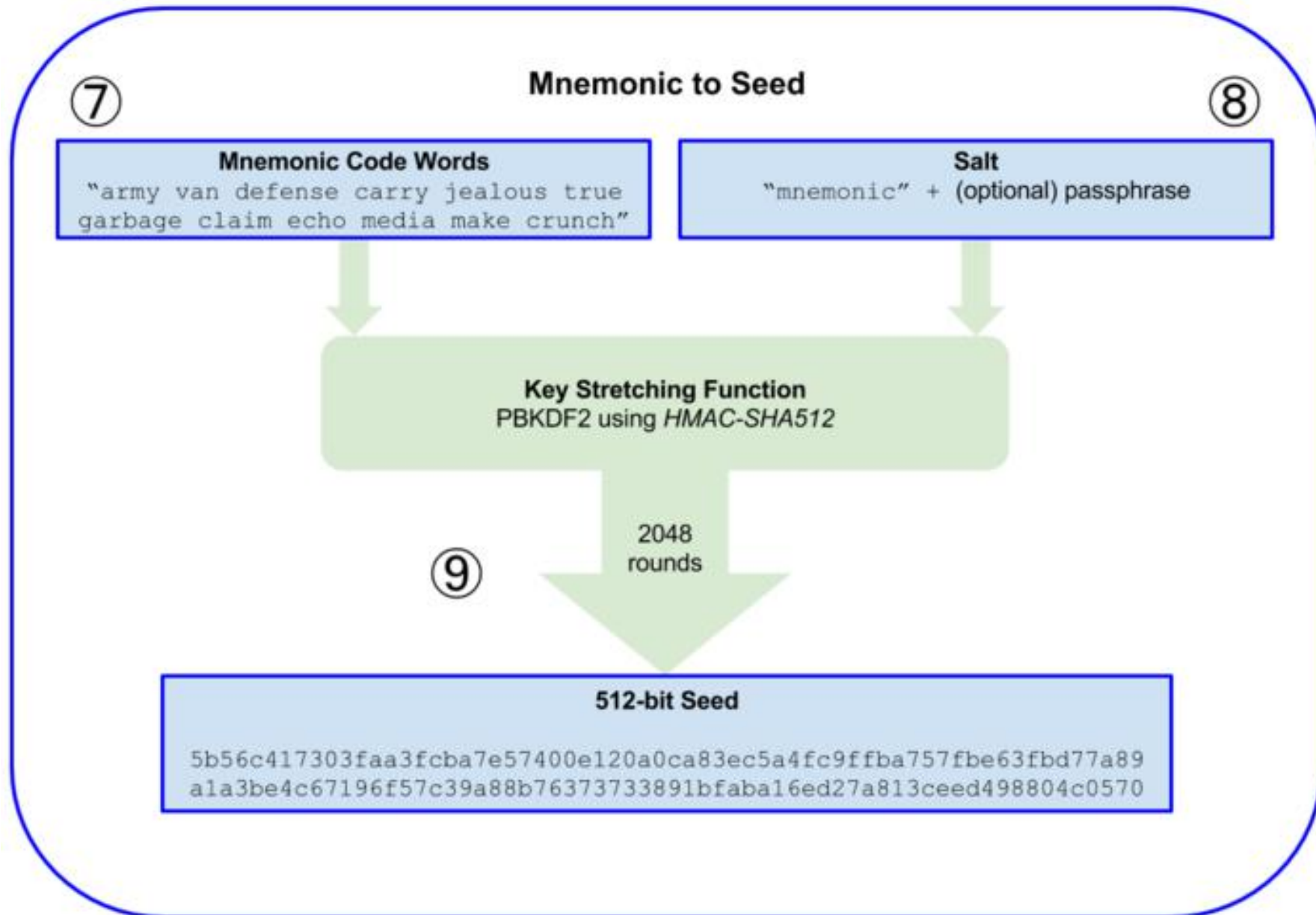
begin to use
the wallet

A stylized illustration of a white smartphone with a blue circular home button at the bottom. The screen is light gray and displays a list of four words stacked vertically: 'abc', 'word', 'sector', and 'good'. The text is in a simple, dark gray sans-serif font.

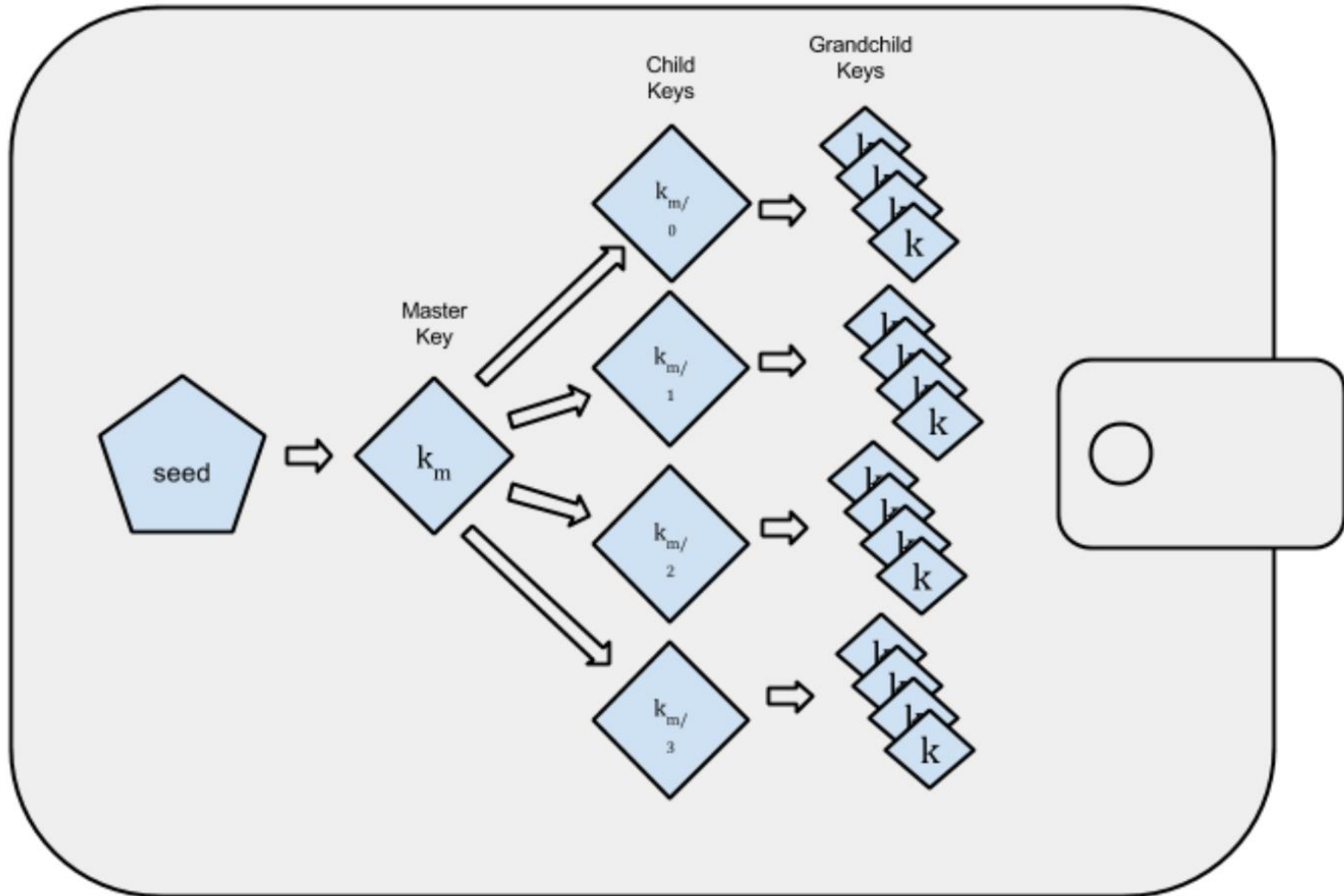
next page



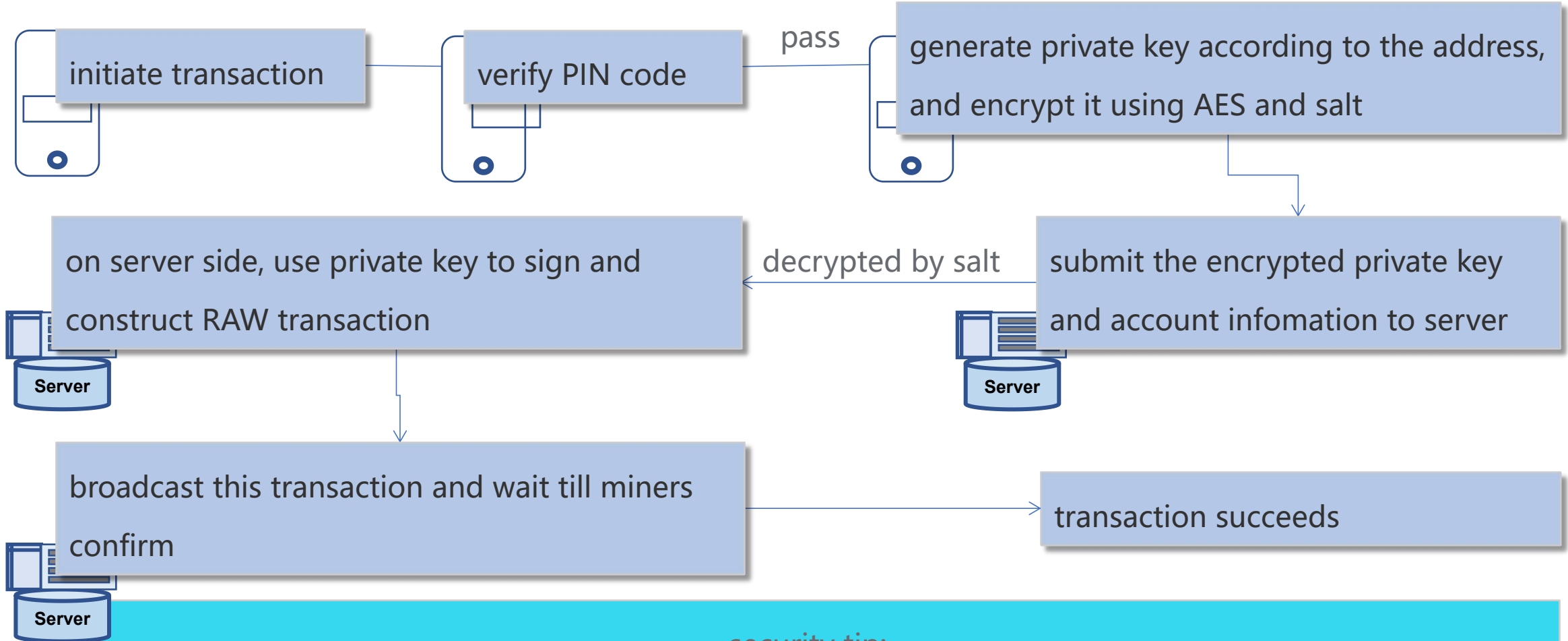
Mnemonic words generate seed



Seed generate addresses and private keys(HD wallet architecture)



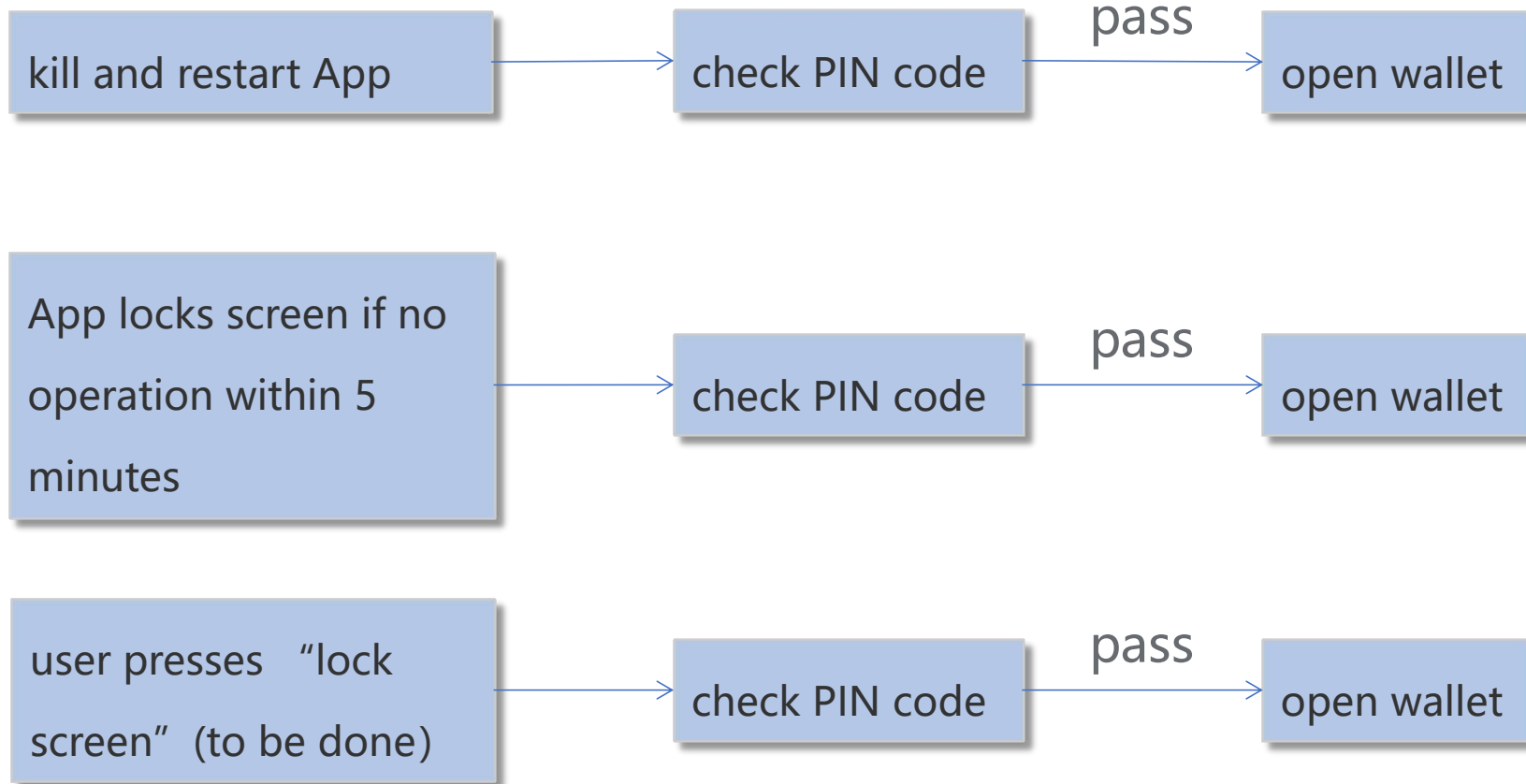
Transaction process



security tip:

private key is generated at the moment that a transaction is created. OmniWallet does not store this key on server or local. This private key is encrypted during communication between mobile side and server side. Even if the data package is intercepted by hackers, it is hard to decrypt the data to get plain text.

Screen locker



security tip:

if user lost his mobile phone, the screen locker will prevent others from accessing the wallet.

Security Assessment

