Smart wallets

Interplay of UX and contract design decisions

Richard Meissner | @rimeissner
Tobias Schubotz | @tschubotz

A brief history of Gnosis smart wallets

Gnosis MultiSig

- 2017 Gnosis prepared their token sale
  - Multiple stakeholders of the company should manage the assets
  - High security requirements

Gnosis MultiSig

- 2017 Gnosis prepared their token sale
  - Multiple stakeholders of the company should manage the assets
  - High security requirements

- Stefan implemented Gnosis MultiSig
  - Configurable threshold to transfer assets (**Multi-factor authentication**)
  - Owners can be changed (**Simple “social” recovery**)
  - Exception rules for asset access (**Daily limit**)

More use cases for asset management

- Gnosis builds **prediction market** platform and **exchange** mechanisms for the outcome token
    - High value assets
    - Lots of contract interactions

More use cases for asset management

- Gnosis builds **prediction market** platform and **exchange** mechanisms for the outcome token
  - High value assets
  - Lots of contract interactions

- Provide same security for prediction market assets as Gnosis MultiSig
  - Multi-factor authentication
  - Recovery logic

More use cases for asset management

- Gnosis builds **prediction market** platform and **exchange** mechanisms for the outcome token
    - High value assets
    - Lots of contract interactions

- Provide same security for prediction market assets as Gnosis MultiSig
    - Multi-factor authentication
    - Recovery logic

- Provide improved contract interaction
    - Reduce gas usage
    - Batched transactions

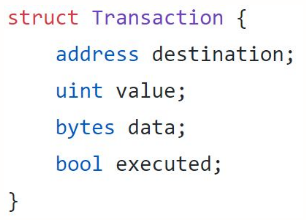
Gnosis Safe

- Reduced gas usage
- Improve security and access control
- Usability improvements

Gnosis Safe - Reduced gas usage

No on-chain transaction information vs all information on-chain

MultiSig



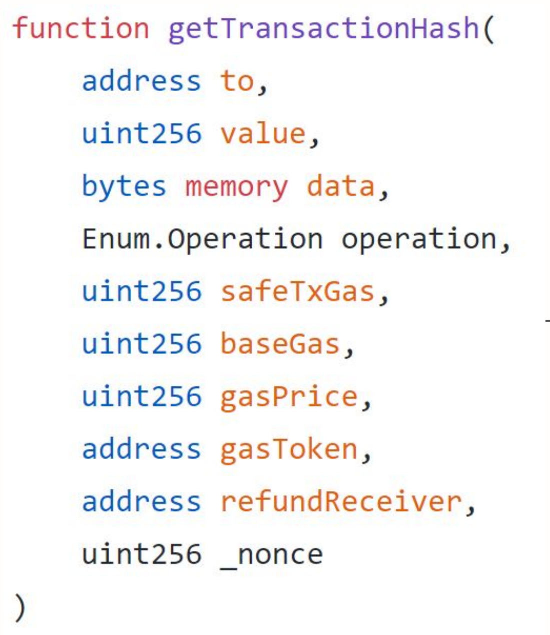
```
struct Transaction {
    address destination;
    uint value;
    bytes data;
    bool executed;
}
```

Safe

- Transaction data needs to be shared off-chain (e.g. IPFS)

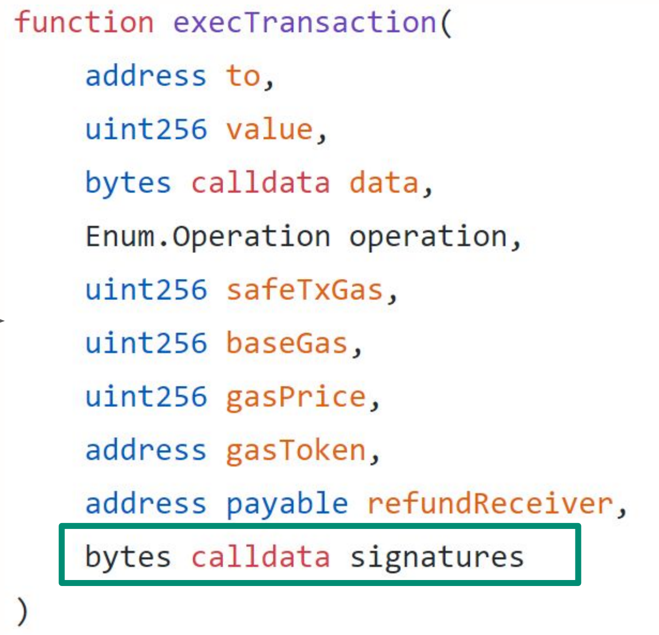
Gnosis Safe - Reduced gas usage

Off-chain confirmation (signatures) vs on-chain confirmation



```
function getTransactionHash(
    address to,
    uint256 value,
    bytes memory data,
    Enum.Operation operation,
    uint256 safeTxGas,
    uint256 baseGas,
    uint256 gasPrice,
    address gasToken,
    address refundReceiver,
    uint256 _nonce
)
```

Combined signatures of transaction hash

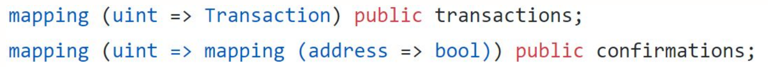


```
function execTransaction(
    address to,
    uint256 value,
    bytes calldata data,
    Enum.Operation operation,
    uint256 safeTxGas,
    uint256 baseGas,
    uint256 gasPrice,
    address gasToken,
    address payable refundReceiver,
    bytes calldata signatures
)
```

Gnosis Safe - Reduced gas usage

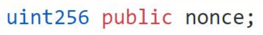
Single on-chain nonce vs mapping of executed transaction

MultiSig



```
mapping (uint => Transaction) public transactions;
mapping (uint => mapping (address => bool)) public confirmations;
```

Safe

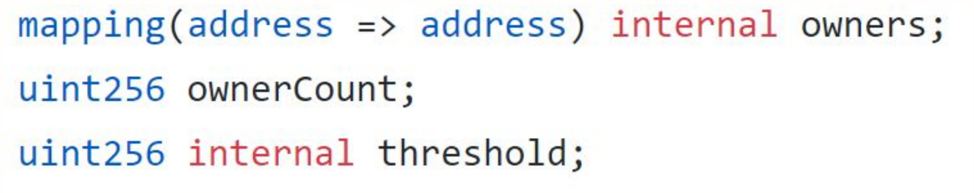


```
uint256 public nonce;
```

Gnosis Safe - Security and access control

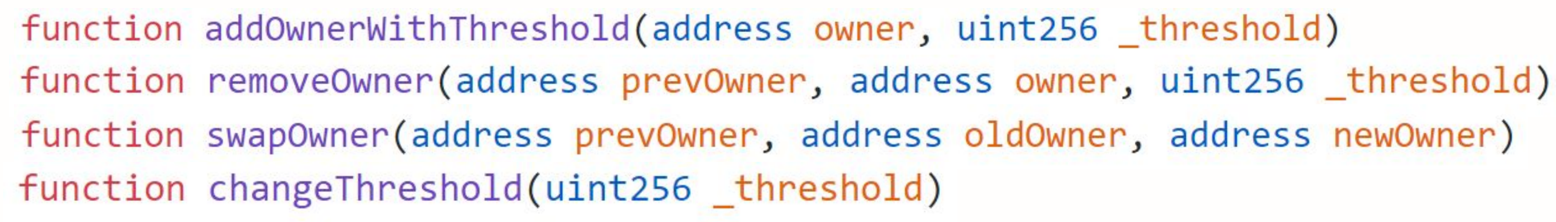
Multi-factor authentication

- Linked-list for owners with threshold



```
mapping(address => address) internal owners;
uint256 ownerCount;
uint256 internal threshold;
```

- Owner management functions

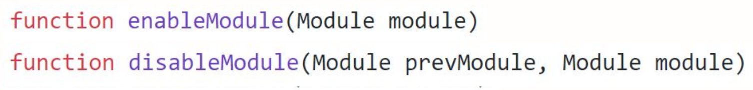


```
function addOwnerWithThreshold(address owner, uint256 _threshold)
function removeOwner(address prevOwner, address owner, uint256 _threshold)
function swapOwner(address prevOwner, address oldOwner, address newOwner)
function changeThreshold(uint256 _threshold)
```

Gnosis Safe - Security and access control

Extendable access logic with modules

- Module management functions

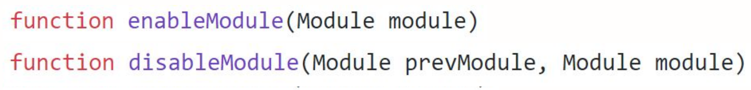


```
function enableModule(Module module)
function disableModule(Module prevModule, Module module)
```

Gnosis Safe - Security and access control

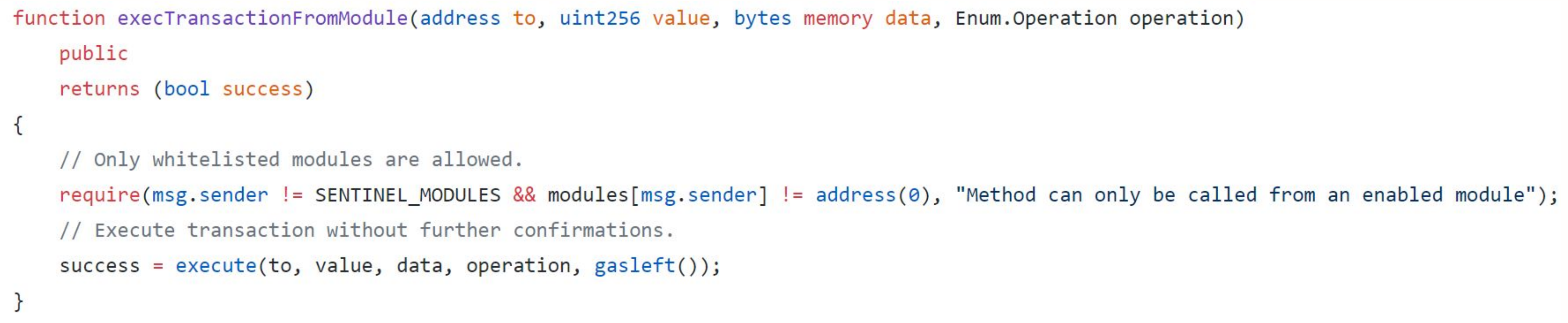
Extendable access logic with modules

- Module management functions



```
function enableModule(Module module)
function disableModule(Module prevModule, Module module)
```

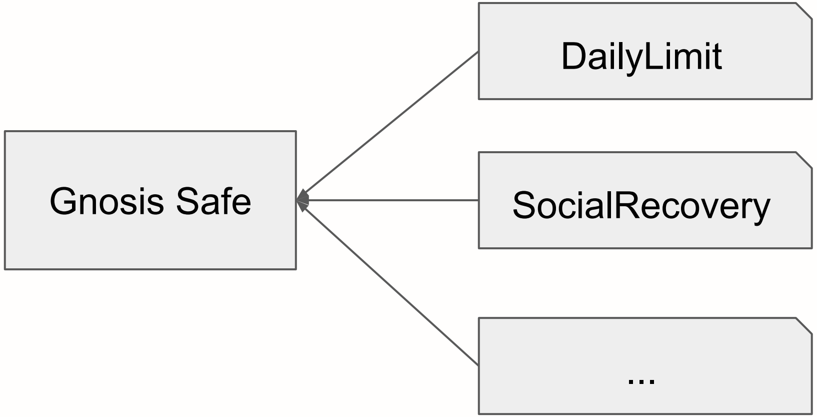
- Module execution function



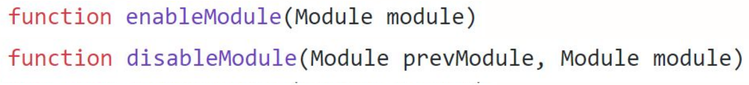
```
function execTransactionFromModule(address to, uint256 value, bytes memory data, Enum.Operation operation)
    public
    returns (bool success)
{
    // Only whitelisted modules are allowed.
    require(msg.sender != SENTINEL_MODULES && modules[msg.sender] != address(0), "Method can only be called from an enabled module");
    // Execute transaction without further confirmations.
    success = execute(to, value, data, operation, gasleft());
}
```

Gnosis Safe - Security and access control

Extendable access logic with modules

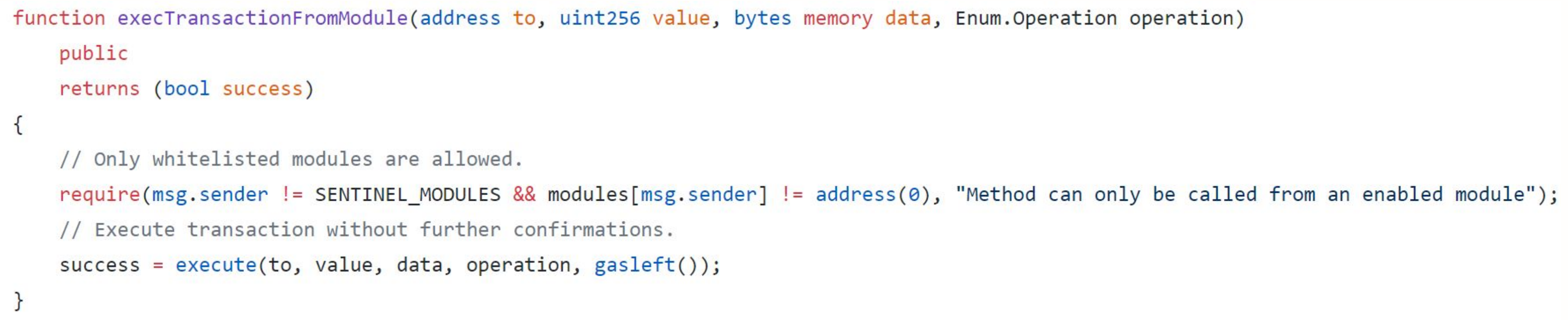


- Module management functions



```
function enableModule(Module module)
function disableModule(Module prevModule, Module module)
```

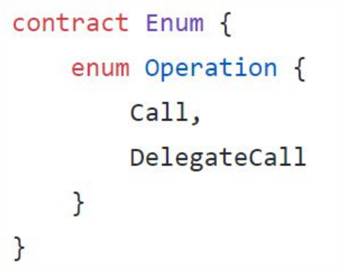
- Module execution function



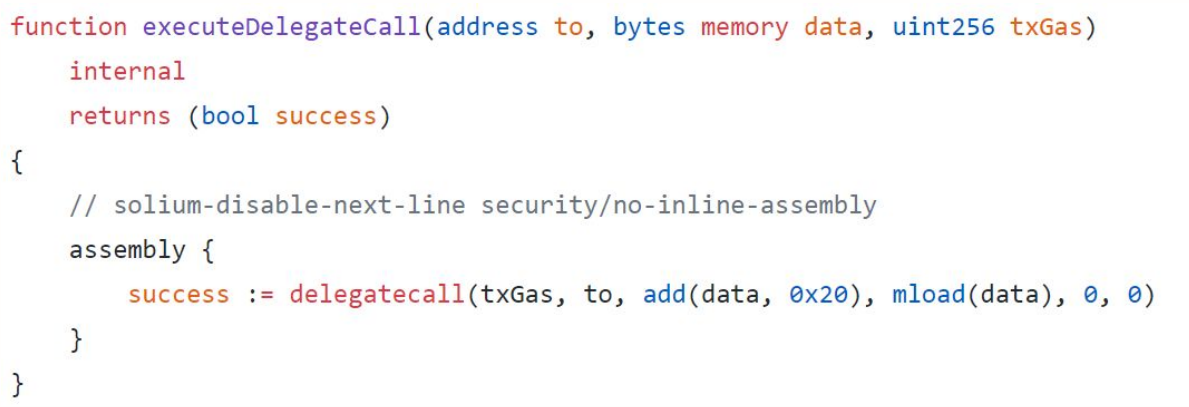
```
function execTransactionFromModule(address to, uint256 value, bytes memory data, Enum.Operation operation)
    public
    returns (bool success)
{
    // Only whitelisted modules are allowed.
    require(msg.sender != SENTINEL_MODULES && modules[msg.sender] != address(0), "Method can only be called from an enabled module");
    // Execute transaction without further confirmations.
    success = execute(to, value, data, operation, gasleft());
}
```

Gnosis Safe - Usability improvements

Extendable execution logic with libraries



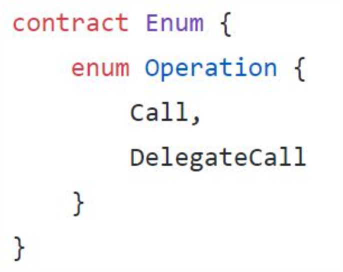
```
contract Enum {
    enum Operation {
        Call,
        DelegateCall
    }
}
```



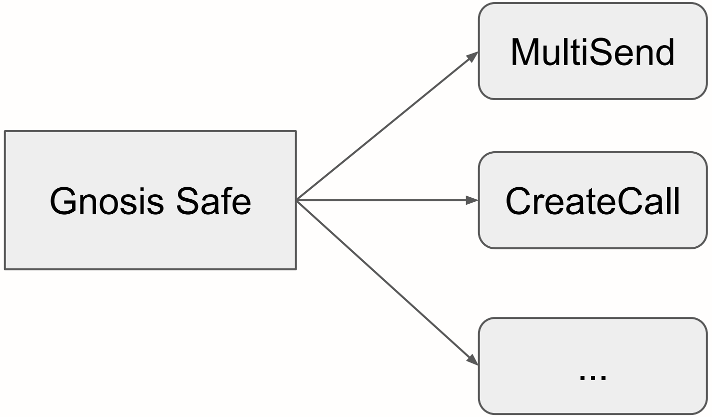
```
function executeDelegateCall(address to, bytes memory data, uint256 txGas)
    internal
    returns (bool success)
{
    // solium-disable-next-line security/no-inline-assembly
    assembly {
        success := delegatecall(txGas, to, add(data, 0x20), mload(data), 0, 0)
    }
}
```

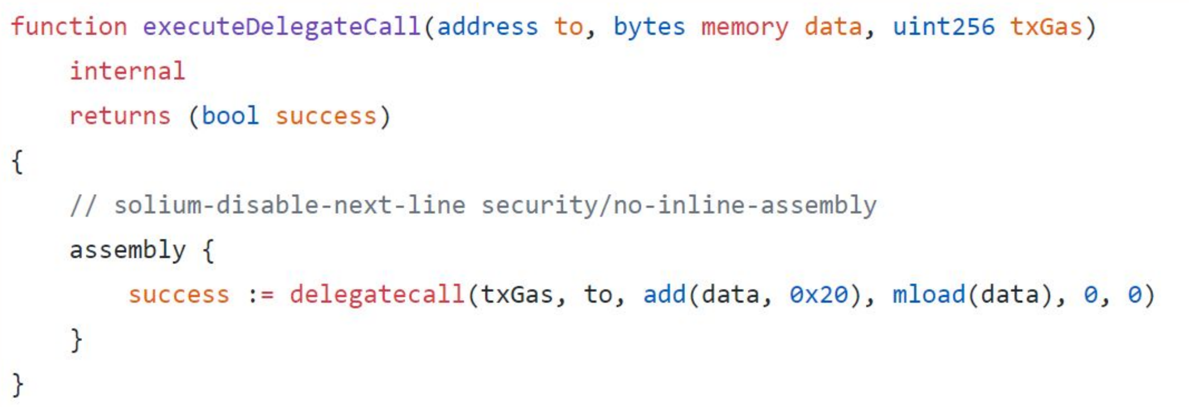
Gnosis Safe - Usability improvements

Extendable execution logic with libraries



```
contract Enum {
    enum Operation {
        Call,
        DelegateCall
    }
}
```

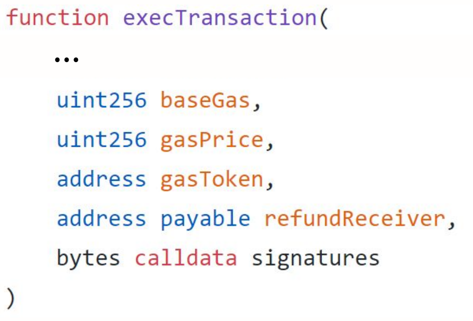




```
function executeDelegateCall(address to, bytes memory data, uint256 txGas)
    internal
    returns (bool success)
{
    // solium-disable-next-line security/no-inline-assembly
    assembly {
        success := delegatecall(txGas, to, add(data, 0x20), mload(data), 0, 0)
    }
}
```

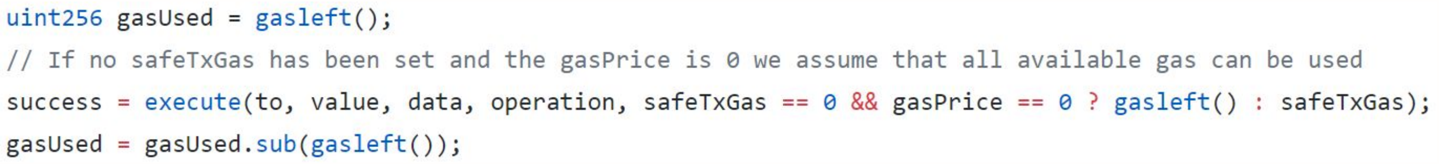
Gnosis Safe - Usability improvements

Payment option for **meta transaction**



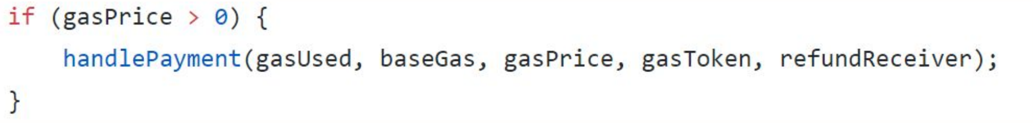
```
function execTransaction(
    ...
    uint256 baseGas,
    uint256 gasPrice,
    address gasToken,
    address payable refundReceiver,
    bytes calldata signatures
)
```

...



```
uint256 gasUsed = gasleft();
// If no safeTxGas has been set and the gasPrice is 0 we assume that all available gas can be used
success = execute(to, value, data, operation, safeTxGas == 0 && gasPrice == 0 ? gasleft() : safeTxGas);
gasUsed = gasUsed.sub(gasleft());
```

...

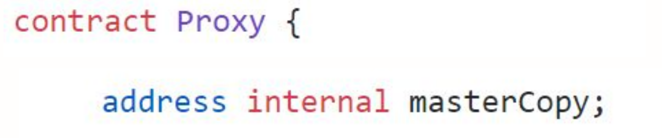


```
if (gasPrice > 0) {
    handlePayment(gasUsed, baseGas, gasPrice, gasToken, refundReceiver);
}
```

Gnosis Safe - Usability improvements

Upgradability with proxies

- Master copy address defined in Proxy and master copy

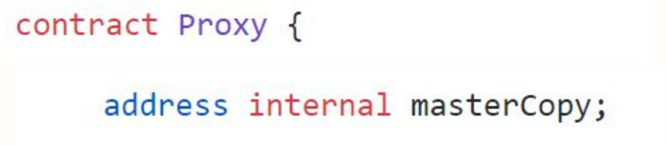


```
contract Proxy {

     address internal masterCopy;
```

Gnosis Safe - Usability improvements

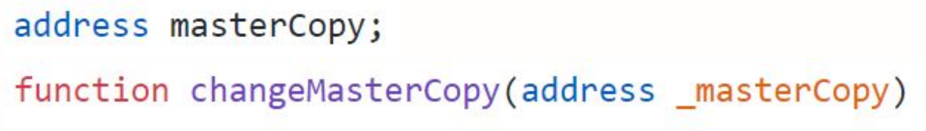
Upgradability with proxies

- Master copy address defined in Proxy and master copy



```
contract Proxy {
     address internal masterCopy;
```

- Functions to update master copy in master copy

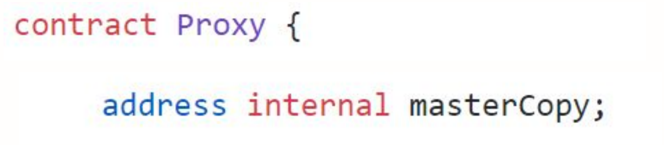


```
address masterCopy;
function changeMasterCopy(address _masterCopy)
```

Gnosis Safe - Usability improvements

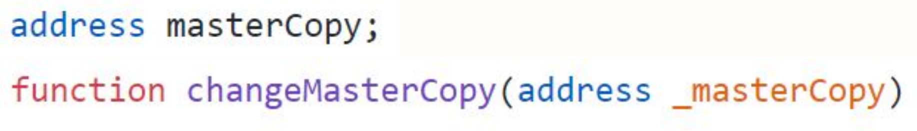
Upgradability with proxies

- Master copy address defined in Proxy and master copy

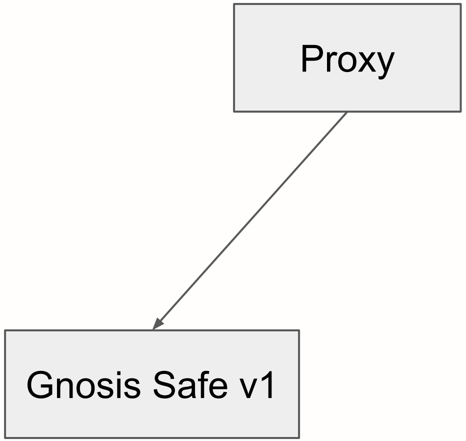


```
contract Proxy {
     address internal masterCopy;
```

- Functions to update master copy in master copy



```
address masterCopy;
function changeMasterCopy(address _masterCopy)
```



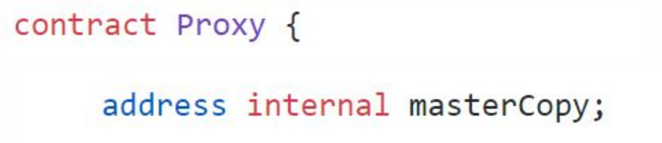
Proxy

Gnosis Safe v1

Gnosis Safe - Usability improvements

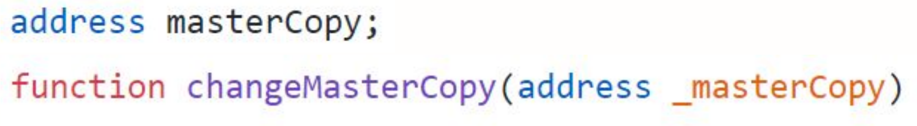
Upgradability with proxies

- Master copy address defined in Proxy and master copy

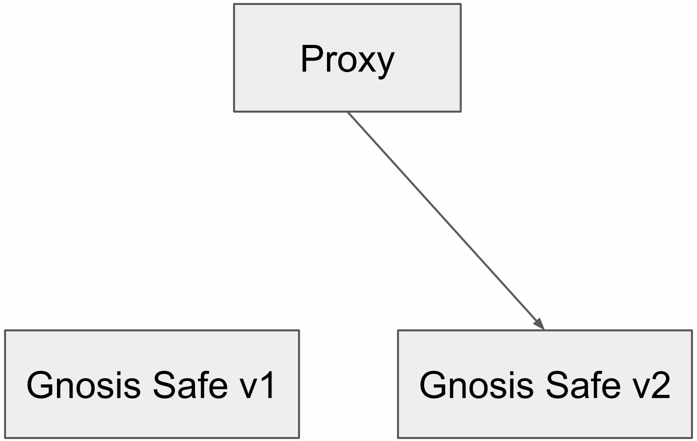


```
contract Proxy {

     address internal masterCopy;
```

- Functions to update master copy in master copy



```
address masterCopy;

function changeMasterCopy(address _masterCopy)
```



Contract summary

Gnosis MultiSig

- High gas usage
  - All information on-chain
  - Only on-chain confirmation

Gnosis Safe

- Optimized gas usage
  - No on-chain information
  - Confirmation via signatures

Contract summary

Gnosis MultiSig

- High gas usage
  - All information on-chain
  - Only on-chain confirmation

- Not extendable
  - Special version with daily limit
  - No libraries

Gnosis Safe

- Optimized gas usage
  - No on-chain information
  - Confirmation via signatures

- Extendable
  - Modules for advanced access logic
  - Library for advanced execution logic

Contract summary

Gnosis MultiSig

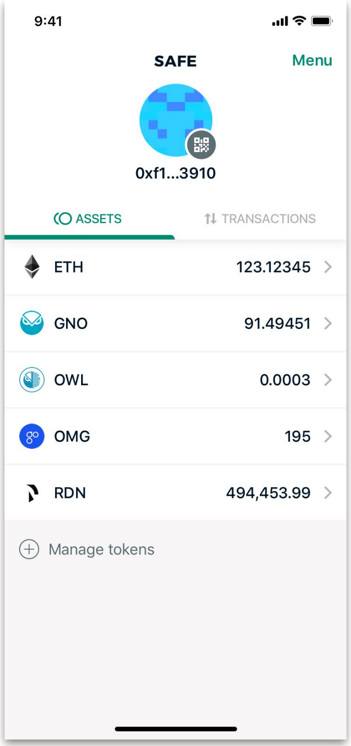
- High gas usage
  - All information on-chain
  - Only on-chain confirmation
- Not extendable
  - Special version with daily limit
  - No libraries
- Advanced Ethereum knowledge required
  - Account with ETH required
  - Knowledge about gas prices required

Gnosis Safe

- Reduced gas usage
  - No on-chain information
  - Confirmation via signatures
- Extendable
  - Modules for advanced access logic
  - Library for advanced execution logic
- No Ethereum knowledge required
  - No additional account with ETH required
  - Gas prices can be abstracted

Impact of contract design decisions on UX: Gnosis Safe & Gnosis Safe *for Teams*

Gnosis Safe *mobile apps* - For individuals



9:41

SAFE

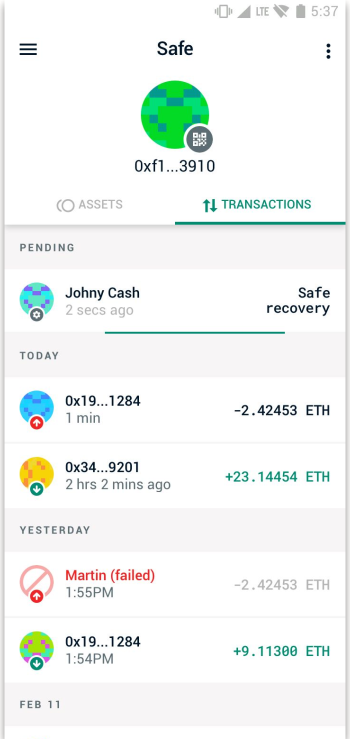
Menu

0xf1...3910

ASSETS | TRANSACTIONS

ETH	123.12345
GNO	91.49451
OWL	0.0003
OMG	195
RDN	494,453.99

Manage tokens



LTE 5:37

Safe

0xf1...3910

ASSETS | TRANSACTIONS

PENDING

Johny Cash 2 secs ago	Safe recovery

TODAY

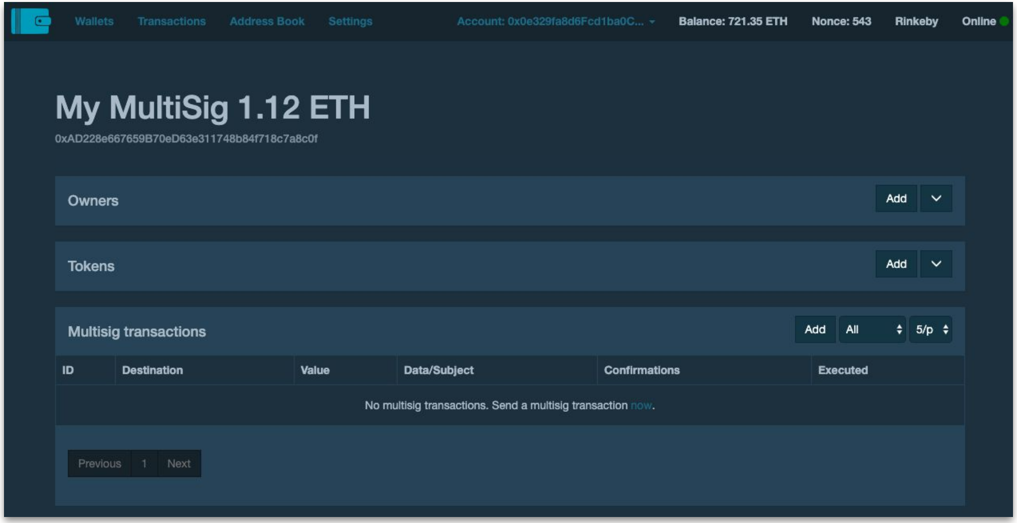
0x19...1284 1 min	-2.42453 ETH
0x34...9201 2 hrs 2 mins ago	+23.14454 ETH

YESTERDAY

Martin (failed) 1:55PM	-2.42453 ETH
0x19...1284 1:54PM	+9.11300 ETH

FEB 11

Gnosis Safe *for Teams* - Manage crypto funds collectively



Balance: 721.35 ETH Nonce: 543 Rinkeby Online

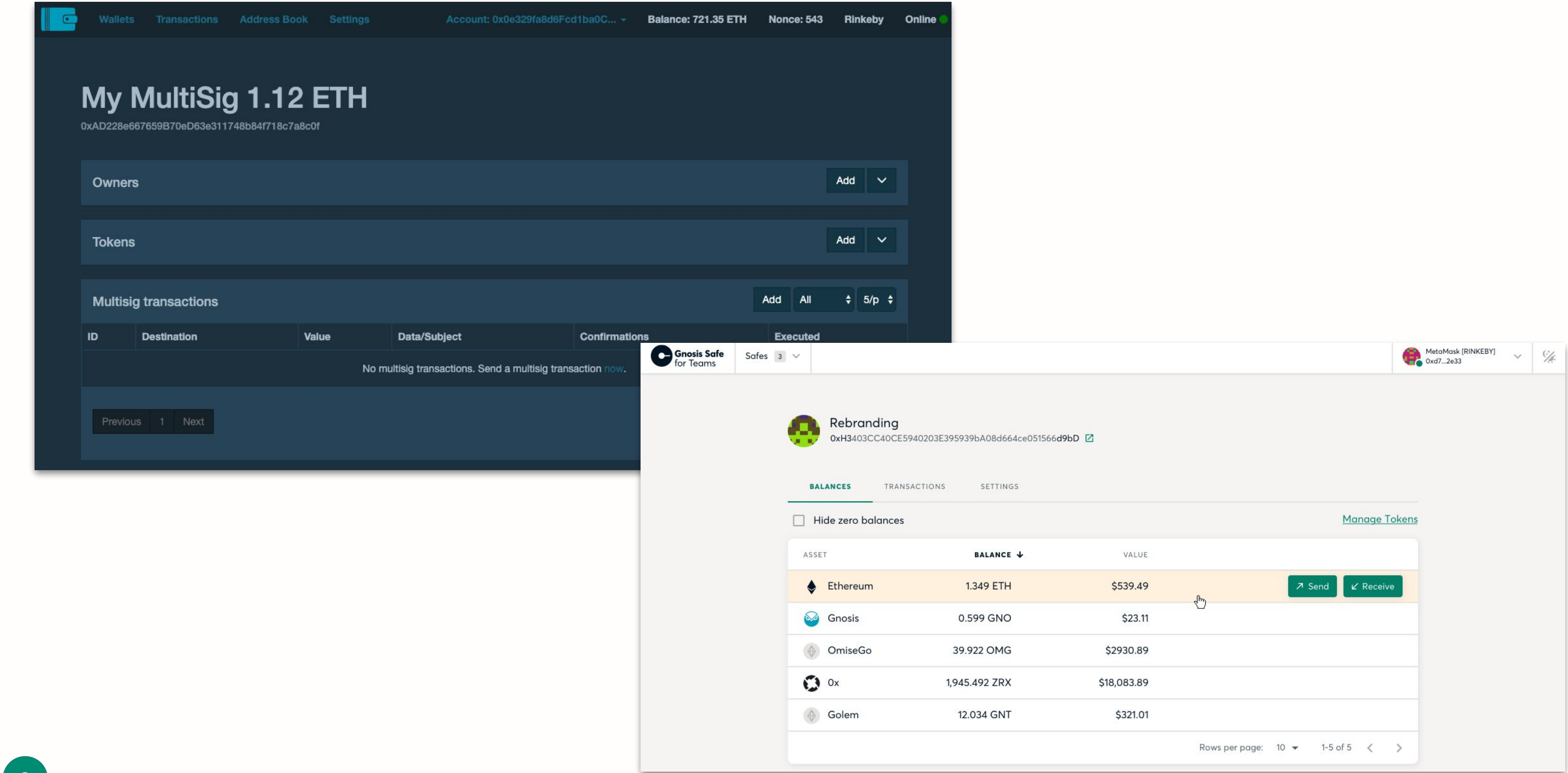
My MultiSig 1.12 ETH

0xAD228e667659B70eD63e311748b84f718c7a8c0f

ID	Destination	Value	Data/Subject	Confirmations	Executed

No multisig transactions. Send a multisig transaction now.

Gnosis Safe *for Teams* - Manage crypto funds collectively



My MultiSig 1.12 ETH

0xAD228e667659B70eD63e311748b84f718c7a8c0f

ID	Destination	Value	Data/Subject	Confirmations	Executed

No multisig transactions. Send a multisig transaction now.

Rebranding

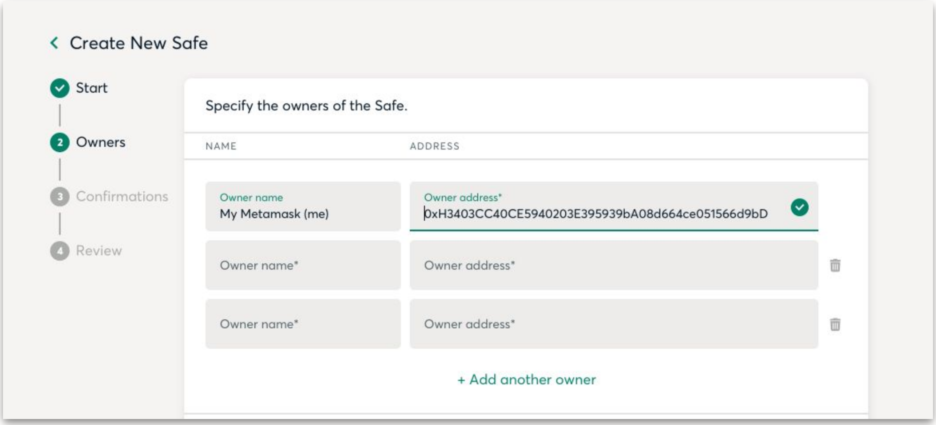
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

□ Hide zero balances

ASSET	BALANCE ↓	VALUE	
Ethereum	1.349 ETH	$539.49	↗ Send ↙ Receive
Gnosis	0.599 GNO	$23.11	
OmiseGo	39.922 OMG	$2930.89	
0x	1,945.492 ZRX	$18,083.89	
Golem	12.034 GNT	$321.01	

Rows per page: 10 1-5 of 5

Gnosis Safe *for Teams* - Flexibility & full control

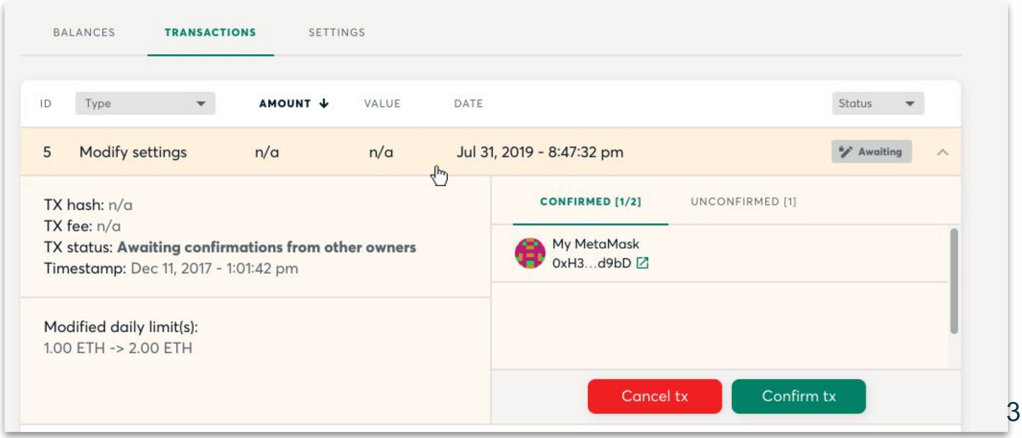


Create New Safe

1. Start
2. Owners
3. Confirmations
4. Review

Specify the owners of the Safe.

NAME	ADDRESS
Owner name My Metamask (me)	Owner address* 0xH3403CC40CE5940203E395939bA08d664ce051566d9bD ✓
Owner name*	Owner address*
Owner name*	Owner address*



ID	Type	AMOUNT ↓	VALUE	DATE	Status
5	Modify settings	n/a	n/a	Jul 31, 2019 - 8:47:32 pm	Awaiting

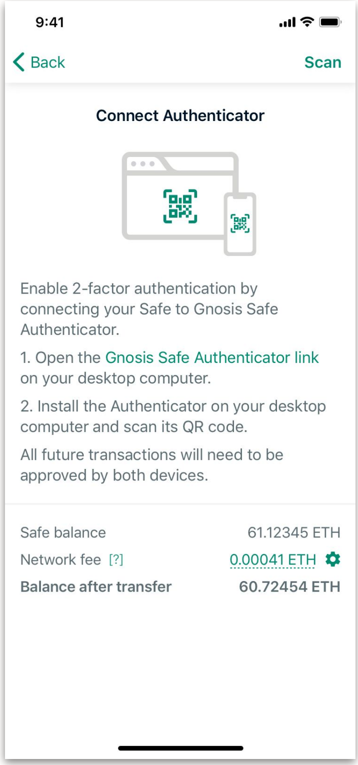
TX hash: n/a
TX fee: n/a
TX status: **Awaiting confirmations from other owners**
Timestamp: Dec 11, 2017 - 1:01:42 pm

Modified daily limit(s):
1.00 ETH -> 2.00 ETH

CONFIRMED [1/2] UNCONFIRMED [1]

My MetaMask
0xH3...d9bD

Gnosis Safe - 2FA & Only necessary info



Connect Authenticator

Enable 2-factor authentication by connecting your Safe to Gnosis Safe Authenticator.

1. Open the Gnosis Safe Authenticator link on your desktop computer.

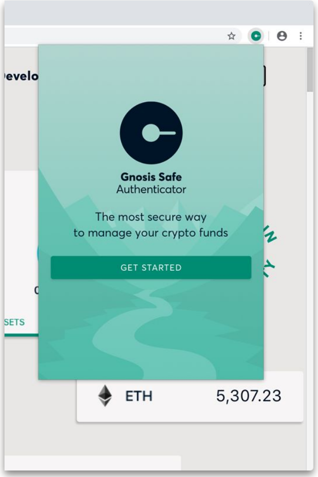
2. Install the Authenticator on your desktop computer and scan its QR code.

All future transactions will need to be approved by both devices.

Safe balance	61.12345 ETH
Network fee [?]	0.00041 ETH
Balance after transfer	**60.72454 ETH**

Mobile app

+

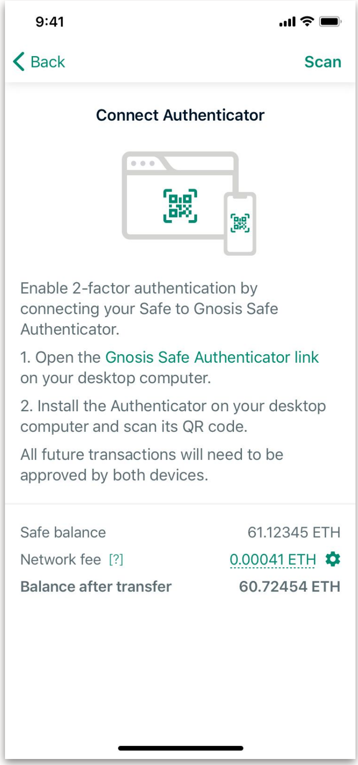


Gnosis Safe Authenticator

The most secure way to manage your crypto funds

Browser extension

Gnosis Safe - 2FA & Only necessary info


9:41

Back Scan

Connect Authenticator

Enable 2-factor authentication by connecting your Safe to Gnosis Safe Authenticator.

1. Open the Gnosis Safe Authenticator link on your desktop computer.

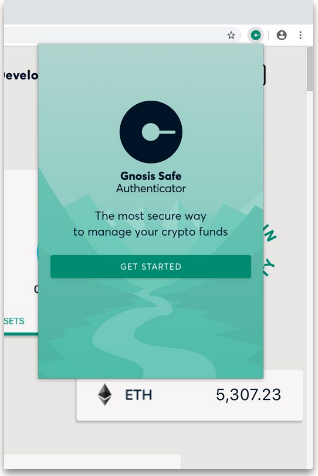
2. Install the Authenticator on your desktop computer and scan its QR code.

All future transactions will need to be approved by both devices.

Safe balance	61.12345 ETH
Network fee [?]	0.00041 ETH
Balance after transfer	**60.72454 ETH**

Mobile app

+

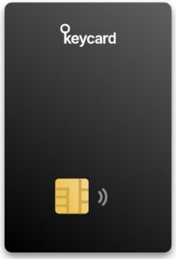

Gnosis Safe Authenticator

The most secure way to manage your crypto funds

GET STARTED

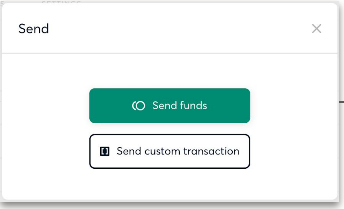
ETH	5,307.23

Browser extension



Hardware wallets

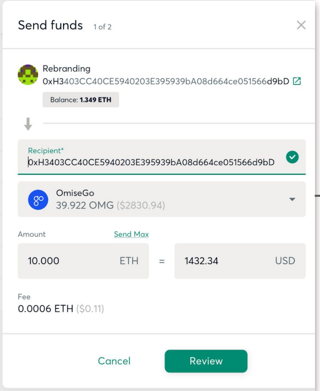
Transactions with the Gnosis Safe *for Teams*



Send

Send funds

Send custom transaction



Send funds 1 of 2

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Balance: **1.349 ETH**

Recipient*
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

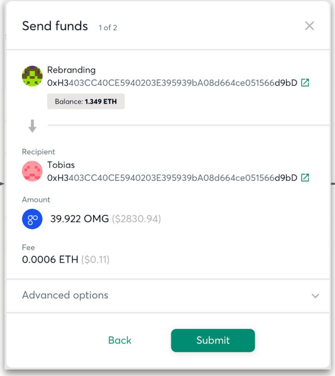
OmiseGo
39.922 OMG ($2830.94)

Amount — Send Max

10.000 ETH = 1432.34 USD

Fee
0.0006 ETH ($0.11)

Cancel — Review



Send funds 1 of 2

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Balance: **1.349 ETH**

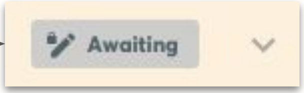
Recipient
Tobias
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Amount
39.922 OMG ($2830.94)

Fee
0.0006 ETH ($0.11)

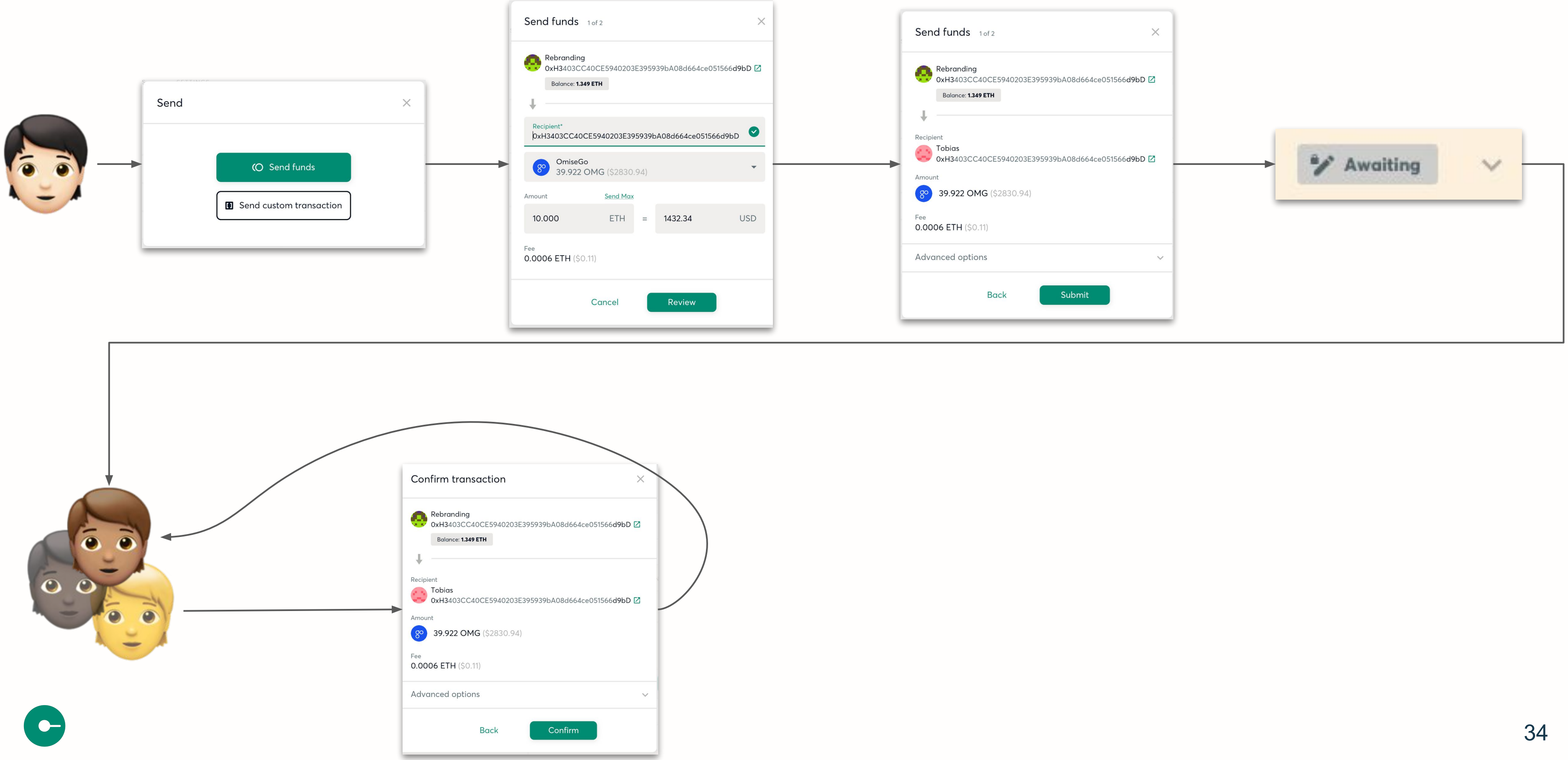
Advanced options

Back — Submit



Awaiting

Transactions with the Gnosis Safe *for Teams*



Send

Send funds

Send custom transaction

Send funds 1 of 2

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD
Balance: **1.349 ETH**

Recipient*
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

OmiseGo
39.922 OMG ($2830.94)

Amount Send Max
10.000 ETH = 1432.34 USD

Fee
0.0006 ETH ($0.11)

Cancel Review

Send funds 1 of 2

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD
Balance: **1.349 ETH**

Recipient
Tobias
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Amount
39.922 OMG ($2830.94)

Fee
0.0006 ETH ($0.11)

Advanced options

Back Submit

Awaiting

Confirm transaction

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD
Balance: **1.349 ETH**

Recipient
Tobias
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

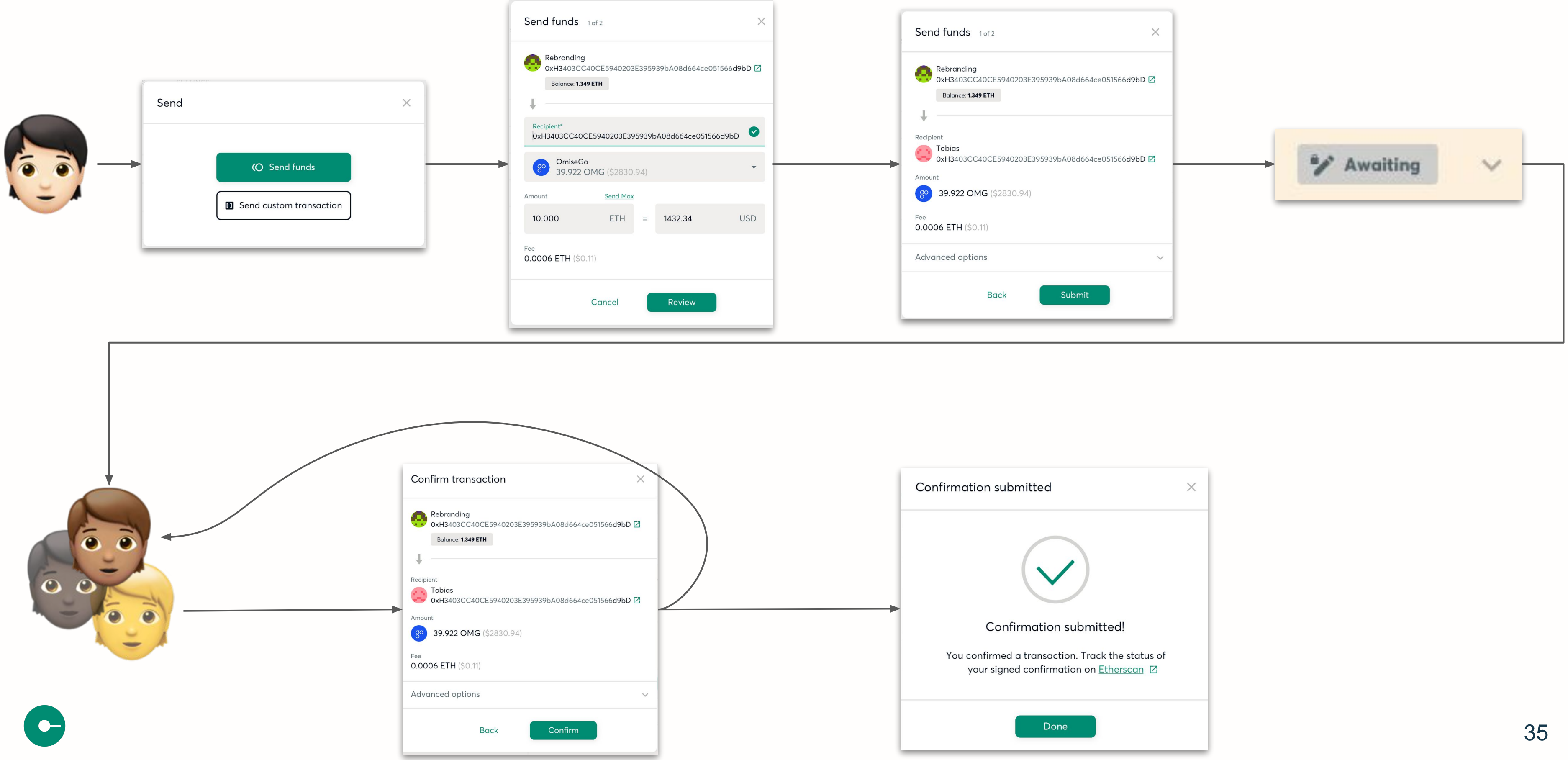
Amount
39.922 OMG ($2830.94)

Fee
0.0006 ETH ($0.11)

Advanced options

Back Confirm

Transactions with the Gnosis Safe *for Teams*



Send

Send funds

Send custom transaction

Send funds 1 of 2

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Balance: 1.349 ETH

Recipient*
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

OmiseGo
39.922 OMG ($2830.94)

Amount Send Max

10.000 ETH = 1432.34 USD

Fee
0.0006 ETH ($0.11)

Cancel Review

Send funds 1 of 2

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Balance: 1.349 ETH

Recipient
Tobias
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Amount
39.922 OMG ($2830.94)

Fee
0.0006 ETH ($0.11)

Advanced options

Back Submit

Awaiting

Confirm transaction

Rebranding
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Balance: 1.349 ETH

Recipient
Tobias
0xH3403CC40CE5940203E395939bA08d664ce051566d9bD

Amount
39.922 OMG ($2830.94)

Fee
0.0006 ETH ($0.11)

Advanced options

Back Confirm

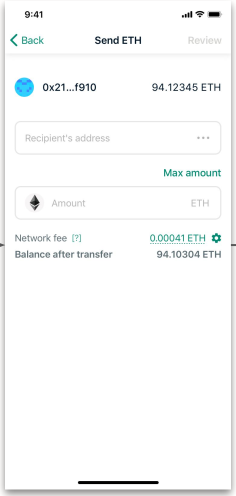
Confirmation submitted

Confirmation submitted!

You confirmed a transaction. Track the status of your signed confirmation on Etherscan

Done

Transactions with the Gnosis Safe



9:41

Back | Send ETH | Review

0x21...f910 94.12345 ETH

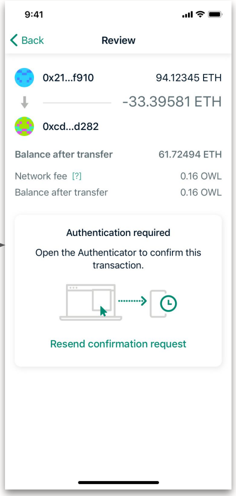
Recipient's address ···

Max amount

Amount ETH

Network fee [?] 0.00041 ETH

Balance after transfer 94.10304 ETH



9:41

Back | Review

0x21...f910 94.12345 ETH

-33.39581 ETH

0xcd...d282

Balance after transfer 61.72494 ETH

Network fee [?] 0.16 OWL

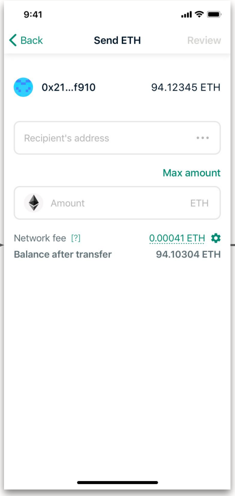
Balance after transfer 0.16 OWL

Authentication required

Open the Authenticator to confirm this transaction.

Resend confirmation request

Transactions with the Gnosis Safe



9:41

Back Send ETH Review

0x21...f910 94.12345 ETH

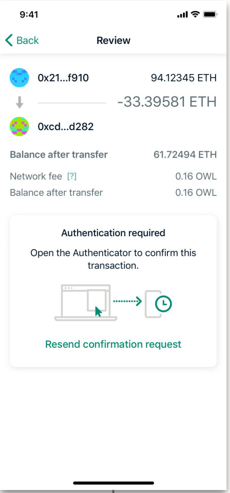
Recipient's address

Max amount

Amount ETH

Network fee [?] 0.00041 ETH

Balance after transfer 94.10304 ETH



9:41

Back Review

0x21...f910 94.12345 ETH

-33.39581 ETH

0xcd...d282

Balance after transfer 61.72494 ETH

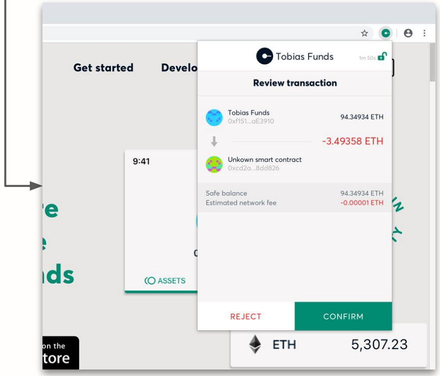
Network fee [?] 0.16 OWL

Balance after transfer 0.16 OWL

Authentication required

Open the Authenticator to confirm this transaction.

Resend confirmation request



Tobias Funds 1m 50s

Review transaction

Tobias Funds 0xf151...aE3910 94.34934 ETH

-3.49358 ETH

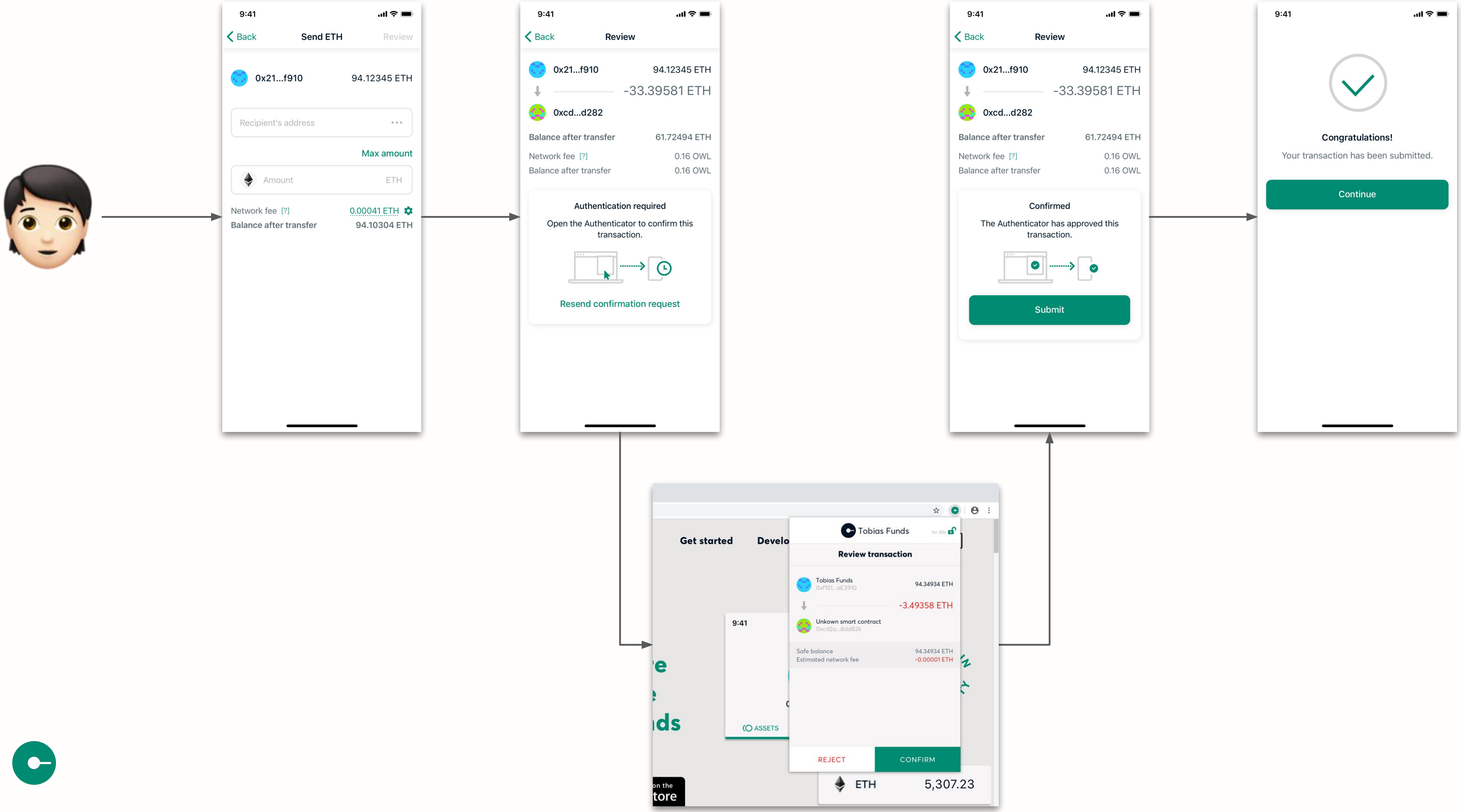
Unkown smart contract 0xcd2a...8dd826

Safe balance 94.34934 ETH

Estimated network fee -0.00001 ETH

REJECT CONFIRM

Transactions with the Gnosis Safe



9:41

Back | Send ETH | Review

0x21...f910 94.12345 ETH

Recipient's address

Max amount

Amount ETH

Network fee [?] 0.00041 ETH

Balance after transfer 94.10304 ETH

9:41

Back | Review

0x21...f910 94.12345 ETH

-33.39581 ETH

0xcd...d282

Balance after transfer 61.72494 ETH

Network fee [?] 0.16 OWL

Balance after transfer 0.16 OWL

Authentication required

Open the Authenticator to confirm this transaction.

Resend confirmation request

Get started Develo

Tobias Funds 1m 50s

Review transaction

Tobias Funds 0xf151...aE3910 94.34934 ETH

-3.49358 ETH

Unkown smart contract 0xcd2a...8dd826

Safe balance 94.34934 ETH

Estimated network fee -0.00001 ETH

REJECT | CONFIRM

9:41

ASSETS

ETH 5,307.23

9:41

Back | Review

0x21...f910 94.12345 ETH

-33.39581 ETH

0xcd...d282

Balance after transfer 61.72494 ETH

Network fee [?] 0.16 OWL

Balance after transfer 0.16 OWL

Confirmed

The Authenticator has approved this transaction.

Submit

9:41

Congratulations!

Your transaction has been submitted.

Continue

What are current challenges for smart wallets?

Why haven’t smart wallets seen more adoption?

- Smart contract wallets are still relatively new
- Users are more comfortable with what they were first presented

Why haven’t smart wallets seen more adoption?

- Smart contract wallets are still relatively new
- Users are more comfortable with what they were first presented
- “It won’t happen to me” syndrome
- Fears over security (Parity multi-sig hack)
  - Gnosis Safe has been audited and formally verified
  - Trust will come with time

Why haven’t smart wallets seen more adoption?

- Smart contract wallets are still relatively new
- Users are more comfortable with what they were first presented
- “It won’t happen to me” syndrome
- Fears over security (Parity multi-sig hack)
  - Gnosis Safe has been audited and formally verified
  - Trust will come with time
- **Full potential not yet leveraged**

Features unique to smart wallets

Features unique to smart wallets

- Improved access control:
  - Multi-factor authentication

Features unique to smart wallets

- Improved access control:
  - Multi-factor authentication
  - Transfer limits
  - Whitelists

Features unique to smart wallets

- Improved access control:
  - Multi-factor authentication
  - Transfer limits
  - Whitelists
  - Seedless recovery

Features unique to smart wallets

- Improved access control:
  - Multi-factor authentication
  - Transfer limits
  - Whitelists
  - Seedless recovery
- Allow 3rd parties to submit transactions (“Meta transactions”)
  - “Gas less” transactions / let dapps pay fees
  - Pay transaction fees in ETH or ERC20 tokens

Features unique to smart wallets

- Improved access control:
  - Multi-factor authentication
  - Transfer limits
  - Whitelists
  - Seedless recovery
- Allow 3rd parties to submit transactions (“Meta transactions”)
  - “Gas less” transactions / let dapps pay fees
  - Pay transaction fees in ETH or ERC20 tokens
- Simplified interaction with other contracts
  - Batching of transactions

Gnosis Safe

https://safe.gnosis.io

Richard Meissner | @rimeissner
Tobias Schubotz | @tschubotz