



FORECAST THE FUTURE



CONSENSYS

Stefan George,
CTO, Gnosis



<https://gnosis.pm>

New multisig wallet

- Multisig transactions
 - Multiple parties have to agree on a transaction before execution.
- Cold storage
 - Keeping keys offline, signing transactions offline.

Why?

- Ethereum Foundation Multisig Wallet
 - Battle tested: > 1M ETH (>10M USD)
 - No multisig for non ETH transactions
- Token market cap will soon pass ETH (USD token, App-token, ...)
- Ether as a token (EIP 101)

```
344 function execute(address _to, uint _value, bytes _data) external onlyowner returns (bytes32 _r) {
345     // first, take the opportunity to check that we're under the daily limit.
346     if (underLimit(_value)) {
347         SingleTransact(msg.sender, _value, _to, _data);
348         // yes - just execute the call.
349         _to.call.value(_value)(_data);
350         return 0;
351     }
```

Security bad practice



LOGIN

Search by Address / Txhash / Block / Token

GO

LANGUAGE

HOME

BLOCKCHAIN

ACCOUNT

TOKEN

CHART

MISC



All Accounts

Home / Accounts

A total of 1047794 accounts found (88,804,117.217 Ether)

Displaying the last 100000 records only

First Prev Page 1 of 4000 Next Last

Rank	Address	Balance	Percentage	TxCount ↓
1	0xb794f5ea0ba39494ce839613ffba74279579268 (Poloniex ColdWallet)	6,224,999.825933404787792424 Ether	7.00980993%	385
2	0xe853c56864a2ebe4576a807d26fdc4a0ada51919 (Kraken_3)	6,149,328.000424 Ether	6.92459786%	81
3	 0xab7c74abc0c4d48d1bdad5dcb26153fc8780f83e	2,900,000.00413797094280789 Ether	3.26561436%	167
4	0x53d284357ec70ce289d6d64134dfac8e511c8a3d	1,378,753.086041281477994073 Ether	1.55257789%	14985
5	 0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae (EthDev)	1,081,460.563608465139479303 Ether	1.21780453%	301
6	0xd56d423cdc0e437babbdff79c4fa38904ff8d128	898,999.99616 Ether	1.01234045%	6
7	0x6f46cf5569aefa1acc1009290c8e043747172d89	857,808.408072454767876554 Ether	0.96595567%	281

Security

- Multiple security audits
 - ConsenSys internal by Joseph Chow
 - Initiated by EF, conducted by Martin Holst Swende
- Bug bounties
 - Gnosis bug bounty
 - Weifund bug bounty
- A previous version was used by Golem



User interface

Security can be ensured only if a user is aware of the result of his own interactions.

- Bytecode is not human readable
- 460+ transactions to 0x0 address with \$70,000 worth of ETH
- Investments sent to token contract instead of sale contract (SDTV)
- No comprehensive UI for multisig transactions available until today

DEMO

Future work/Work in progress

- Integration of Ledger- & Trezor wallet & uPort
- Automation of ABI loading
- Alerts: Get email notification when new transaction was submitted/confirmed/executed
- Separation of account management from Ethereum node



<https://github.com/ConsenSys/MultiSigWallet>





<https://wallet.gnosis.pm>

GET YOUR MONEY OFF CENTRALIZED EXCHANGES!