



Secure wallet and storage solutions

JP Aumasson, Head of Security

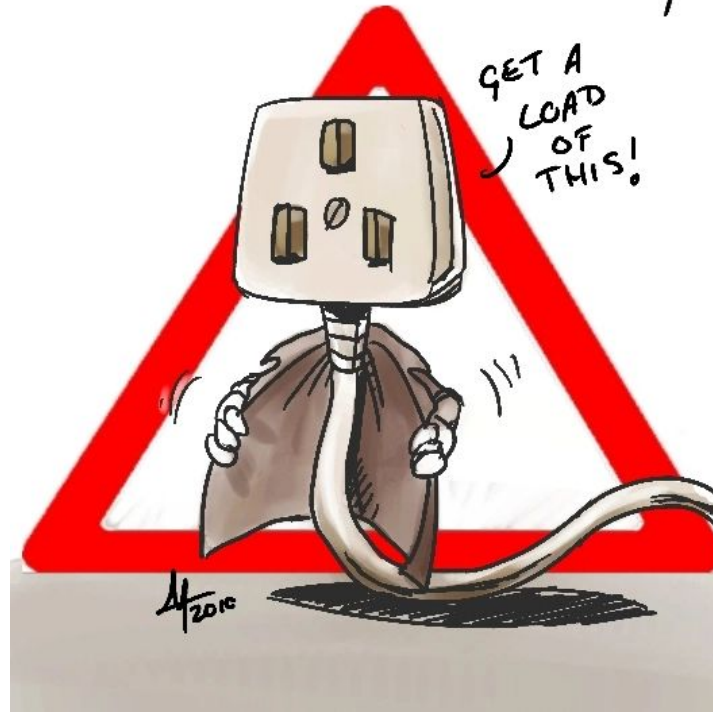


Secure wallet and storage solutions

JP Aumasson, Head of Security



WARNING!
SHAMELESS PLUG



BUY OUR PRODUCT




This is the slide about the company, Taurus Group SA

- Founded in Geneva in April 2018, by team of four: private banker, hedge fund manager, lawyer, crypto guy; F&F initial funding
- Now more than 10 persons, mostly engineers, among the best in CH
- We have customers too!

This is the slide about the company, Taurus Group SA

- Founded in Geneva in April 2018, by team of four: private banker, hedge fund manager, lawyer, crypto guy; F&F initial funding
- Now more than 10 persons, mostly engineers, among the best in CH
- We have customers too!



TRADE

*Digital asset trading
platform and
services*

Broker for private investors

Dealing desk for institutional
investors (incl. ICO cash-out)

This is the slide about the company, Taurus Group SA

- Founded in Geneva in April 2018, by team of four: private banker, hedge fund manager, lawyer, crypto guy; F&F initial funding
- Now more than 10 persons, mostly engineers, among the best in CH
- We have customers too!



TRADE

Digital asset trading platform and services

Broker for private investors

Dealing desk for institutional investors (incl. ICO cash-out)



INVEST

Advisory in digital assets & blockchain investing

Digital asset research incl. technology assessment

Structured products / collective investment schemes

Securitization / tokenization of assets

This is the slide about the company, Taurus Group SA

- Founded in Geneva in April 2018, by team of four: private banker, hedge fund manager, lawyer, crypto guy; F&F initial funding
- Now more than 10 persons, mostly engineers, among the best in CH
- We have customers too!



TRADE

Digital asset trading platform and services

Broker for private investors

Dealing desk for institutional investors (incl. ICO cash-out)



INVEST

Advisory in digital assets & blockchain investing

Digital asset research incl. technology assessment

Structured products / collective investment schemes

Securitization / tokenization of assets



PROTECT

High-security cold storage vault for digital assets

High-security storage solution

This is the slide about the company, Taurus Group SA

- Founded in Geneva in April 2018, by team of four: private banker, hedge fund manager, lawyer, crypto guy; F&F initial funding
- Now more than 10 persons, mostly engineers, among the best in CH
- We have customers too!



TRADE

Digital asset trading platform and services

Broker for private investors

Dealing desk for institutional investors (incl. ICO cash-out)



INVEST

Advisory in digital assets & blockchain investing

Digital asset research incl. technology assessment

Structured products / collective investment schemes

Securitization / tokenization of assets



PROTECT

High-security cold storage vault for digital assets

High-security storage solution

OTHER

Source of crypto funds analysis

ICO consulting

Training & conferences

This is the slide about the company, Taurus Group SA

- Founded in Geneva in April 2018, by team of four: private banker, hedge fund manager, lawyer, crypto guy; F&F initial funding
- Now more than 10 persons, mostly engineers, among the best in CH
- We have customers too!



TRADE

Digital asset trading platform and services

Broker for private investors

Dealing desk for institutional investors (incl. ICO cash-out)



INVEST

Advisory in digital assets & blockchain investing

Digital asset research incl. technology assessment

Structured products / collective investment schemes

Securitization / tokenization of assets



PROTECT

High-security cold storage vault for digital assets

High-security storage solution

OTHER

Source of crypto funds analysis

ICO consulting

Training & conferences

Storage solution, for whom?

Not for private individuals, but for **organizations** that need

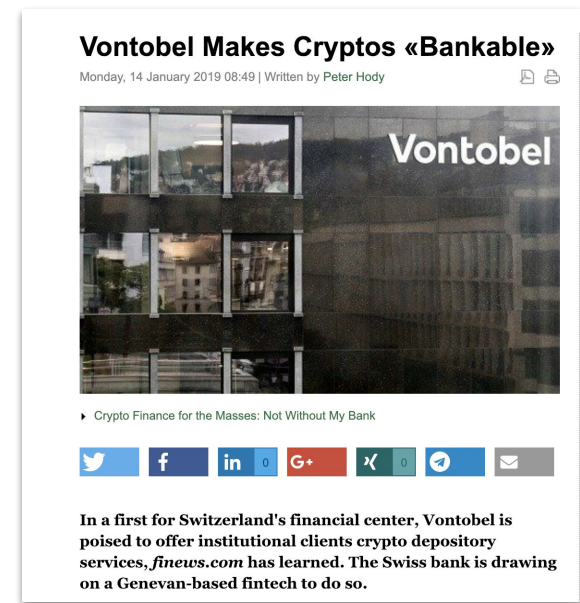
1. To **store** lots of crypto money, be it their own or as custodians
2. Use the solution in **compliance** with regulations and governance processes, such as "4-eyes control", nostro/client wallet segregation, etc.

Typical **customers**:

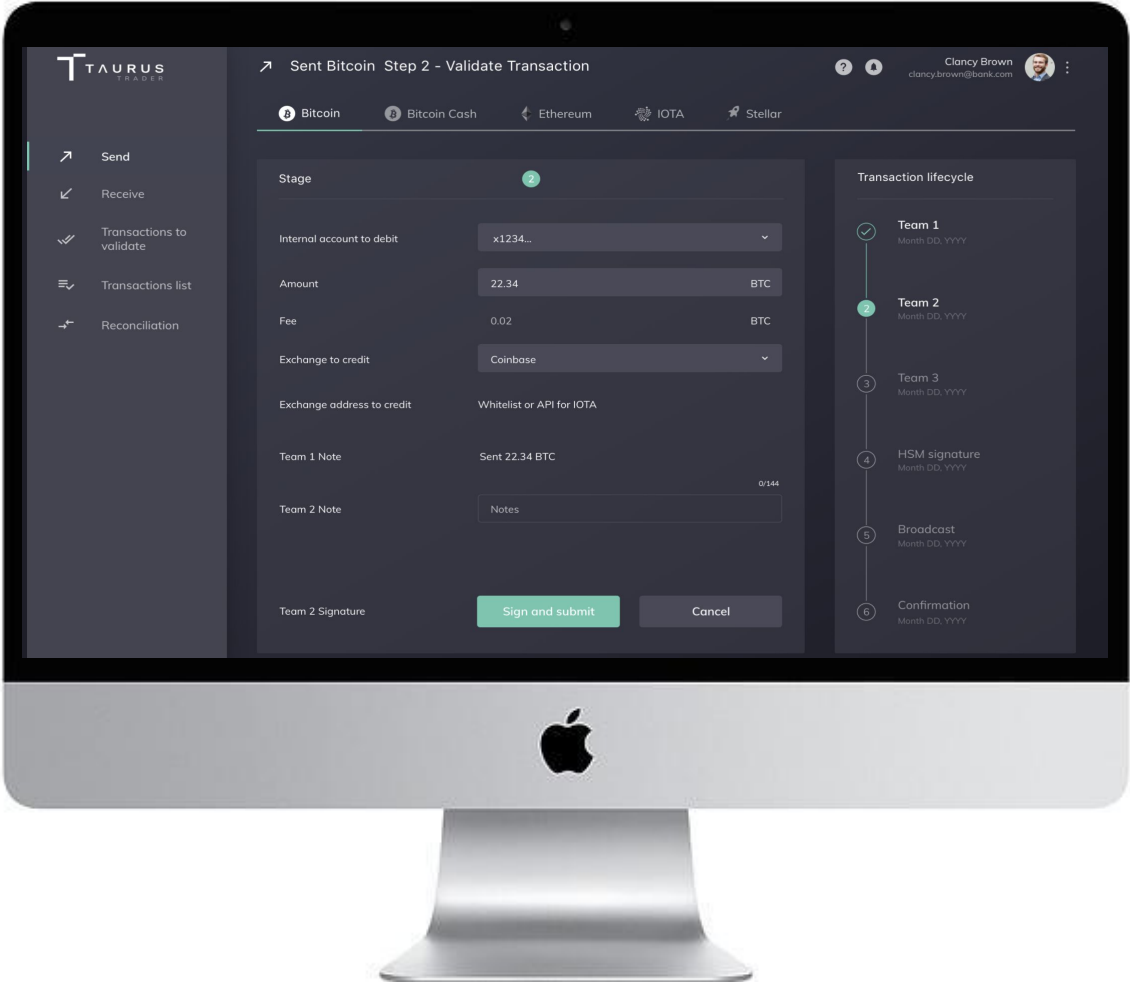
- Private banks
- Hedge funds
- Asset managers

Strict security, functional, and usage **requirements**:

- Prevent insider theft and loss of funds
- High service availability, detailed logging
- On-premise, rather than SaaS
- UI should be usable by non-tech personnel

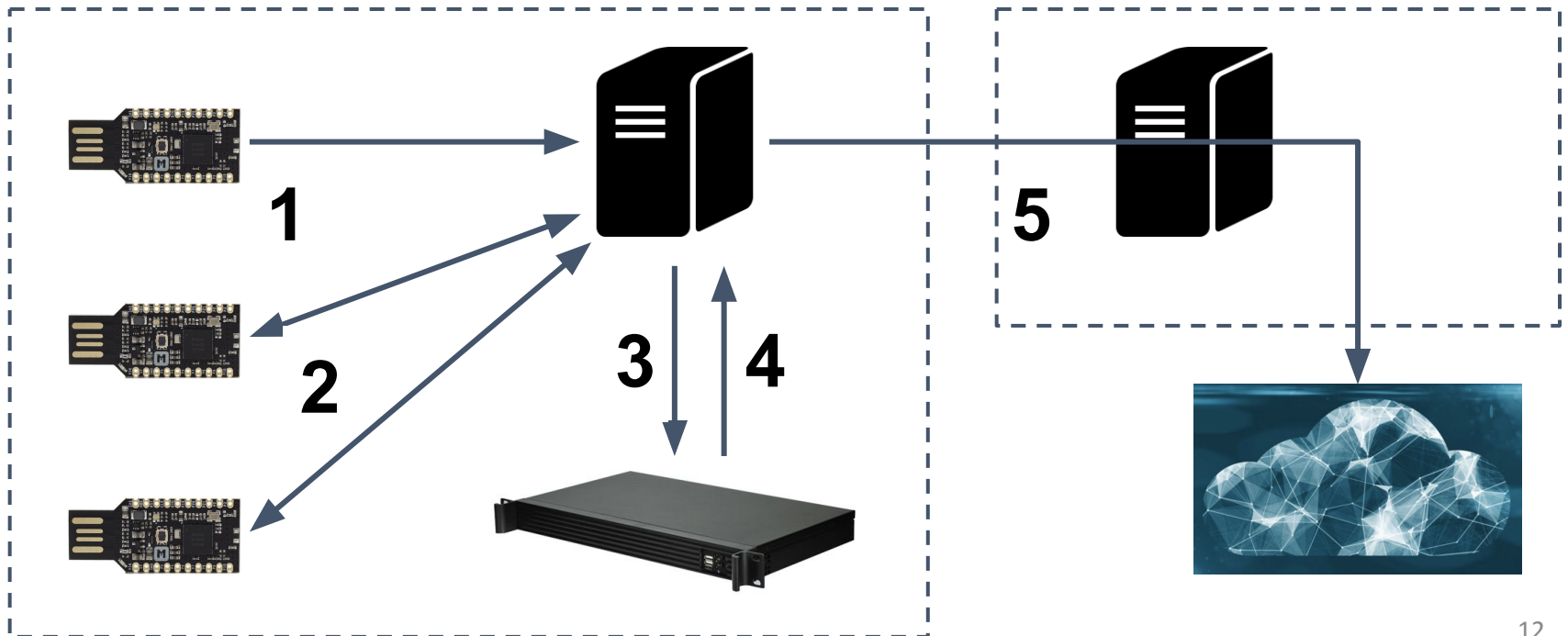


Web-like GUI, dark mode!



Storage solution? Easy! *(I know I suck at diagrams)*

1. **Transaction request**, by requester using some hardware device, authorizations criteria verified by the backend
2. **Transaction approval**, by approvers using their hardware devices
3. **HSM receives the request**, checks the approvals and other things
4. **HSM creates and signs** the actual blockchain tx, sends it to the backend
5. Signed is sent to another network and **broadcasted** to its blockchain network





That's it?

Looks easy but **nothing is easy**

Let's look at a few of the challenges faced, focusing on **security** matters

More questions than answers, can't disclose all the details here ;-)



Having fun with HSMs

What model to choose? Criterias include

- Support for crypto functionalities (secp256k1, BIP32, etc.)
- Ability to add custom software (for altcoins)
- Security assurance and certifications (fwiw)
- Cost, service and support
- Customers preference and familiarity with a brand or model

Now that we have an HSM, we discover its **SDK, toolchain**, etc.

Emulation mode is convenient, but doesn't emulate everything :-/

We discovered **undocumented** behavior and bugs in the HSM...

Debugging can be a real pita, when HSM logs need to be extracted manually and don't contain all the relevant information

Error messages aren't all ways useful ("general error")



Key generation and ceremonies

Ceremony required to:

- Generate **secrets**, create backups, load them in the HSM
- Load **data** into the HSM: certificates, etc.
- Load **custom code** into the HSM

Customer needs to run a **ceremony for each software update!** Costly and error-prone, need to minimize the logic in the HSM and the number of updates

Key generation **inside or outside** HSMs?

What **PRNG** to use? Is a hardware/quantum RNG really better? (spoiler: no)

How to **split** the secrets? SSS? ssss?

What **storage media** for secret shares?

What **procedure** to move them to safes in different locations?



Some altcoins are more equal than others

Bitcoin and Ethereum are well documented:

- Standard BIP32/BIP44 with test vectors and CLI tools
- Need to be careful with support of address types, features (segwit, etc.)
- We wrote our own C wallet code to run in the HSM...

How to best deal with Ethereum's **nonce/counter** mechanism?

What if a customer needs a **"batch" mode**?

How to have **multisig**-like mechanism we not all coins support multisigs (or implement it differently)? What's a coin-agnostic solution?

What to do when a coin has no test vectors, **no usable testnet**?

How to plan and deal with **forks**?

How to broadcast txs **reliably** when there are no reliable public nodes?



Secure software is hard

Back-end and related services are critical, yet often overlooked

- Written in Go, for the usual reasons
- We had to rewrite our own version of several components, because open-source versions were not reliable (or inexistent)
- Good "observer" software doesn't exist, wrote our own

Front-end is a web-like UI, JS etc.

- Minimized the amount of trusted components as much as possible
- How to securely interact with hardware devices for signature etc.?

Many bugs, inconsistencies, and other shortcomings found in **open-source code**

Secure SDLC, because software is more likely to fail than crypto

- Internal code reviews, of our own and third-party components
- Best practices etc.
- Third-party audit



Conclusions

An enterprise wallet solution is much more than a "signing machine"

The crypto part is by far not the hardest part

Anticipating questions:

- So it it a cold wallet or hot wallet?
 - Warm :-p
- How much does it cost?
 - "It depends"
- What coins do you support?
 - Those that customers ask for: BCH, BTC, ETC, ETH & ERC20, IOTA, XLM, XRP, and more...