Riddle & Code®

LIBERATING HUMANS AND MACHINES.

DIGITAL ASSET MANAGEMENT SOLUTION

NOV 2019 V 1.0

Riddle & Code®

DIGITAL ASSET MANAGEMENT SOLUTION

"WE ARE PROUD OF OUR NEW CUSTODY SOLUTION THAT RESPECTS ALL REGULATORY AND COMPLIANCE REQUIREMENTS. OUR COOPERATION WITH RIDDLE&CODE HAS ENABLED US TO BYPASS THE COMPETITION AND TO REAFFIRM OUR FIRST-MOVER ROLE IN THE AREA OF BLOCKCHAIN BANKING SERVICES" -

Alastair Fiddes, Falcon Group COO

Riddle & Code®

WE SET OUT TO

PROVIDE THE MOST **SECURE**, MOST CONVENIENT **OPEN SOURCE** DIGITAL ASSET MANAGEMENT SOLUTION

Riddle & Code®

A NEW BREED OF ASSET MANAGEMENT

An innovative combination of hardware and software that stores, secures and manages digital assets.
Audited by swiss financial regulatory bodies, our solution includes state-of-the-art security and features.

It has been designed based on banking and financial institution requirements, to secure their assets and those of their clients in the form of custody services.

UNIQUE SELLING PROPOSITION

- It combines hardware and software to achieve the highest level of security
- Secrets are never stored on one single device, eliminating the single-point-of-failure problem
- It eliminates the need to transfer funds between hot and cold storage
- It allows integration into regulated fintech and banking processes
- It fully supports custody service via forward deterministic key derivation and allows to offer these services to clients
- It successfully went through exhaustive code audit and is accepted by Swiss regulatory bodies
- It verifiably proves segregation of assets, freeing banks from backing custody crypto assets with FIAT in CH.
- It introduces banking grade multi-device, multi-trader signature schemes

Plus:
Solution has acceptanc
from financial Regulato
bodies in Switzerland

Riddle & Code®

BANKING GRADE

Our solution has been successfully deployed at Swiss banks providing the integration with traditional core banking systems.

It offers a state of the art **key management and unlimited key derivation** scheme for the creation and management of custodian accounts.

It supports mapping of custodian accounts to the traditional client accounts **to meet the requirements of asset segregation.**

Our solution provides a full banking industry compliant **audit trail**.

First wallet to receive regulatory **acceptance by Swiss regulatory bodies**.

Riddle & Code®

OPEN

We believe that the complexity of todays attack vectors on current technology can not be managed by a single organization anymore.

Rigorous peer reviews represent the most reliable alternative to achieve the highest resilience in the complex technology system.

For that reason our solution follows a strict **open source** approach. Our **code** is made **public** and hardware designs are shared with our clients to prevent vendor lock in situations

Riddle & Code®

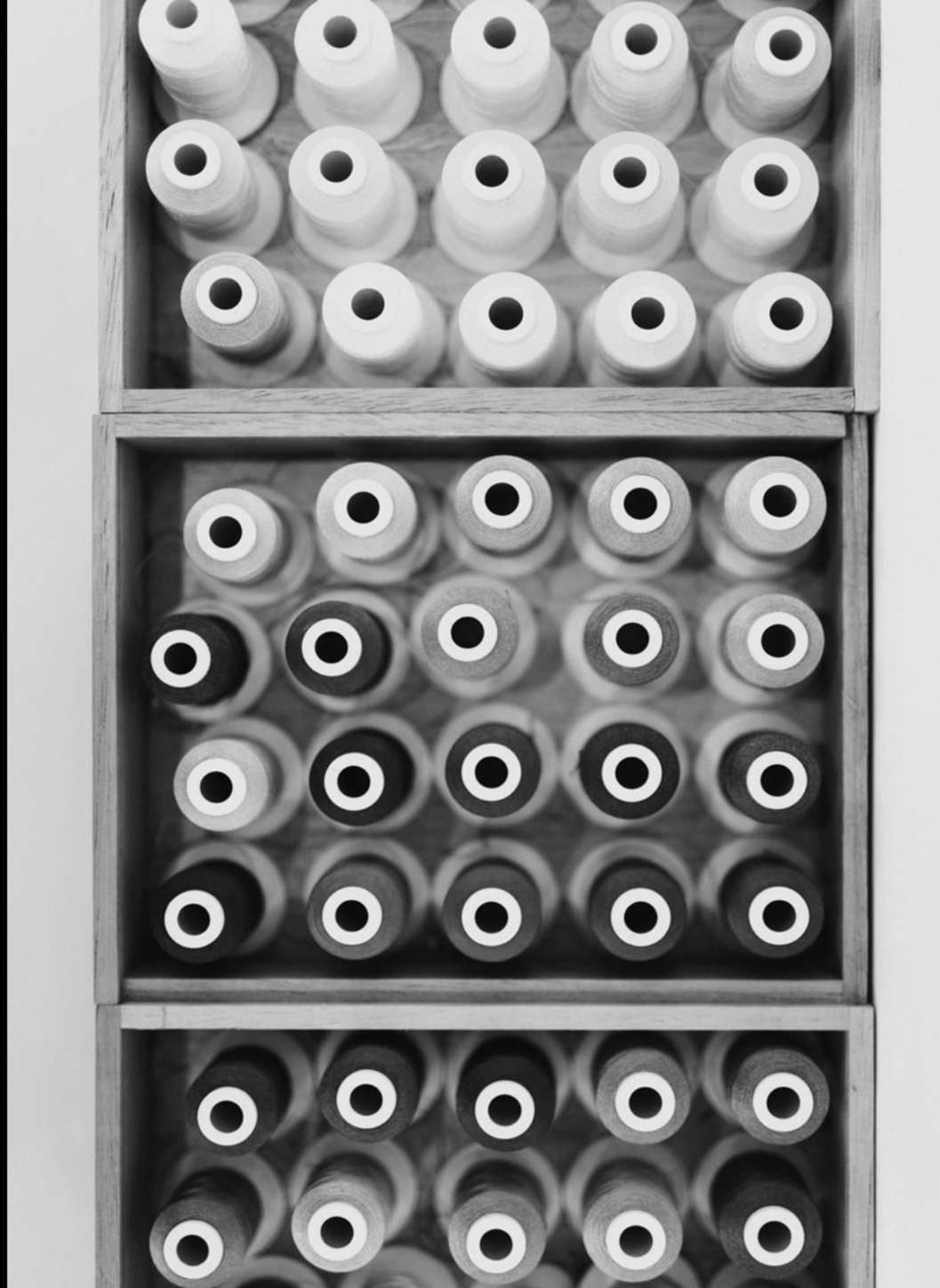
AGILE

Our solution design allows to load new crypto algorithms onto the hardware wallets in reliable and fast implementation cycles.

Our architecture allows to disregard the need to transfer funds between hot and cold wallets resulting an improved usability and reduced process complexity.

Customizable approval workflows

The digital asset management solution is designed to support the issuing, securing and trading of tokens and therefore offers a product that extends beyond cryptocurrencies.



Riddle&Code®

SECURE

RIDDLE&CODE's deployed signature scheme is based on Shamir's secret sharing to sign transactions.

In contrast to traditional multi-sig solutions security is increased by dividing a secret (the signing secret) into slices, giving each signee its own unique part.

This method prevents that the signing secret is stored on a single device, avoiding a single point of failure, like in the case of traditional HSM-based solutions.

Riddle & Code®

HOT vs COLD WALLETS

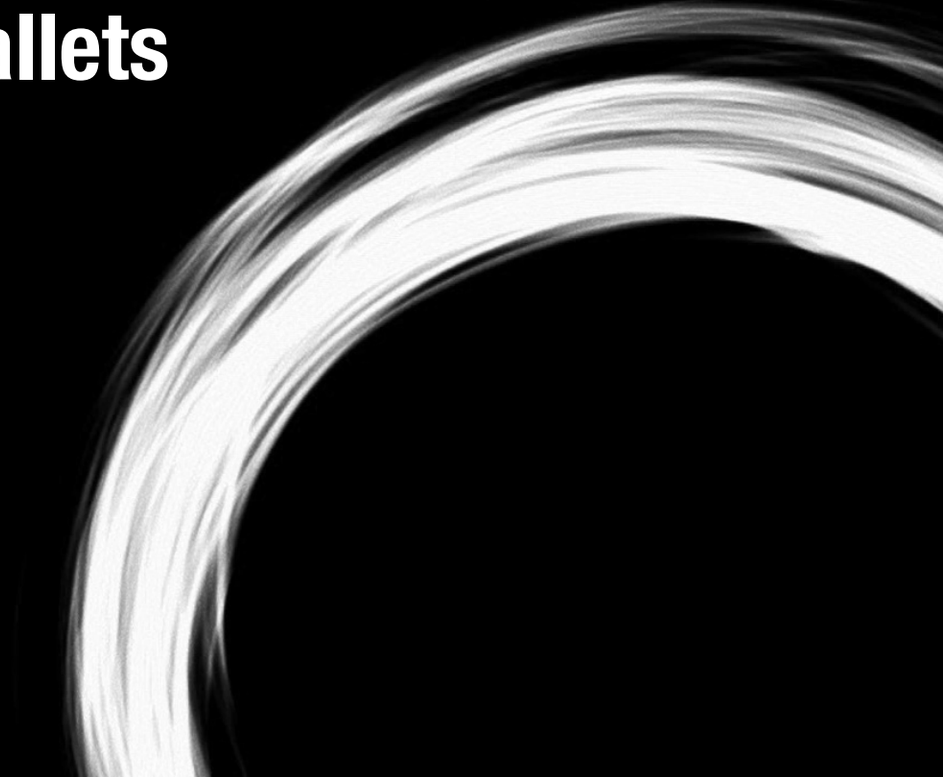
Exchanges traditionally transfer funds from cold to hot wallets on a daily basis depending on the requirements of liquidity.

Using a wallet where secrets are never stored on a single device allows to avoid the need to swap funds on a daily basis, increasing the security of these funds and lower the operational efforts.

Even if exchanges want to stick to their traditional set-up of cold and hot wallets, our solution is used to move funds between these wallets.

Another option is to use our solution in a cold/hot wallet setup as the hot wallet, reducing the attack vectors on this wallet drastically, basically turning a formerly hot wallet into a secure “cold/hot” wallet that can perform transactions at any time since secrets are never stored on a device.

Drastically improve daily operations when moving funds between cold and hot wallets



POLICY LAYER

Security Feature

- Allows to further enhance the security by introducing rule-based operations
- Rules get cryptographically signed with a Signature Device and sit in a Trusted Execution Environment

Example

If TX value exceeds a defined threshold, then a C-level manager needs to co-sign the transaction

Samples policy rules

- Time-based condition (e.g. within 2 hours)
- Asset/currency-based rules (e.g. Equals/unequal BTC)
- White/Blacklist (e.g. transactions can only be sent to Whitelist entries)
- Transaction price (e.g. <,>,= 15 BTC)
- Transaction value (e.g. <,>,= 15.000 €)
- % margin limit definition for trades (e.g. Trade is below 10%)
- Signer/Role assignment (e.g. Belongs to Group A)
- Limit of total trade value: daily/weekly/monthly
  (e.g. max total trade value per day 250.000)

Riddle & Code®

REGULATORY COMPLIANCE

RIDDLE&CODE'S digital asset management solution is approved by Swiss regulatory bodies. This compliancy requires to meet all provisions regarding audit trails and reconciliation features.

Using our solution enables a bank or an exchange to meet the regulatory provisions regarding mandatory audit trails, segregation of accounts or reconciliation.

In the light of increasing regulatory frameworks this feature will be crucial for companies that want to participate in regulated crypto or token markets of the close future.

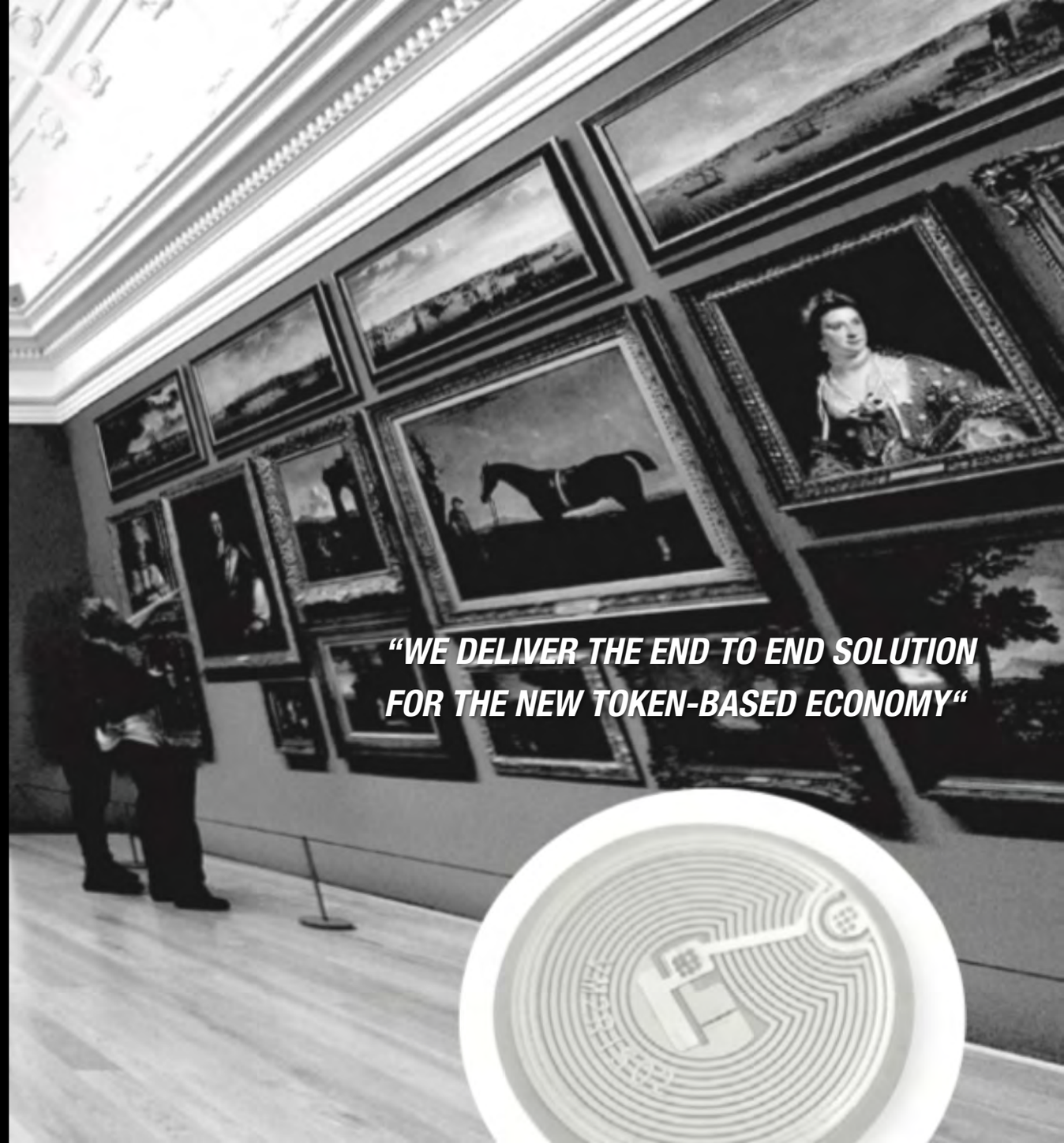
Riddle & Code®

TOKENISATION READY

The combination of our **digital asset management solution** and the crypto tags of our **object solution** provides a secure and integrated method to link physical objects to digital tokens.

Features:

Create, store and manage tokens based on fungible and non fungible physical assets alike



Riddle & Code®

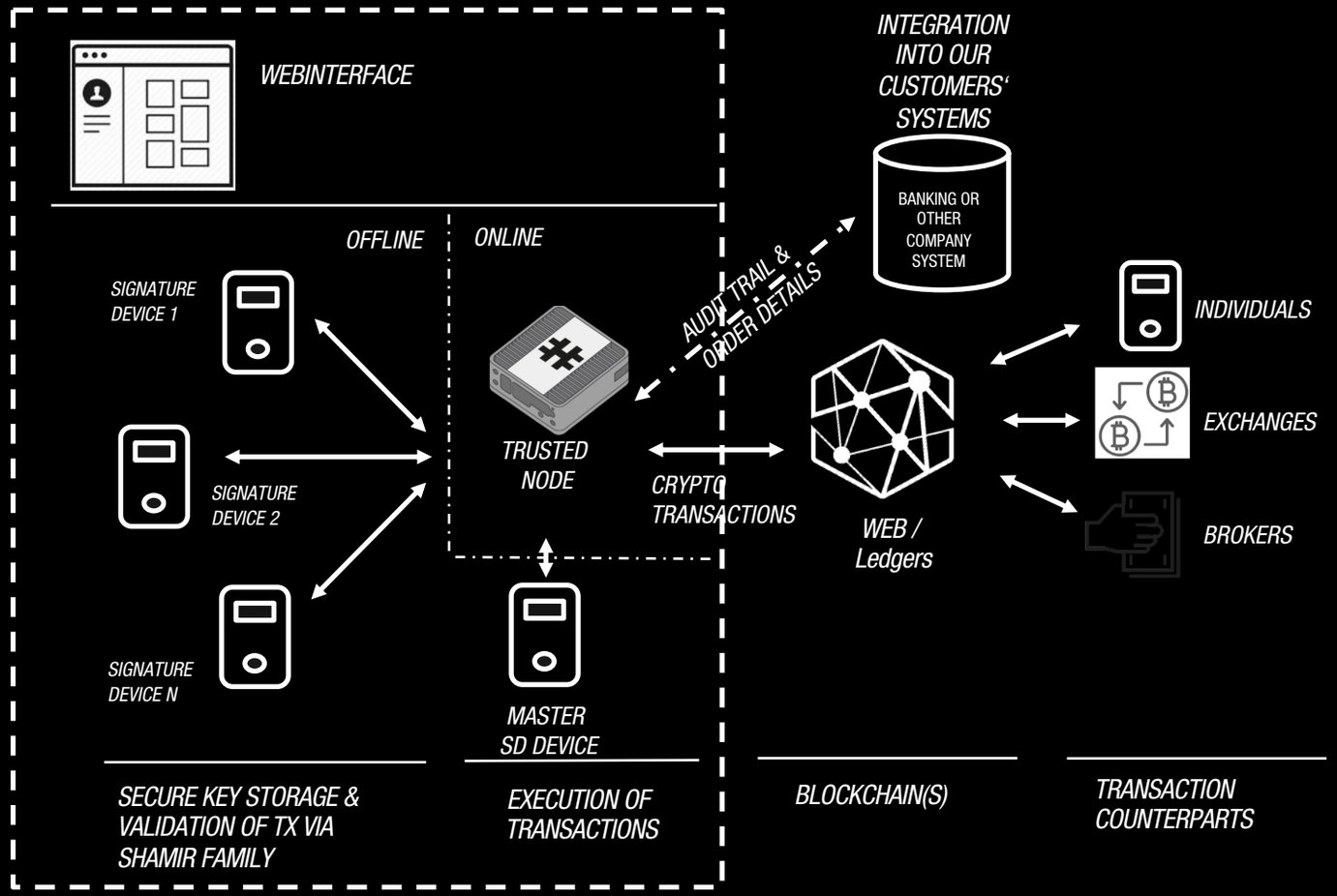
INNOVATIVE SIGNATURE SCHEMES

By replacing a HSM-based key management and signing through distributed multi-hardware-wallet setup our solution enables true multi-device, multi-signature for any crypto currency or token utilising Shamir secret sharing algorithms.

This setup supports a number of innovative signing schemes.
For example traders in different physical locations or time-zones can co-sign transactions.

Riddle & Code®

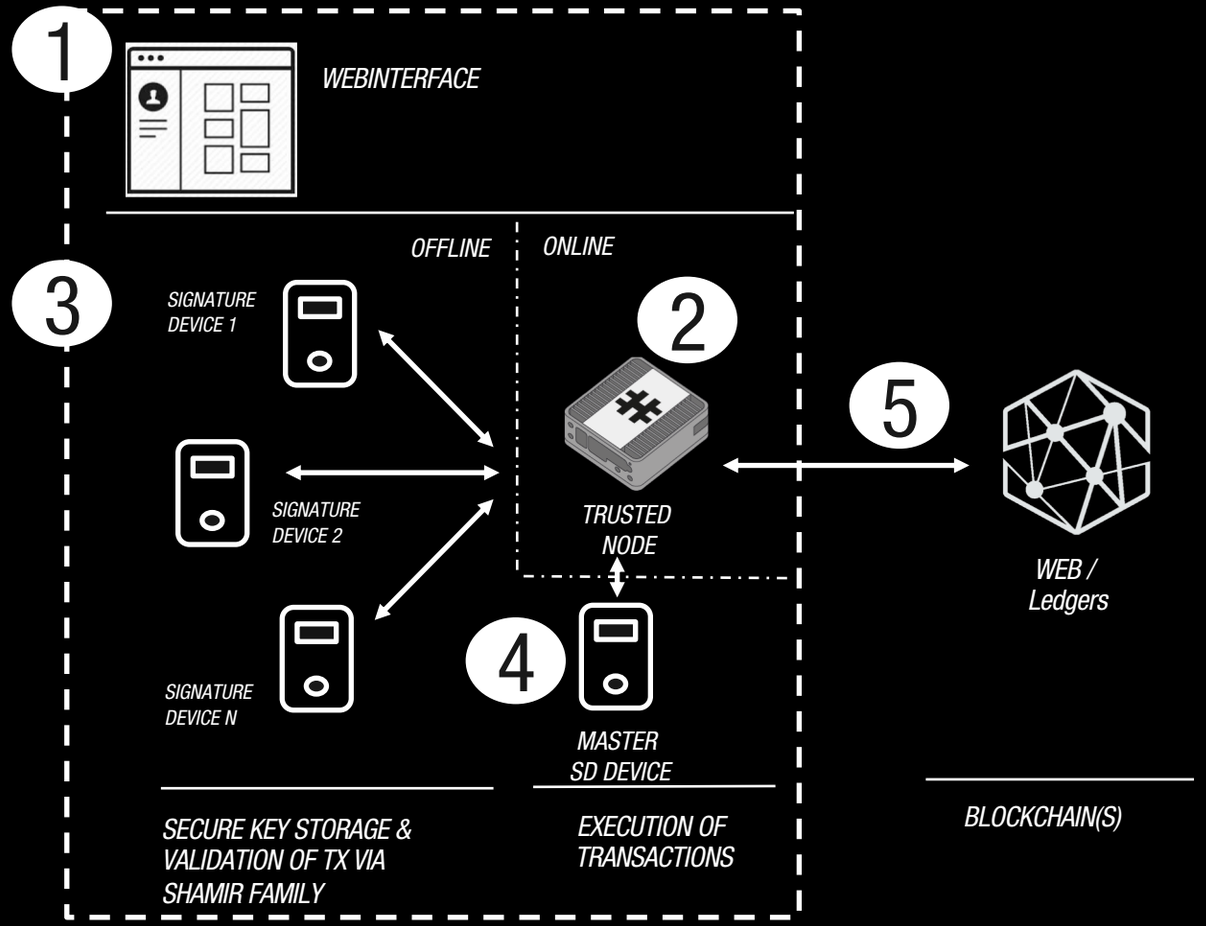
ARCHITECTURE



COMPONENTS

- Trusted node (TN)
- Signature devices (SD)
- Web interface
- External system integration via API
- Audit log via API
- Syslog

SIGNING PROCESS



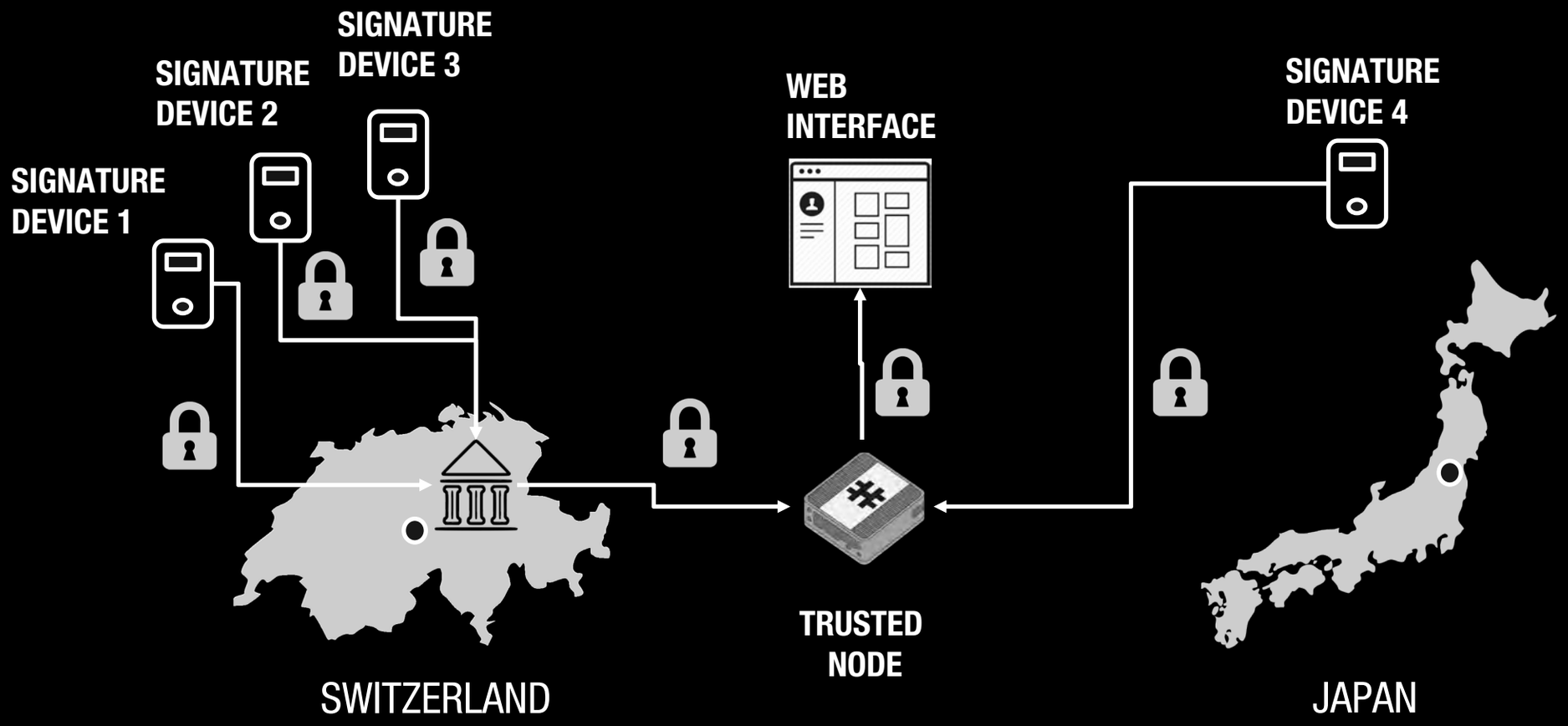
1. Via the **web interface** transactions are prepared and initiated
2. The **trusted node** creates the related raw transaction with pending signatures and sends it to the signature devices for approval/signing.
3. Each **signature device** signs the raw transaction with its Shamir's secret slice. The number of signature devices in configurable (m of n) via the web interface.
4. The **master signature** device collects and decrypts the signatures, recovers the master secret, signs the transaction and sends it back to the trusted node. The master secret is zeroized.
5. The **trusted node** broadcasts the signed transaction to the target blockchain/DLT

DISTRIBUTED SIGNING SCHEMES

DISTRIBUTED SIGNING #1

BANK-TO-BANK MULTI-SIGNATURE

High value transactions get signed by three traders in the Switzerland headquarter and by the CFO, currently on a business trip, e.g. in Japan.

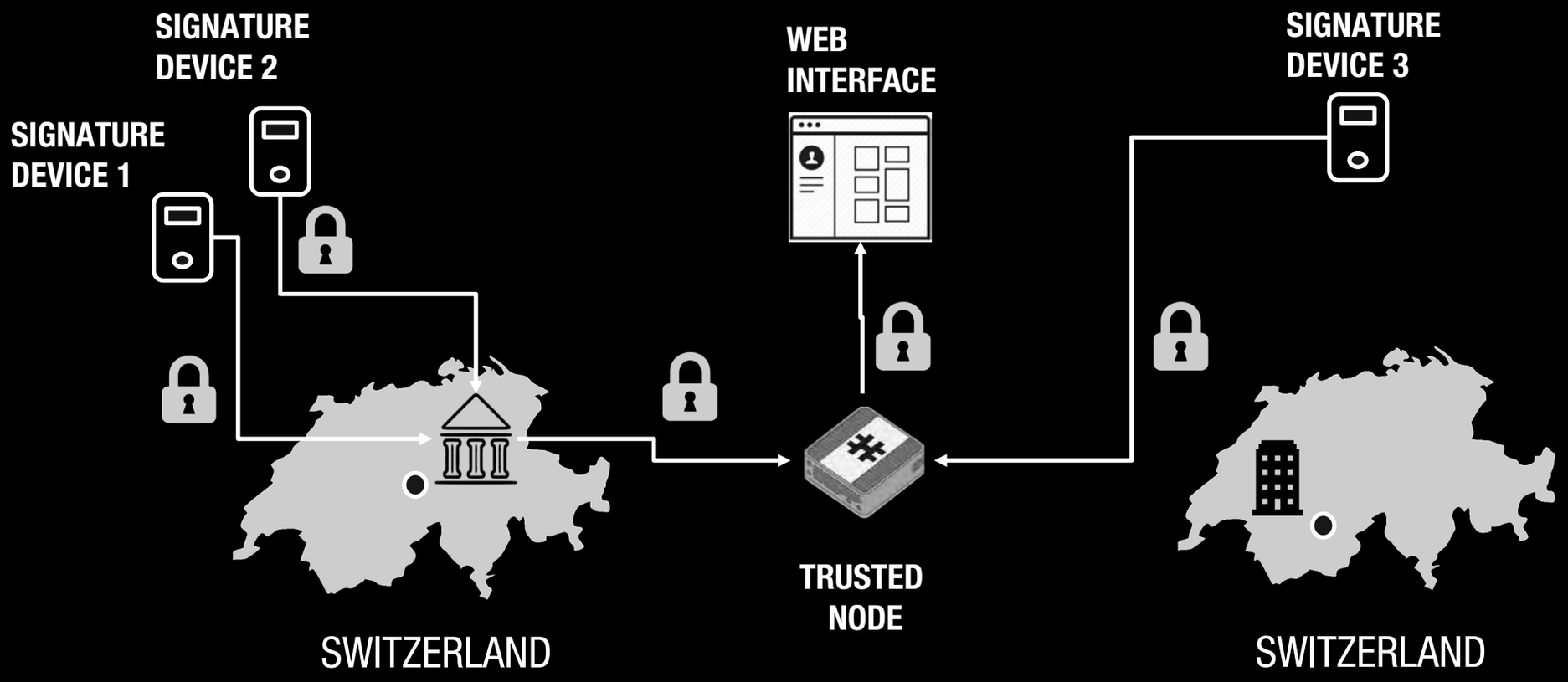


DISTRIBUTED SIGNING SCHEMES

DISTRIBUTED SIGNING #2

CLIENT MULTI-SIGNATURE

High value transactions get signed by two traders in the bank or exchange, the client gets notified and co-signs to complete the transaction.

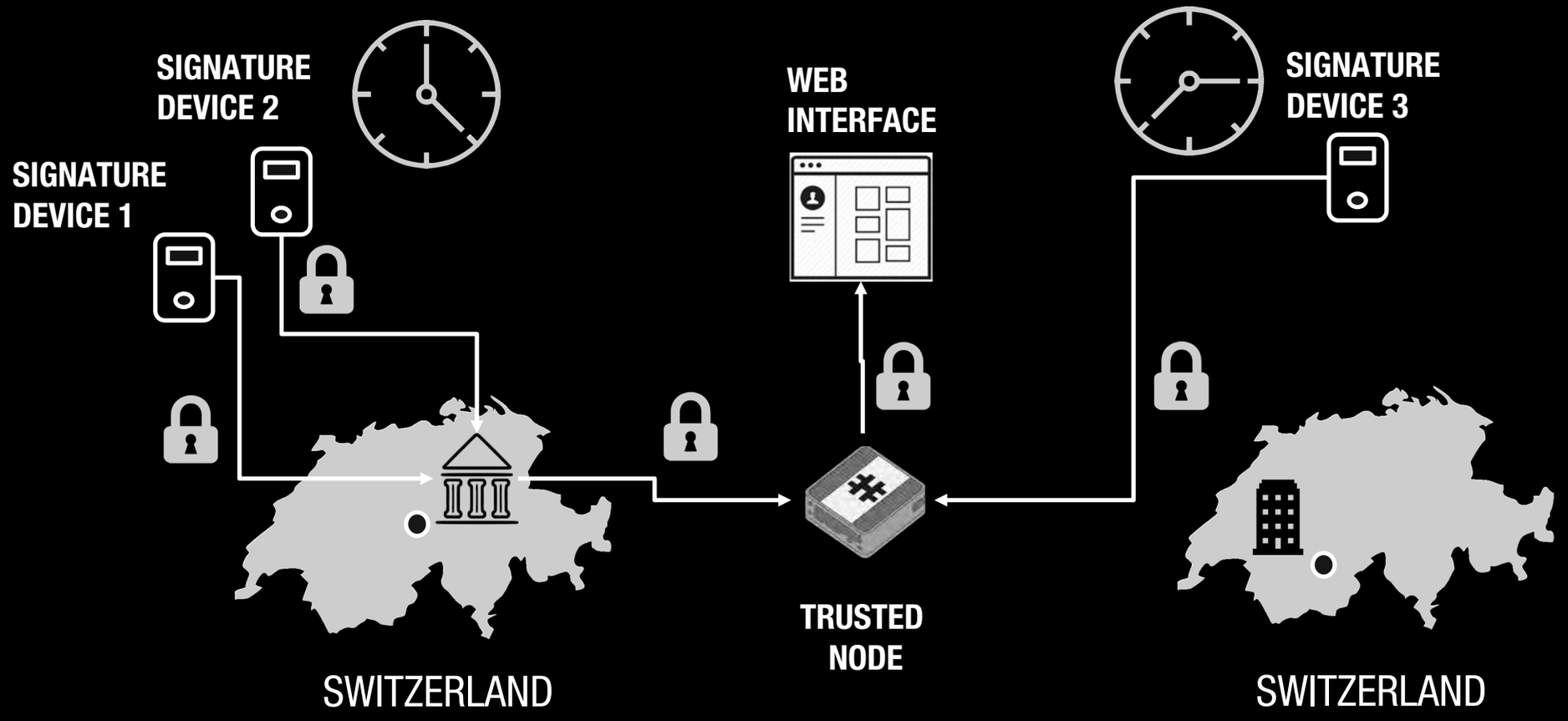


DISTRIBUTED SIGNING SCHEMES

DISTRIBUTED SIGNING #3

TIME-DELAYED SIGNING

In specific cases, transactions may not need to be executed immediately. Our solution features a time delay functionality to accommodate such use cases.

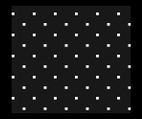


Riddle & Code®

FEATURES

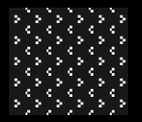
SECURE

- **SIGNING SECRETS** are never stored on a single device
- Real time audit logging
- Account/wallet **SEGREGATION**
- Successful code **AUDITS**
- **SELF-ENCRYPTING** data storage
- **SECURE** communication between all devices
- **POST-QUANTUM SIGNATURES**
- All functions of an HSM
- Full business rules & process support
- **FIPS 140-2** compliant



OPEN

- **Peer reviewed OPEN SOURCE** approach
- **DECENTRALIZED** solution design
- Built to **SECURE FEDERATED BLOCKCHAIN** nodes
- Proximity & **DISTRIBUTED** signatures
- Full support of **TOKEN** Economy
- Manage secrets belonging to token wallets



AGILE

- **MULTI SIGNATORY** function for ALL cryptocurrencies
- Threshold Signatures according to business rules
- **FULLY CUSTOMISABLE** approval workflows
- Multilevel approver identification up to **3FA**
- **SEGREGATION** of roles
- Supports enforcement of local regulatory requirements (e.g. amount of transfers, signatures, location of the approver)
- **TIME-DELAYED** transactions
- **CUSTODY** service via forward deterministic **KEY DERIVATION**
- Code flexibility
  - **AGILE REVISIONS**
  - easily add new currencies

Riddle & Code®

SUPPORTED CURRENCIES

The solution currently supports 32 types of crypto assets (and derivatives thereof). Bitcoin-forked or ERC-20 assets are counted as one type.

- BITCOIN
- LITECOIN
- BITCOIN CASH
- BITCOIN GOLD
- RIPPLE
- DASH
- IOTA
- STELLAR
- BITCOIN SV
- ETHEREUM
- ETHEREUM CLASSIC
- DOGECOIN
- ERC20

Additional cryptocurrencies and tokens can be implemented on request.

Riddle & Code®

AVAILABLE CURRENCIES – Q1/2020

BITCOIN	DASH	ELEMENT	ZENCASH
BITCOIN CASH	BINANCE	QTUM	RAVENCOIN
BITCOIN GOLD	STELLAR	CORDAR3	DIGIBYTE
BITCOIN DIAMOND	CARDANO	LISK	KOMODO
IOTA	MONERO	PIVX	MAIDSAFECOIN
ETHEREUM	TEZOS	DOGECOIN	MONACOIN
RIPPLE	AUGUR	DECRED	FUJICOIN
LITECOIN	NEM	TENDERMINT	WANCHAIN
TETHER	ZCASH	LIQUID	PIVX

CONTACT

For all inquiries you can reach us at

office@riddleandcode.com
Tel.: +43.1. 205 774 0039 (main switch)

RIDDLE&CODE GmbH
Orbi Tower, 10th floor
Thomas-Klestil-Platz 13
1030 Vienna
Austria/Europe

RIDDLE&CODE GmbH is registered in the commercial register of the Commercial Court of Vienna under: FN 462779 h, VAT identification number: ATU72126558

LIBERATING HUMANS AND MACHINES.