Block-safe

Hardware-Sicherheit für Distributed-Ledger-Technologie

utimaco®

Mario Galatovic

Distributed Ledger Technologies - Potential risks

utimaco®

CONSENSUS

- Attack by external party
- Collusion by entities running nodes

CONTROL OF SIGNING KEY

- Theft of private key and use elsewhere
- Attacker getting rights to use private key
- Single person control of key depends on integrity of one person
- Risk depends on the value or action controlled by the private key.
- Risk is increased for concentration points such as wallets, gateways and exchanges

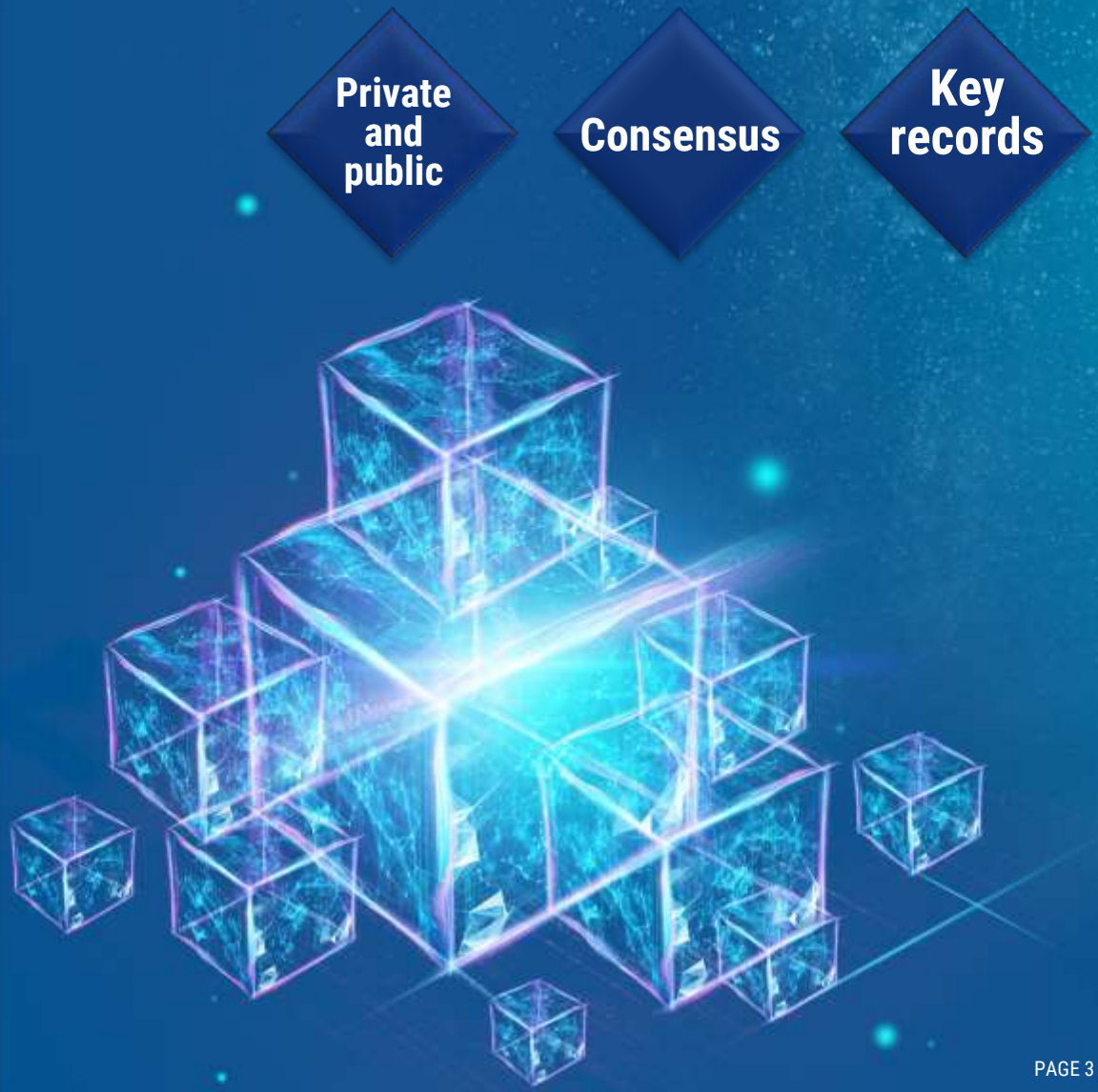
CONFIDENTIALITY

- Entities may not want all data readable by competitors

Block-safe Value Proposition

utimaco®

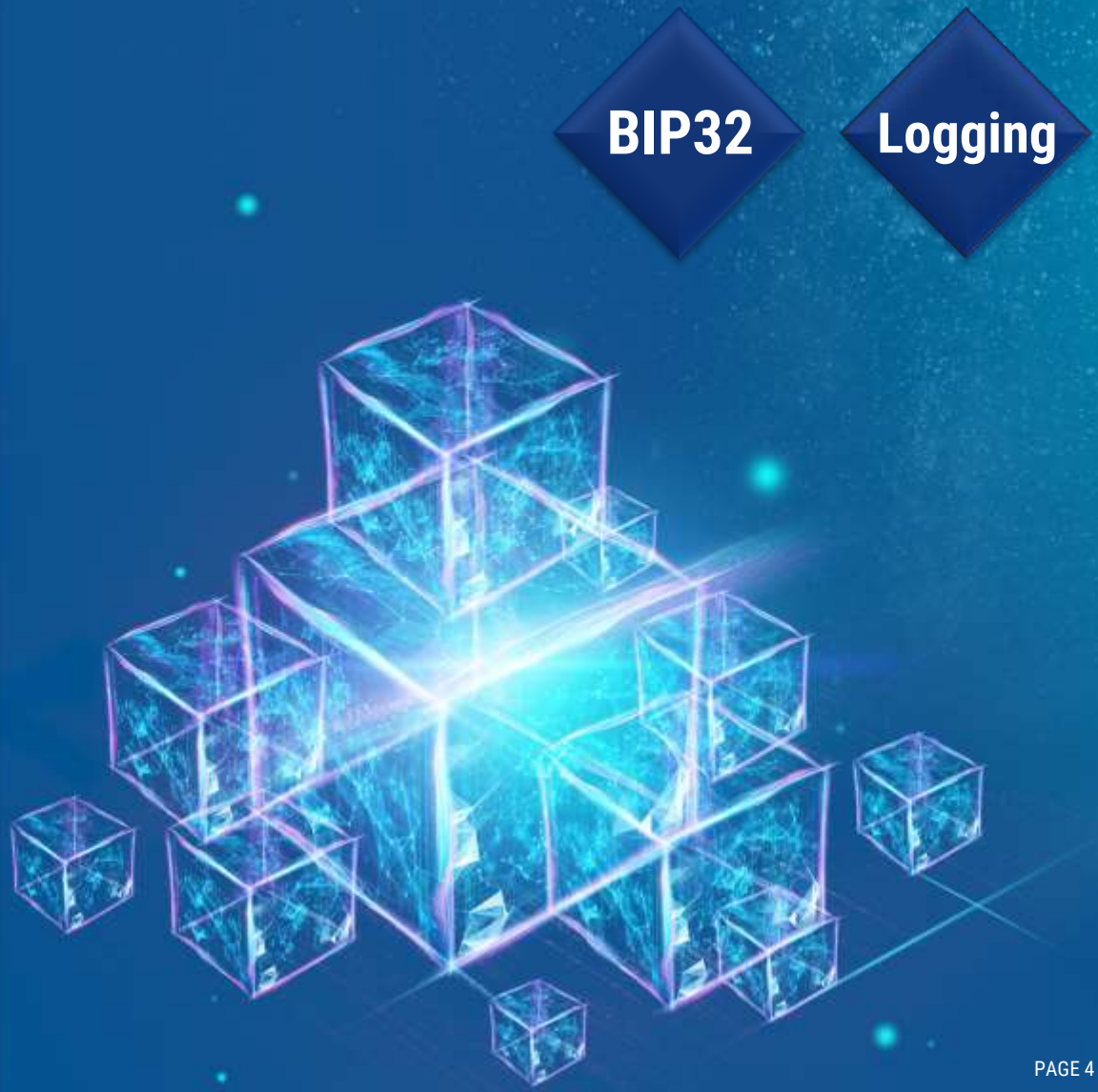
- **Generation of private and public key pairs**
  - Blockchains specific elliptic curves
  - Bitcoin and Ethereum blockchain **Secp256k1**
  - Stellar **Ed25519**
- **MultiSig**
  - M keys to authorize / **Consensus**
- **Encrypt, decrypt and use key records from key databases**
  - Solutions which maintain a significant number of keys need to use key databases to store these keys
  - The HSM can receive an encrypted key and use it within the secure environment



Block-safe Value Proposition

utimaco®

- **Secure Storage for Private Keys**
- **Hierarchical Deterministic Wallet Support**
  - Ability to derive key-pairs in a secure environment from a single key master according to **BIP32**
- **Logging**
  - Being able to audit and monitor how and when keys are used can offer an additional layer of security



Block-safe 1.00

utimaco®

- **Client-side Support**
  - PKCS #11 VDM
- **Support for Distributed Ledger Technology (DLT)**
  - BitCoin
  - Ethereum
  - Hyperledger
  - R3/Corda

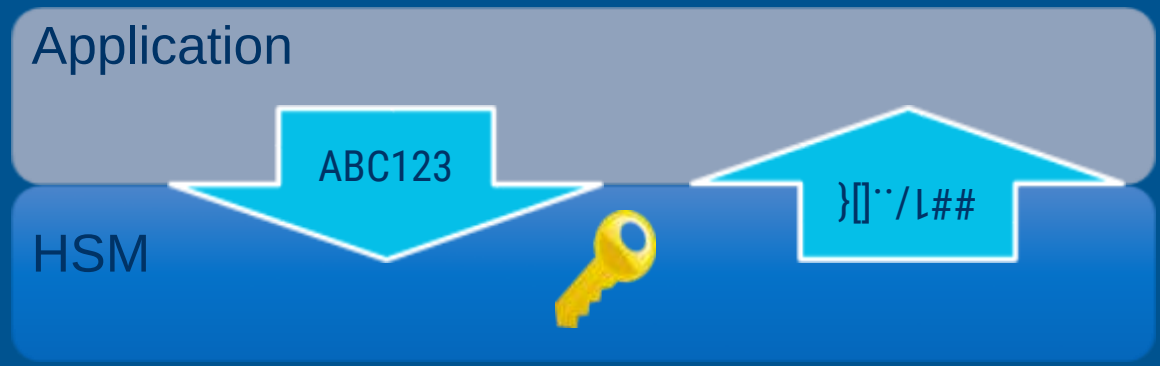
CryptoServer Cloud

- **All products available in Utimaco‘s cloud offering**
- **Additional data centers hosting the HSMs**
  - Better redundancy and lower latency per continent
- **Availability depending on customer demand**

Utimaco portfolio

Purpose of an HSM

- Hardware cryptographic resource
  - Secure memory
  - Quality of keys
- Secure Key Management
- Follow best practices
- Open API, protocols
  - Easy integration with commercial apps
- Certified products
  - FIPS 140-2L3 and L4
  - PCI
  - CC EAL4+



Product Portfolio

utimaco®

Disk Encryption | Authentication Identity and Access Management | Key Injection | PKI | Code Signing | Signature Creation / Document Signing | Cloud | Card Issuance | Alternative Payment / Mobile | Inter-Banking | ESKM

Software

DiskEncrypt
Encryption Software for Hard Disk Drives

Firmware Packages

SecurityServer
General Purpose HSM

CryptoServer CP5 VS-NfD
Securing classified information

PaymentServer
Incl. SDK

CryptoServer SDK
Customization through Firmware Development

CryptoServer CP5
Qualified Signature Creation Device

TimestampServer
Reliable Time Stamps

CryptoScript
Customization through Scripting

Platforms

Se-Series
12/52/500/1500

CSe-Series
10/100

CryptoServer

Cloud

Appliances

Atalla
Payment HSM for Banks and Payment Processors

AT1000

Atalla

ESKM
Enterprise Secure Key Manager

ESKM

Block-safe

utimaco®

Utimaco Block-safe is a HSM for protecting sensitive data and associated keys for blockchain systems using distributed ledger technology (DLT) and wallets.

Use it to create “Know your customer” transparency and speed up cross-border settlements.

- Private and public
- Consensus
- Key records
- BIP32
- Logging

Thank you!

Mario Galatovic

Director Strategic Partners
Mario.galatovic@utimaco.com

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696-0
Web www.utimaco.com
E-Mail info@utimaco.com