The innovation in the IT-Security
BlueSpice & Secure Wiki

Meet the latest security requirements with Secure Wiki Services.

Use crypto processes to prove the authenticity

and trustworthiness of your wiki-stored data.

BlueSpice MediaWiki

inblockio

inblock.io assets GmbH

Speaker Introduction - Tim Bansemer

- Background in IT security consulting, network & system administration
- Founder & CEO of inblock.io assets GmbH, a company focused on promoting digital sovereignty (Since 2017)
- Working with Bitcoin and Ethereum projects and distributed systems (Since 2017)
- Actively involved in community outreach and events related to digital distributed governance
- Member of the European Society for Digital Sovereignty

Tim Bansemer

Mission Statement: inblock.io assets GmbH

We believe in *digital sovereignty for self-directed, sustainable, and trusted value creation.*

We achieve this by *developing resilient, open-source services to enhance trust.*

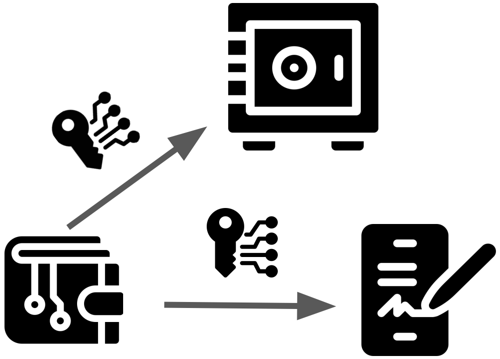
*Today, we introduce **AQUA,** a technology implemented as a **Wiki-Extension** to establish **Secure Wiki's** for reliable knowledge and data management.*

*This extension can be seamlessly integrated into **BlueSpice** or any other MediaWiki platform.*

Developing “AQUA” - Secure Wiki Technology

- Began in April 2021 as a free and **open-source project by inblock.io**
- Chosen in September 2021 as a prototype for the federal education platform (open-source solutions) for **digital verification of educational certificates,** proposed by Dataport AöR
- **Collaboration with Hallo Welt! for enterprise wiki integration**
- Project completed in Q1 2022 with **prototype ready for piloting**
- Project resumed in Q1 2023 in collaboration with Hallo Welt!

With AQUA, we create **Secure Wiki**’s using cryptography:



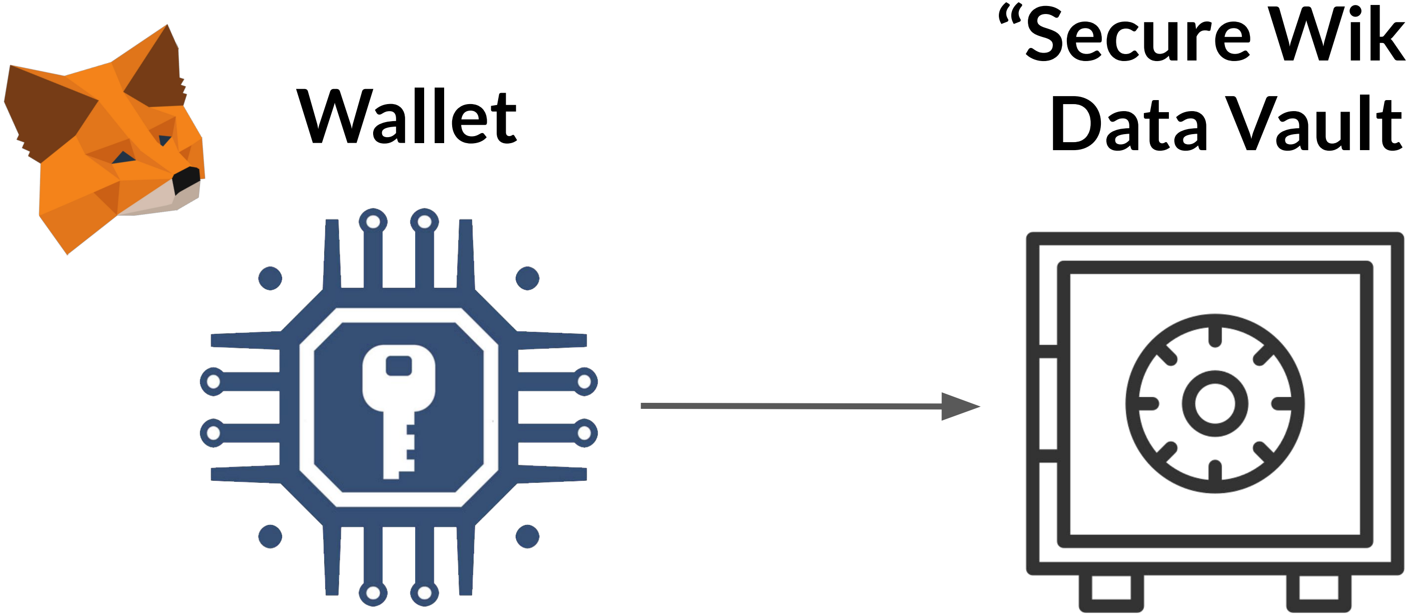
- **Service 1**: Enabling **digital signatures** through wallets
- **Service 2**: Safeguarding **data integrity**
- **Service 3**: Providing **cryptographic timestamping**

Enabling new methods of contract and access management!

Services 1: E-Signature Service

- Allow for passwordless login with your digital signature (optional)
- Digitally sign documents with secure and verifiable signatures
- Track progress and responsibilities using BlueSpice workflows
- Keep all documents within your organization for signing
- Verify signatures with a browser extension by someone without your infrastructure via an offline browser or command line extension

Separation of Concerns



Wallet

“Secure Wiki”
Data Vault

ID-Key

Service

Wallet / Data-Vault

“Secure Wiki”

Wallet’s ONE JOB: KEEP PRIVATE KEYS SAFE!

- Should be stupid, simple, safe
- Operations:
  - Signing
  - De- / Encrypt
  - Publishing transactions to service (e.g. witness networks)
- Ability to choose “high level of assurance”
- Takes care of key recovery mechanisms

Data-Vault - KEEP DATA SAFE!

- Air Gapped on local machine
- All actions authorized though wallet
- General data governance (maximum flexibility -> we use mediawiki)
- Encrypt / Protect data
- Strong access control
  - Share / Publish private data
- Backup / Recovery

Secure your private key by password

The Metamask web-wallet alone has a low (level 1) level of assurance.

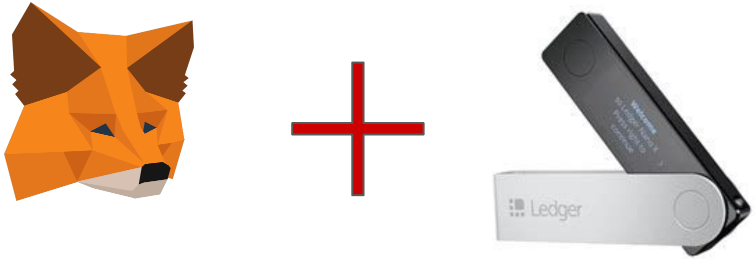
MetaMask is the most common browser blockchain wallet applications on the web and their developer teams strive for increased security to keep crypto-assets of their 10 Million+ Users safe. We use it mainly **OFFLINE as a distributed key management software.**

- MetaMask requires a password to be unlocked

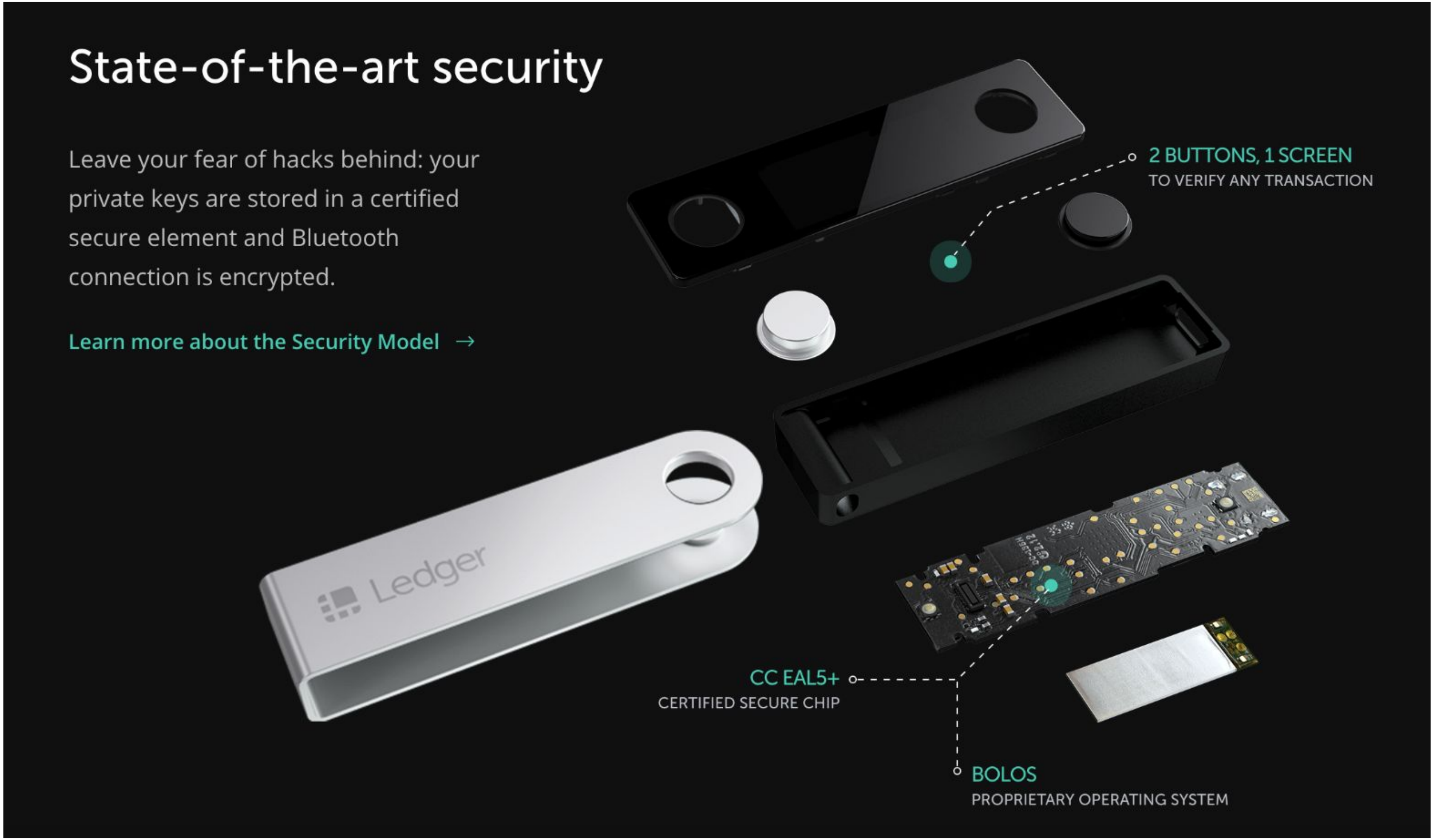
Secure your private key with protected hardware

Metamask offers integration with Hardware-Wallets which raises the level of assurance by having at least 2 authentication factors:

- e.g. a token with a password or pin for min. level 2
- the hardware-tokens are build to be tamper proof (Ledger, Trezor)
  - ○ E.g. Ledger X EAL5+ Certified (See Product-Page)



Product Page



State-of-the-art security

Leave your fear of hacks behind: your private keys are stored in a certified secure element and Bluetooth connection is encrypted.

Learn more about the Security Model →

Demo: Passwordless login with a Wallet

- Replacing Password and Username
- LDAP Users can be extended with wallet address as attributes to login into services which support OIDC
- Show: Metamask Webextension
- Show: Login into
  - matrix https://app.element.io/#/login
  - Secure Wiki Testinstance https://pkc.inblock.io
- See basic local address to name-resolution
- Signing a message (see with the userpage creation)

Digital ID as a Wallet (possible integration, not yet integrated)

Möglichkeit die auf Ihrem Personalausweis hinterlegten Daten einzusehen.

- Integration can be extended with other powerful methods for digital signing
- Digital ID "Digitaler Personalausweis" provided by Governikus GmbH

Service 2: Integrity Verification

Safeguard against manipulation:

- Unauthorized access by hackers
- Malicious employees altering records
- System errors corrupting data

Integrity Verification

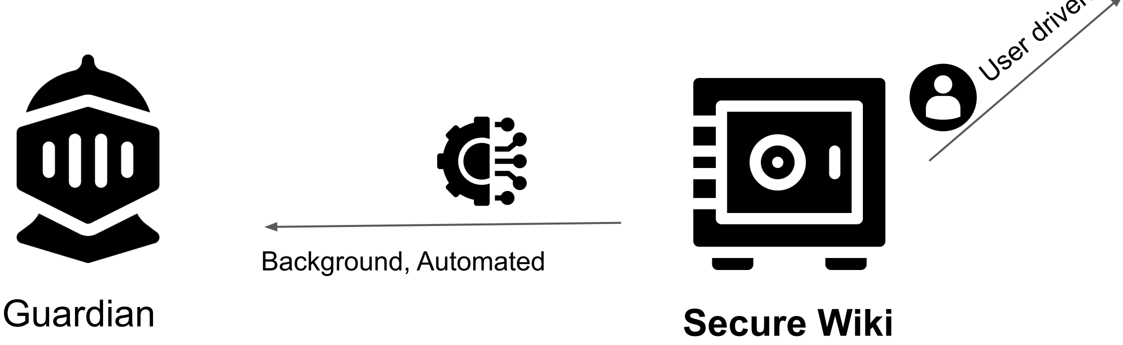
- Ensure your data remains trusted with a **immutable revision history** **(**hash-chains**)**
- Also **Immutable links** (we link hashes which belong to revisions)

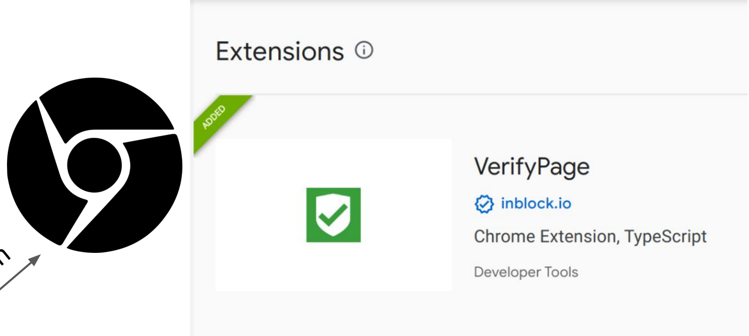
Scenarios:

- Audit trail
- Integrity check after backup and recovery
- Cloud integrity security
- …

Services 2: Integrity verification

Verify by Guardian or Browser-Extension



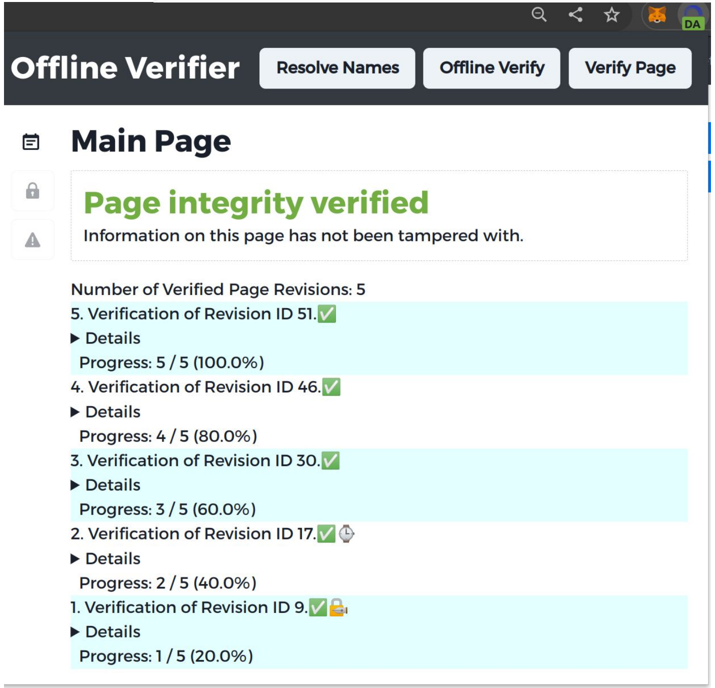


VerifyPage

inblock.io

Chrome Extension, TypeScript

Developer Tools



Main Page

Page integrity verified

Information on this page has not been tampered with.

Number of Verified Page Revisions: 5

5. Verification of Revision ID 51.✅
▶ Details
Progress: 5 / 5 (100.0%)

4. Verification of Revision ID 46.✅
▶ Details
Progress: 4 / 5 (80.0%)

3. Verification of Revision ID 30.✅
▶ Details
Progress: 3 / 5 (60.0%)

2. Verification of Revision ID 17.✅⏱
▶ Details
Progress: 2 / 5 (40.0%)

1. Verification of Revision ID 9.✅🔏
▶ Details
Progress: 1 / 5 (20.0%)

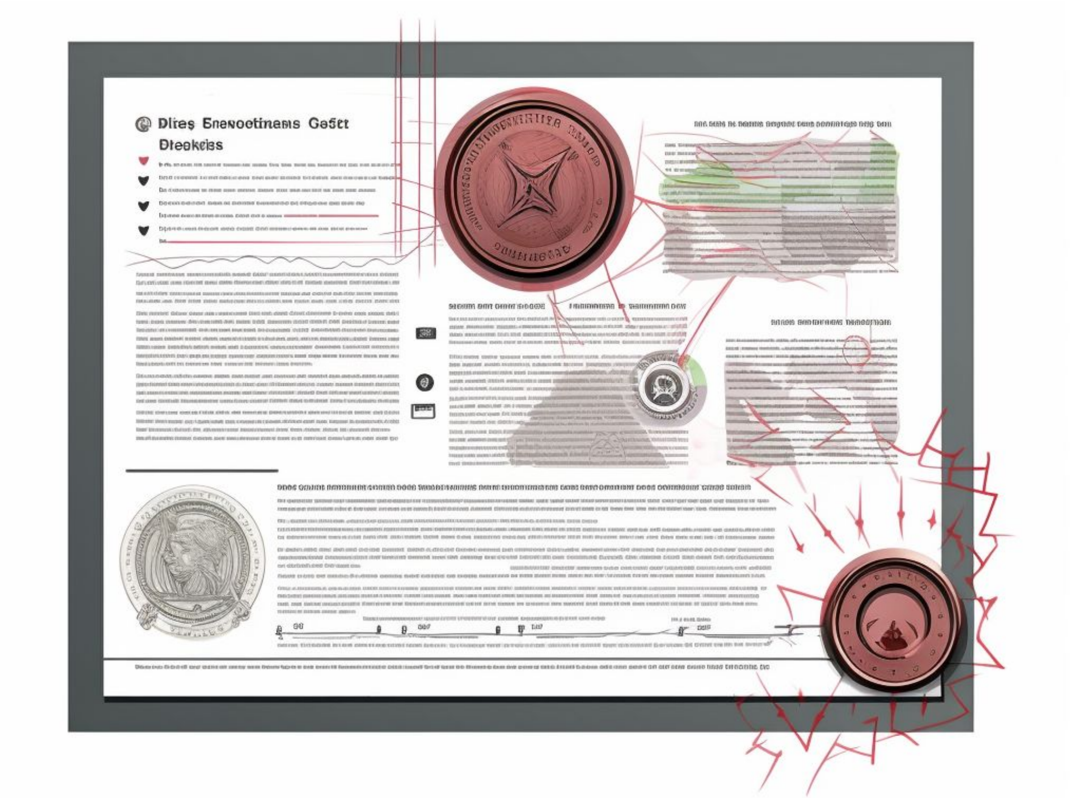
- Retrieves articles and validates them against their cryptographic metadata
- Returns cryptographically secure log files

Demo

- Integrity of an article
  - see “Very important contract”
- See failed signature (attack of eve)
- See failed integrity (attack of eve)
  - Classification of data (Fake-News)
  - Documentation of events (Historian)
- See import / export procedure
- See immutable Links in action
- See offline verification

Service 3:
Digital Cryptographic Timestamping

Service 3 : Integrity + Signature + Timestamping = E-Notary



Service 3: Digital Cryptographic Timestamping

- To prove to a third party that a document hasn't been altered (by regenerating one with cryptographic metadata), **a proof of existence through cryptographic timestamping** is needed
- Digital cryptographic timestamping serves as a **secure, tamper-proof method for validating document authenticity, providing an additional layer of trust and credibility**
- Timestamping can also help **resolve disputes by providing irrefutable evidence of the documents* existence** and its contents at a specific point in time

Benefits of Timestamped, Verified, and Signed Documents

Enables machine and human-readable contracts

- Digital signatures prevent forgery and establish accountability
- Integrity verification ensures document authenticity
- Timestamping provides a clear, unalterable timeline

We integrate with various files:

- Supports various file format including Office documents, PDFs, photos and videos
- Allowing for export and import of articles with cryptographic meta-data

Secure Wiki Services + Guardian:

The perfect solution for legally compliant data management

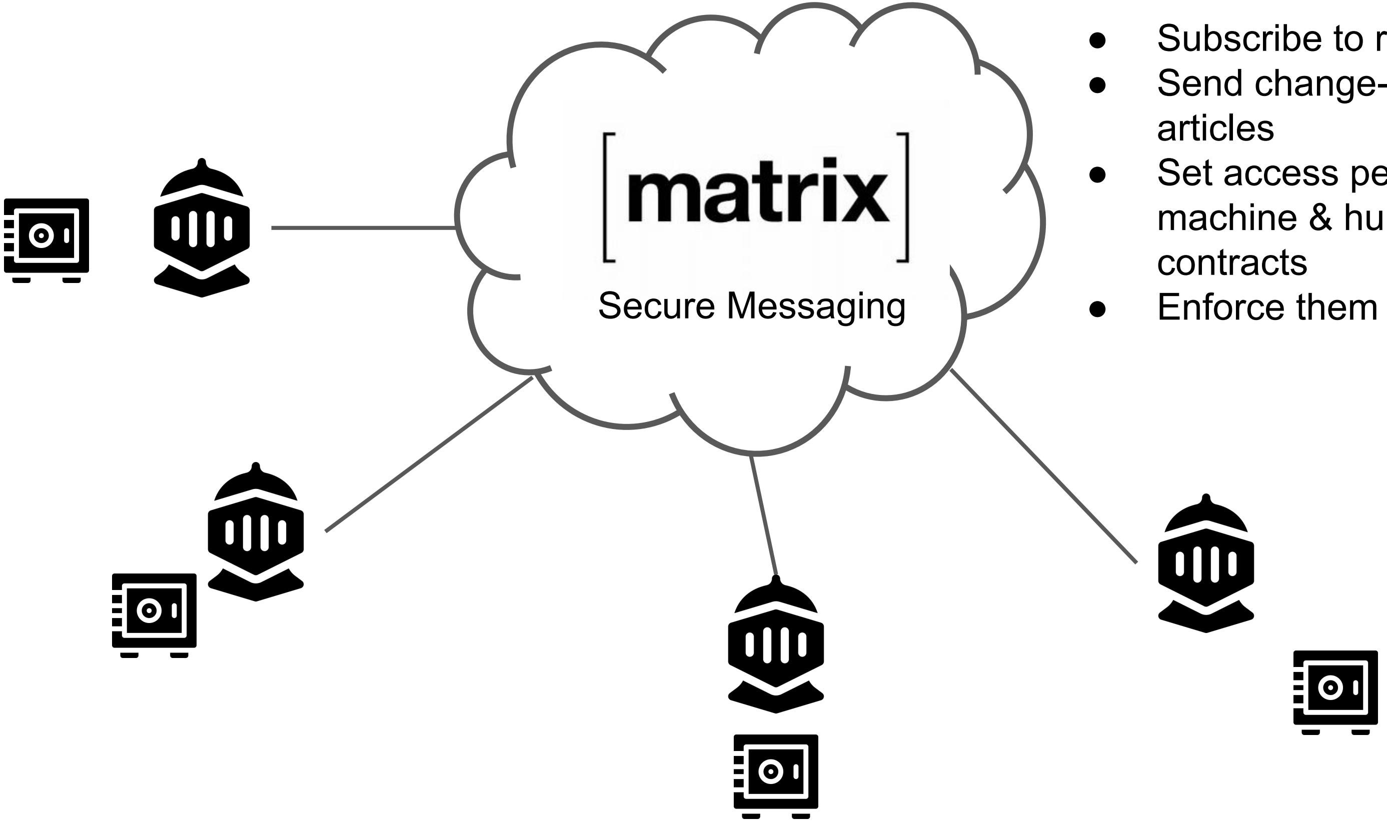
- With BlueSpice and **Secure Wiki** Services, you get a separated data vault **for confidential documents**.
- Your contract drafts remain traceable who has worked on them at all times through signatures and changes are revision-proof stored.
- Facilitates efficient, secure, digital contract management

Demo - Digital Timestamping

- Digital Timestamping
  - Generate Snapshots
  - Publish Snapshots to Ethereum
  - Look into the verifier to see how it looks like
    - Show manipulation failure

The road ahead

Roadmap - Peer-to-peer Secure Wiki



- Subscribe to remote articles
- Send change-proposals to remote articles
- Set access permissions with machine & human readable contracts
- Enforce them with Guardians

Call for action

- Speak to Hallo Welt! GmbH to schedule a shared meeting to **piloting** this software with Hallo Welt! GmbH & inblock.io assets GmbH or if you want to learn more about it
- Learn more about it at Hallo Welt! Website https://bluespice.com/de/secure-wiki/
- Projekt page and source code at https://aqua-protocol.org/ with Github Link.
- Testinstance: https://pkc.inblock.io (Until Friday)