White Paper

How to Implement Blockchain in a Compliant Manner for Banking

The first implementation of the blockchain was designed to protect and keep track of Bitcoin currency transactions.

Since that time, the use of blockchains has spread into many other industries, including banking, finance, and Fintech where a higher level of security assurance is required to keep customer information secure and to comply with a higher standard of security as required by regulators. The blockchain has also found its way into industries that one might not consider at first thought, like media, marketing, travel, and even music streaming.

utimaco®

Blockchain use has grown globally over the last several years. During 2017:

- ➔ Payment and wallet application share were greater than 50%
- ➔ Infrastructure provider market share was 65%
- ➔ North America market share was greater than 50%
- ➔ Europe market share was greater than 25%
- ➔ Global industry size was greater than 200 million

Consider blockchain's future estimates for global market size:

- ➔ APAC market CAGR is expected to be greater than 87% by 2024
- ➔ CAGR is expected to reach more than 75%
- ➔ The blockchain industry is expected to grow to more than $16 billion by 2024
- ➔ By 2024, growth for application providers sector CAGR will be greater than 85%
- ➔ Digital identity application CAGR will reach over 90% by 2024

What is a Blockchain?

Simply put, a blockchain is a chain of blocks, where each block is digital information that is stored in a public or private database (chain). Thus, a blockchain is a growing list of records/transactions (blocks) that are linked using cryptography. Each block in the chain consists of three crucial parts:

1. A cryptographic hash of the previous block
2. A timestamp
3. Transaction data

Each block contains batches of valid transactions that have been hashed and encoded into a Merkle tree. The presence of the cryptographic hash of the previous block links the two blocks to form a chain.

Because of its design, a blockchain resists modification of the data that it contains. Once data has been recorded into a block, it cannot be altered without altering all subsequent blocks in the chain, which would then require the consensus of the network majority. This allows participants of the blockchain to independently and relatively inexpensively verify and audit transactions.

Blockchains are also designed to implement infinite-size ledgers. Thus, a blockchain can expand to accommodate the recording and totaling of an infinite number of economic transactions. Even though the records in a blockchain could be altered blockchains are considered secure by design and represent a distributed computing system with a high level of Byzantine fault tolerance.

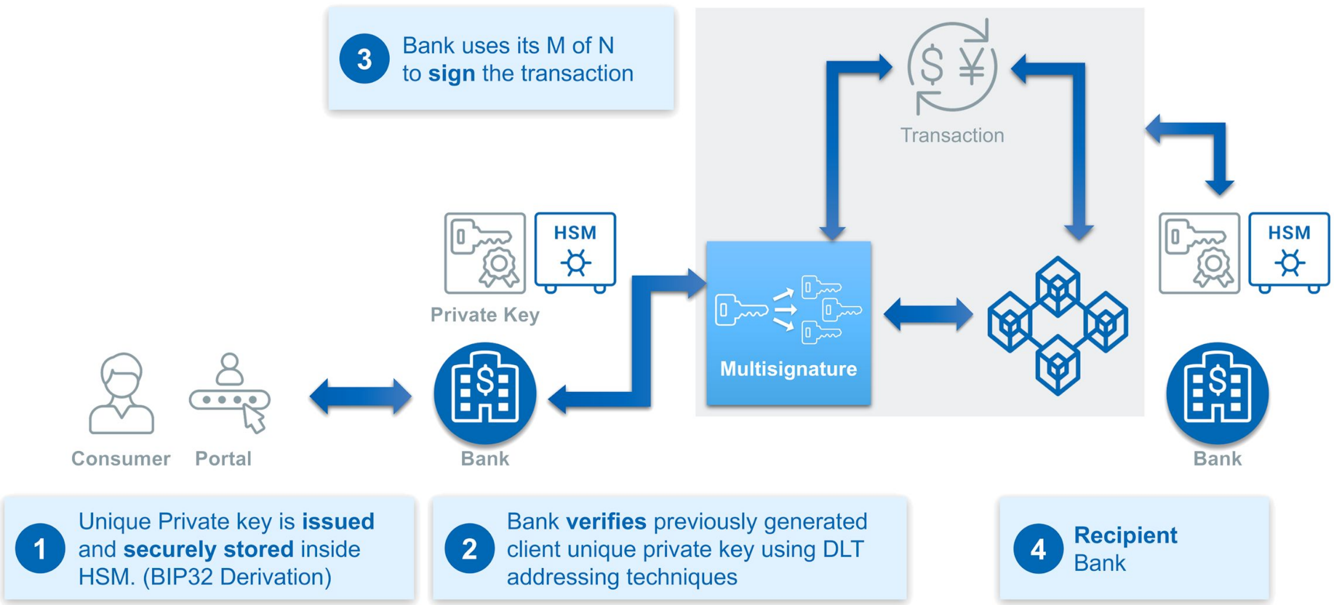
Permissioned Blockchains

Blockchain networks are decentralized networks and their power comes from the forced cooperation between distrusting parties, thus reducing the risk of an 'inside' criminal conspiracy against a system.

Permissioned blockchains differ from simple 'private' blockchains in the sense that there are multiple layers requiring special permissions to operate. The end-goal of a blockchain is almost always to prevent inner fraud from within a network of users (banks, notaries, insurances, etc.).
The way that blockchains can prevent fraud from within a system is by creating a chained record of blocks that grows over time, and where the records are under 'collective' control and validation.

Here is the main lifecycle of a transaction in a permissioned blockchain system:

- ➔ The transaction is ciphered and added to a distributed ledger;
- ➔ All the relevant parties with authorization to access the shared ledger check the details of the transaction;
- ➔ Checked transactions are concatenated as a permanent, immutable component of the shared ledger;
- ➔ The transaction is completed.



3 Bank uses its M of N to **sign** the transaction

1 Unique Private key is **issued** and **securely stored** inside HSM. (BIP32 Derivation)

2 Bank **verifies** previously generated client unique private key using DLT addressing techniques

4 **Recipient** Bank

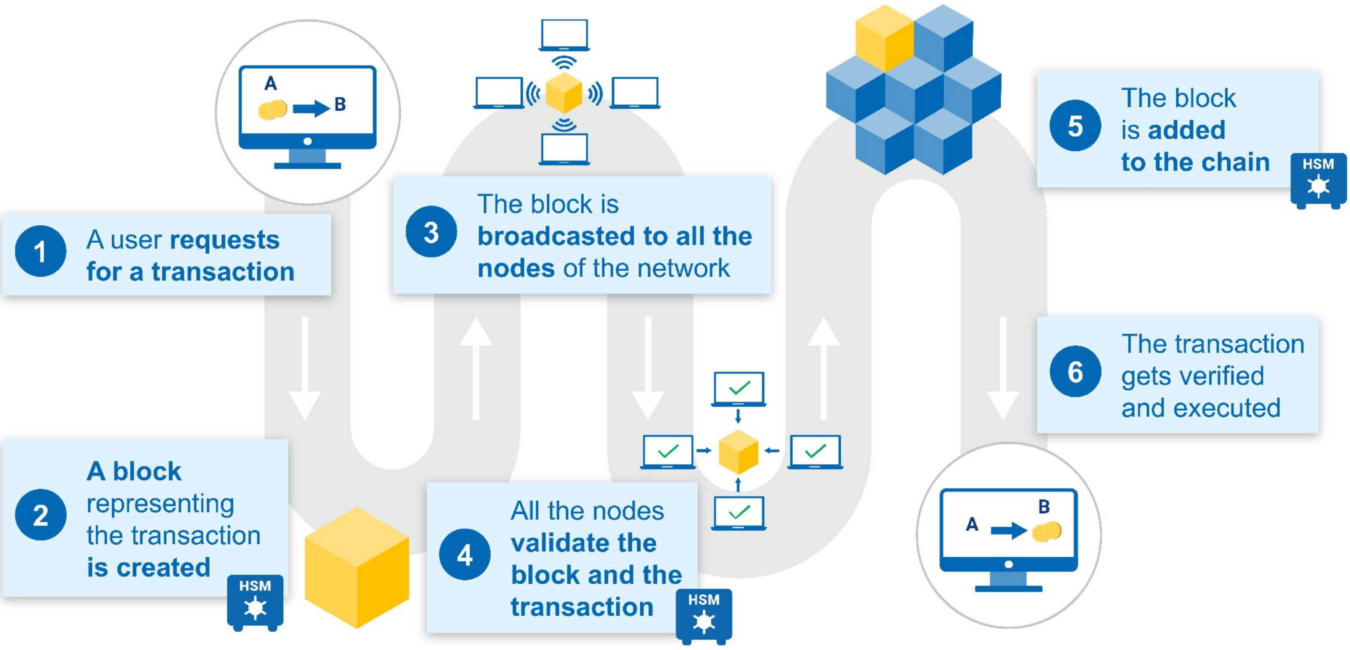
While there are many different types of blockchains, they do have several important similarities:

- ➔ Centralized/Decentralized/Distributed
- ➔ Consensus model (proof of work/state/ID)
- ➔ Public/Private
- ➔ Anonymous/Known Identities

What is a Blockchain?

So how does blockchain work? The process itself could simply be explained in six steps:

1. The user initiates a transaction.
2. A block is created to represent the transaction.
3. The block is then broadcasted to all the nodes within the network.
4. The block and transaction are then validated by all the nodes.
5. The new block is added to the chain.
6. The transaction is verified and executed.


A
B
1 A user requests for a transaction
2 A block representing the transaction is created
HSM
3 The block is broadcasted to all the nodes of the network
4 All the nodes validate the block and the transaction
HSM
5 The block is added to the chain
HSM
6 The transaction gets verified and executed
A
B

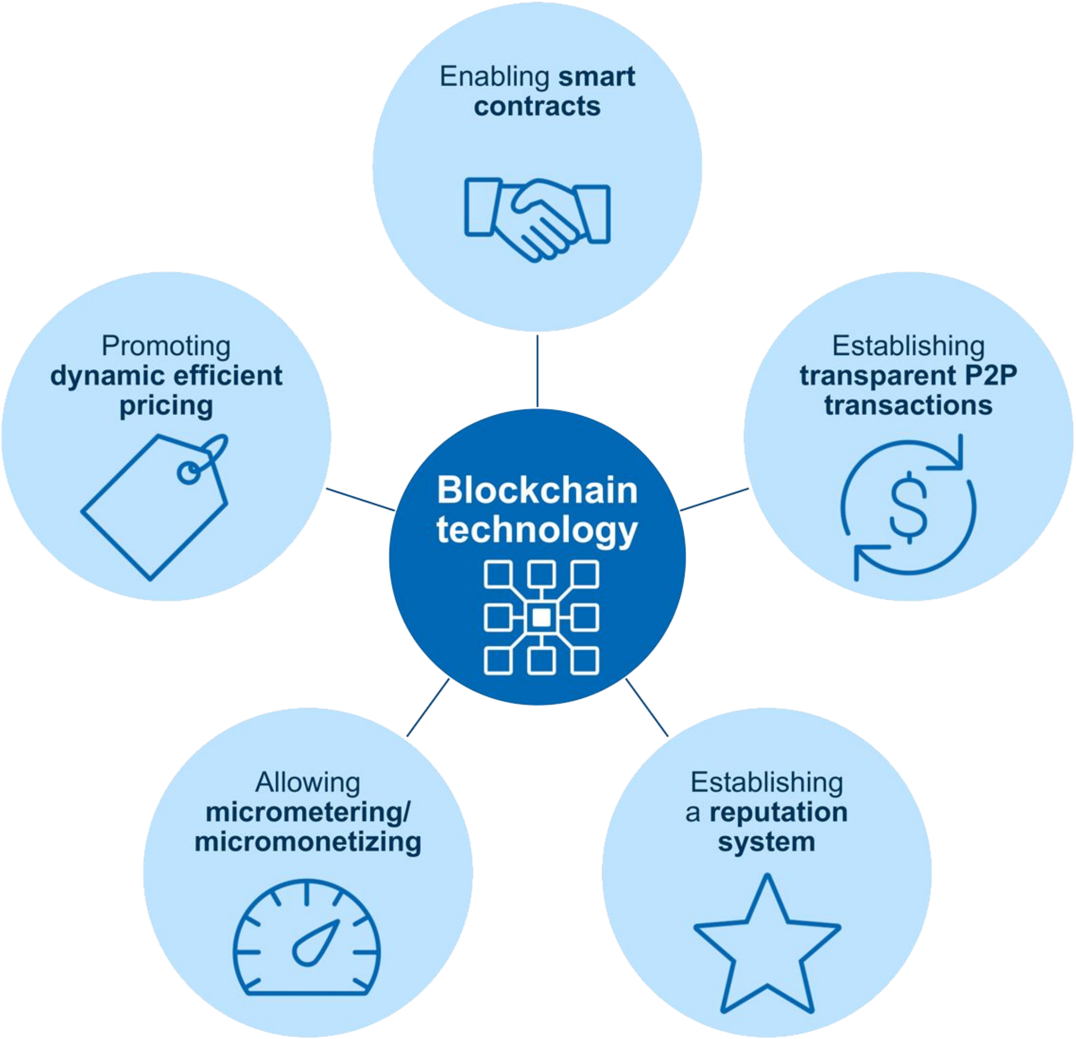
Blockchain and the Banking and Financial Sector

Originally, the technology of the blockchain was conceptualized in 2008 by the entity known as Satoshi Nakamoto. Nakamoto built upon the 1991-1992 work by Stuart Haber and W. Scott Stornetta to design a system where document timestamps could not be tampered with by adding a hash method to timestamp block. The original use of the blockchain was to serve as a public ledger for all cryptocurrency bitcoin transactions on the network. Introducing the blockchain to the banking and financial sector is, of course, the next step in the evolution of this technology to improve the security of financial records and transactions.

Blockchain in the Banking and Financial Sector

For the banking and financial sector, blockchain technology provides the following benefits:

- ➔ Smart contracts through computer protocols to verify, enforce negotiation, and performance of contracts
- ➔ Establishing transparent P2P transactions
- ➔ Establishing a reputation system that allows ratings by online communities to build customer trust
- ➔ Micro-metering/micro-monetizing e.g. allowing for paying for usage for transportation per meter or streaming services by the hour
- ➔ Promoting dynamic efficient pricing based on demand


Enabling **smart contracts**
Promoting **dynamic efficient pricing**
Blockchain technology
Establishing **transparent P2P transactions**
Allowing **micrometering/ micromonetizing**
Establishing a **reputation system**

Key Requirements Where Blockchain Can Help

The banking and financial sector has always faced challenges with customers' pain points. There are three main challenges facing the industry.

#1. Compliance with know-your-customer regulations

The banking and financial sector is responsible for complying with numerous regulations to protect the PII of its customers. It is also responsible for protecting their customers' savings, investment funds, and other money accounts against fraudulent activity. Implementing blockchain technology can help with maintaining compliance with regulations like:

- ➔ FINTRAC
- ➔ RBI
- ➔ USA Patriot Act
- ➔ Anti-Money Laundering
- ➔ PSD2

An added benefit of a blockchain is that it enhances the traceability of fraudulent transactions.

#2. Time to "completion" for "service"

Time is money with all businesses, and this especially includes the banking and financial sector. Delays in completing services for customers such as international money transfers or cross-border transactions can be frustrating for customers who will, in turn, seek the services of competitors who are better equipped to meet their needs. Blockchain technology can reduce lag times due to ensuring secure transactions.

#3. Increases bottom-line margins

Implementing blockchain technology helps increase bottom-line margins through internal operational cost savings and external cost savings.

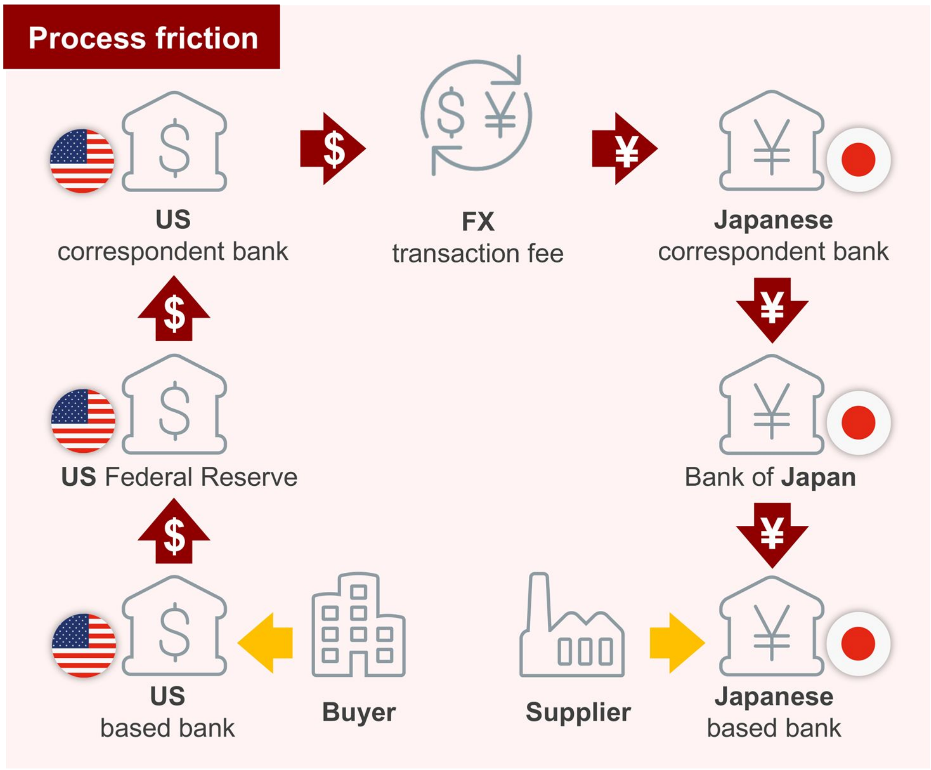
Blockchain Use Cases

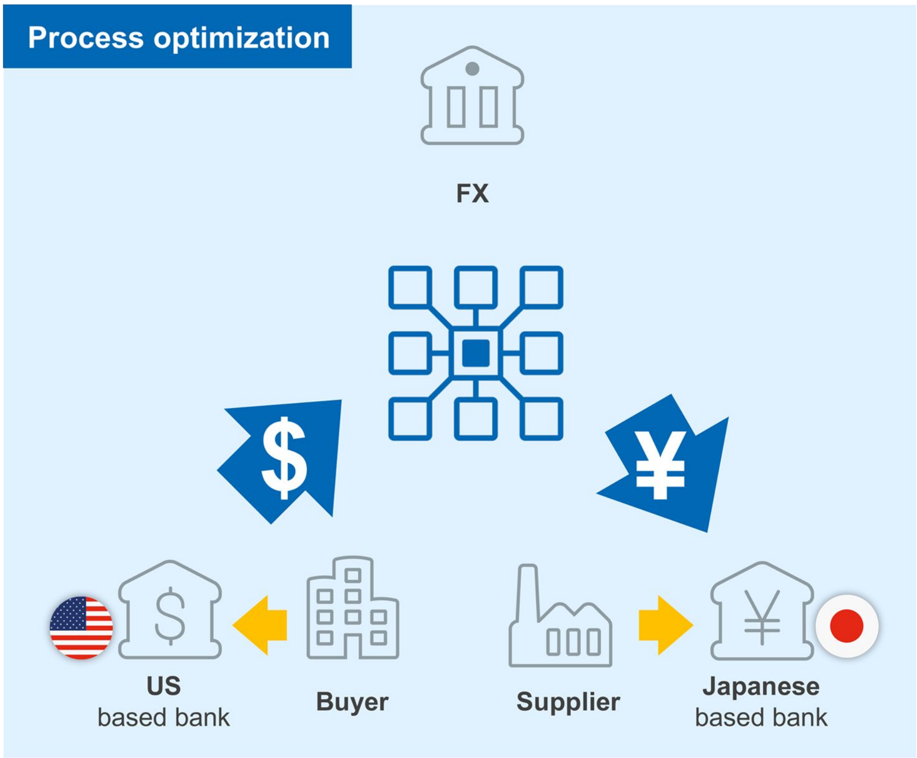
Consider the following use cases to see how a blockchain can be the answer to solving customer pain points.

Cross-Border/Interbank Transactions

Consider a financial transaction between a United States correspondent bank and a Japanese correspondent bank. The transaction process hits friction as it must hit on nine different contact points to complete the transaction.

Blockchain Use Cases - Cross-Border/Interbank Transactions



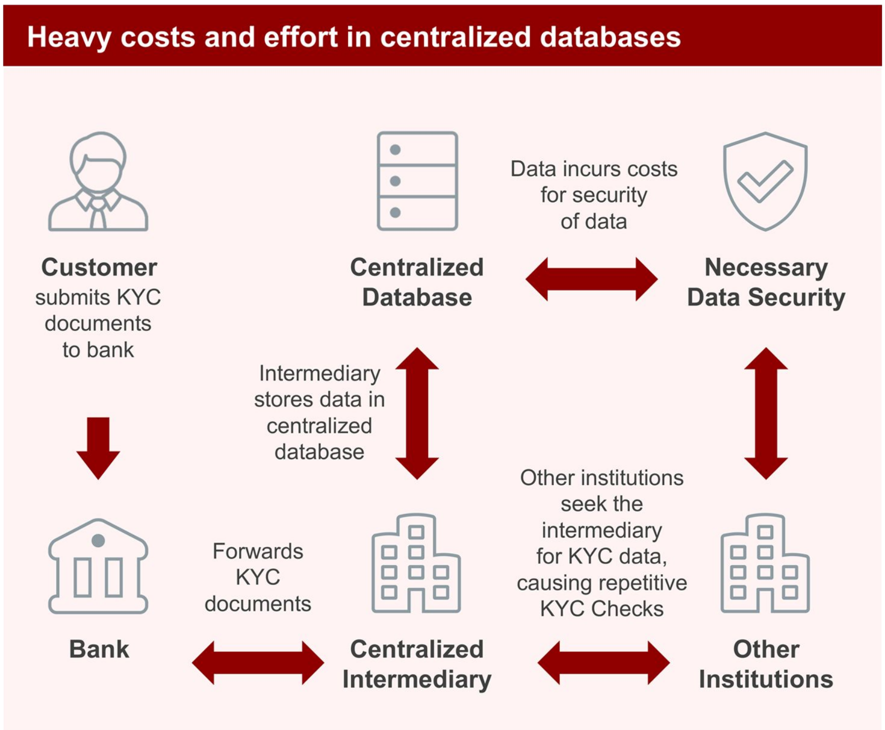


Now consider how a blockchain can optimize the cross-border/interbank transactions by eliminating three contact points, thus decreasing the time needed to process such a transaction.

Blockchain Use Cases

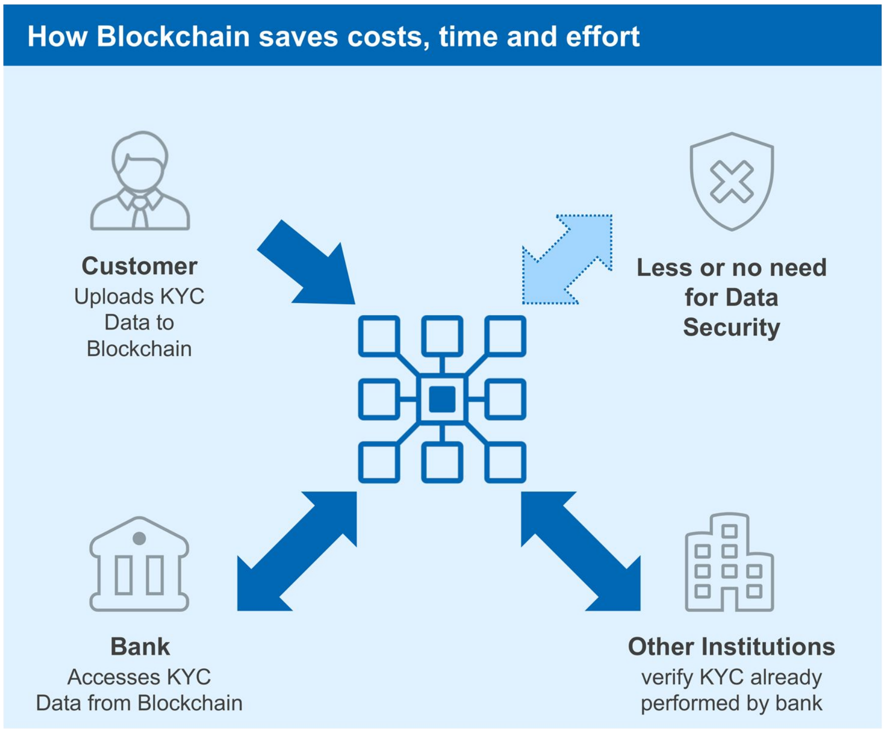
KYC/AML

Consider the heavy costs and effort needed to maintain centralized databases to handle customer KYC documents. Before blockchain, a customer would submit their KYC documents to the bank who would then send the documents to a centralized intermediary where the data is stored in a centralized database where it is kept secure and can be accessed by other institutions when KYC data is needed, thus causing repetitive KYC checks.


Heavy costs and effort in centralized databases

Customer
submits KYC documents to bank
Centralized Database
Data incurs costs for security of data
Necessary Data Security
Intermediary stores data in centralized database
Bank
Forwards KYC documents
Centralized Intermediary
Other institutions seek the intermediary for KYC data, causing repetitive KYC Checks
Other Institutions

Now consider how blockchain can save costs, time, and effort by reducing or eliminating the need for expensive data security. Instead of submitting KYC data to the bank, the customer would upload it to the blockchain. The bank can then access the KYC data from the blockchain, and other institutions can then verify KYC that has already been performed by the bank.


How Blockchain saves costs, time and effort

Customer
Uploads KYC Data to Blockchain
Less or no need for Data Security
Bank
Accesses KYC Data from Blockchain
Other Institutions
verify KYC already performed by bank

Utimaco's HSM for Blockchain Solution

An HSM is a crucial part of the blockchain to secure cryptographic key generation. Utimaco's blockchain technical value proposition offers:

- ➔ Generation of private and public key pairs, including specific elliptic curves, Bitcoin and Ethereum blockchain Secp256k1, and Stellar Ed25519.
- ➔ Proven secure storage of Secure storage for private keys for regulations e.g. PSD2, GDPR
- ➔ Built-in consensus enforcement, M of N to authorize / Multisign MultiSig M keys to authorize/consensus
- ➔ Hierarchical deterministic wallet support for the ability to scale effectively with industry specific required key derivation mechanisms such as with the ability to derive key-pairs in a secure environment from a single key master in accordance with BIP32
- ➔ Encryption, decryption, and use keys records from key databases in a secure environment
- ➔ Auditing and logging for traceability of a transaction by whom from M of N including final commit Logging with the ability to audit and monitor how and when keys are used to provide an additional layer of security.

The HSM

For the most secure compliant solution, a blockchain should always be used with an HSM for secure cryptographic protection of data privacy, integrity and auditability including:key generation.

- ➔ To effectively integrate new deployments into existing ecosystem and meet strict compliance requirements e.g. Smart Automobile Payment enabled leveraging Blockchain
- ➔ For built-in Algorithms, DLT platforms maintained, supported with latest releases and security updates

Utimaco is one of the leading HSM vendors for blockchain and can be your trusted partner in the blockchain ecosystem.

Utimaco Solutions

Block-safe

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

Read more

CryptoServer CP5 (eIDAS & CC)

The Utimaco CryptoServer CP5 is based on the CryptoServer Se Gen2 hardware platform and Common Criteria-certified according to the eIDAS Protection Profile (PP) EN 419 221-5 “Cryptographic Module for Trust Services”.

Read more

CryptoServer cloud

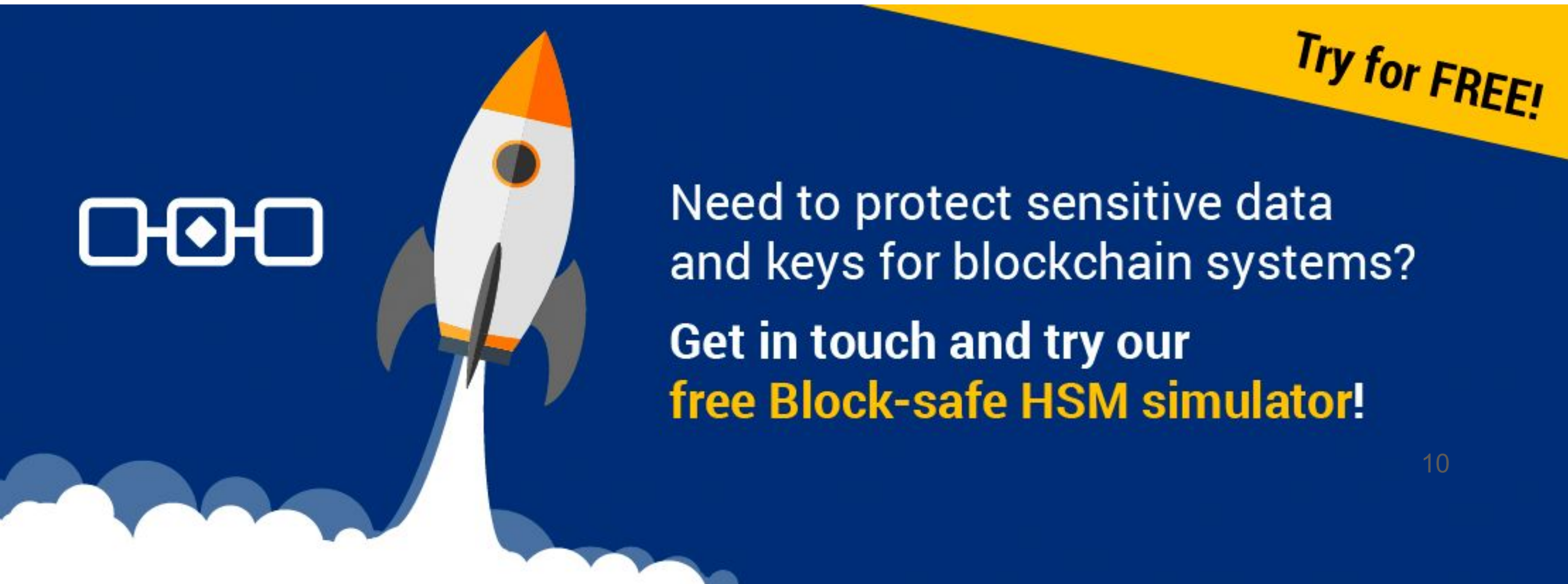
Utimaco CryptoServer Cloud gives you a strategic architectural fit & risk management for your high value assets in a multi-cloud environment!.

Read more

Multi-cloud agility

The advantages of the cloud – ranging from reduced cost and dependence on corporate data centers, to improved scalability, flexibility, performance – are all making the cloud a seemingly inevitable IT strategy for businesses. But what are the challenges of a multi-cloud strategy and how to solve them?

Read more


Try for FREE!
Need to protect sensitive data and keys for blockchain systems?
Get in touch and try our
free Block-safe HSM simulator!

About HSM and Utimaco

About HSMs

HSMs are essential in protecting, managing and securing sensitive cryptographic assets, such as digital encryption keys, custom IP and asset access. Utimaco is now driving a new era as its HSMs are facilitating digital transformation in many key areas including, but not limited to, banking and payments, encryption and blockchain. Utimaco's goal is to protect sensitive data assets in the eventual wake of quantum computing.

About Utimaco

Utimaco is a leading manufacturer of Hardware Security Modules (HSMs) that provide the Root of Trust to many industries, from financial services and payment to the automotive industry, cloud services and the public sector. We keep cryptographic keys and digital identities safe protecting your critical digital infrastructures and high value data assets. Founded in 1983, today Utimaco HSMs are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 260 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit https://hsm.utimaco.com/.