SOLUTION BRIEF

Bringing Trust to Blockchain with Gemalto HSM and SAS Solutions

Blockchain is one of those industry buzzwords that you seem to hear everywhere, but what exactly is it and can you trust it? For the most part, enterprises are implementing blockchain without truly understanding its purpose, and as much as 90% of enterprise blockchain projects launched this year will meet a premature end within 18 to 24 months.* Let us take the mystery out of blockchain and its use cases, and demonstrate how Gemalto can keep your transactions secure.

What is blockchain?

A blockchain is a distributed ledger technology that preserves a continuous chain of records called blocks. Each block is timestamped and linked to previous blocks, using cryptography to verify all records. Unlike traditional approaches, blockchain eliminates the need for centralized control – instead all transactions are decentralized, and verified by the blockchain database itself in the distributed ledger. Contrary to the most popular use case, blockchain technologies don't only secure financial transactions – in fact they can be used to track and verify any kind of digital asset, as well as code or smart contracts. Blockchain use cases include the sharing of medical records, processing IoT transactions, and record keeping for the public sector.

Popular Blockchain Use Cases

#1 Cryptocurrency

A cryptocurrency is a digital form of currency that can transferred between two parties, using cryptography to ensure the transaction is secure. There are over 700 cryptocurrency companies in the world including Bitcoin, Ethereum, Ripple, and Monero, all with their own customized blockchain technologies. The decentralized approach to control used by cryptocurrencies is opposite to our traditional centralized banking systems.

#2 Smart Contracts

Smart contracts are becoming one of the main use cases of blockchain technology. A smart contract is a computer program that describes an agreement. The details of a smart contract are recorded as a set of instructions, preprogrammed with the ability to self-execute and enforce the terms of a contract. Smart contracts allow two anonymous parties to conduct business without the need or cost for a middleman, however many enterprise applications require the parties to be known and authenticated.

#3 Internet of Things (IoT)

Blockchain records a ledger of transactions between devices, web services, and humans, providing a way to track the unique history of interaction. Additionally, blockchain can also enable smart devices to become independent agents, autonomously conducting a variety of transactions. The combination of blockchain and IoT will enable machines to order stock, operate during the most economical times, pay for the delivery of new items, and solicit bids from distributors, to name a few.

Benefits of Blockchain

- Eliminates the need for centralized control
- Trust is distributed between blockchain members
- Transactions are digitally signed using an asset owner public/private key pair
- Once recorded, data in a block cannot be altered retroactively
- Open, distributed ledgers record transactions between two parties efficiently and in a verifiable and permanent way
- Transactions don't have to be just data – they can also be code or smart contracts

Gemalto - Brings Trust to Blockchain

Gemalto secures blockchain in the following three areas: providing strong identities and authentication to gain access to the blockchain; securing core blockchain technologies; and securing communications across the blockchain network.

Strong Identities and Authentication

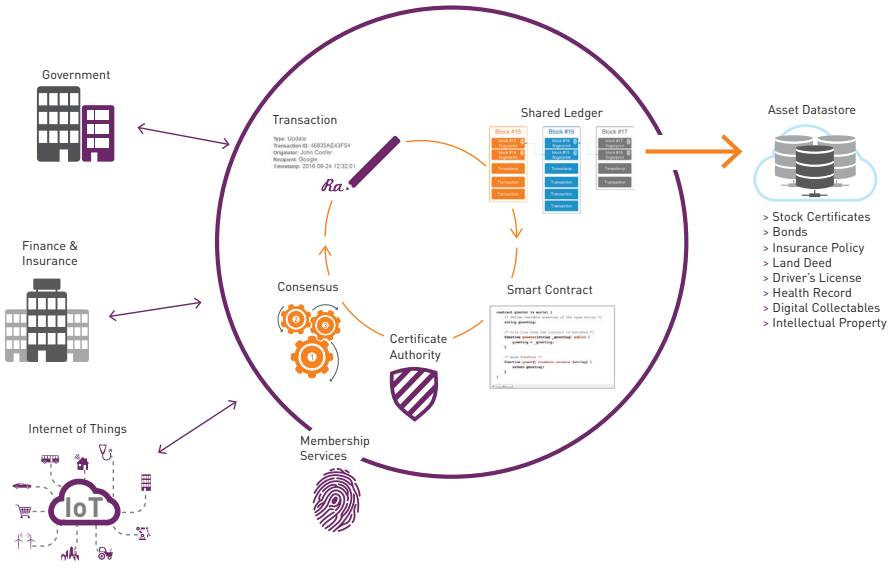
Gemalto provides strong identities to devices and humans using "permissioned" blockchains – where the identity of all members are known.

The Gemalto Public Key Infrastructure (PKI) solutions provide digital identities to devices, commonly called certificates. These technologies are widely used by enterprises today to provide strong authentication and data encryption, and continue to play a critical role in blockchain environments.

For humans using blockchain, SafeNet Authentication Service (SAS) delivers fully-automated, highly secure authentication-as-a service with flexible token options. SAS is tailored to the unique needs of your organization, substantially reducing the total cost of operation.

** Gartner Top 10 Mistakes in Enterprise Blockchain Projects*

Blockchain as an Infrastructure



Securing Core Blockchain Technologies

Public-key cryptography is the fundamental security foundation used by blockchain. The process of securely generating, using and storing cryptographic keys is essential to maintain the security of the blockchain network. Moreover cryptography is used to sign smart contracts to prove their origin, and secure data stored both on and off the blockchain to provide confidentiality of transactions.

Hardware Security Modules

SafeNet HSMs ensure absolute trust by securing cryptographic keys and identities in a hardware root of trust. Only HSMs can provide server side protection of private keys with FIPS 140-2 Level 3 certification. Cryptographic keys kept in software are at risk of theft which compromises the entire blockchain ledger.

SafeNet Luna Network HSMs

SafeNet Luna Network HSMs are dedicated cryptographic processors specifically designed to protect cryptographic keys throughout their lifecycle, and act as a root of trust for the cryptographic infrastructures of the most security conscious organizations in the world. SafeNet Luna Network HSMs store the private keys used by blockchain members to sign all transactions, and ensures that cryptographic keys cannot be used by unauthorized devices or people.

SafeNet ProtectServer HSMs

Like the SafeNet Luna Network HSM, the SafeNet ProtectServer HSM is designed to protect cryptographic keys against compromise while providing encryption, signing, and authentication services. Additionally, SafeNet ProtectServer HSMs use Functionality Modules (FM) to allow the latest blockchain algorithms to be secured in FIPS 140-2 Level 3 certified hardware.

SafeNet ProtectServer HSM FM benefits include:

- Unique level of flexibility for application developers
- Create your own firmware to support the latest blockchain developments using custom FMs
- Ability to execute FMs within the secure confines of the HSM

Securing Communications

SafeNet HSMs are also used to generate and securely store cryptographic keys used in TLS and SSL network connections. TLS and SSL provide a secure method for managing authentication and exchanging messages, securing the integrity of the blockchain transactions.

Gemalto and Blockchain

- Bring trust to blockchain events
- Ensure against unauthorized access of cryptographic keys with FIPS 140-2 Level 3 validated hardware protection
- Hardware root of trust enables best practices for an enterprise
- Support for multiple blockchain applications (Bitcoin, Hyperledger, Ethereum, Altcoins, Monero, and more)
- Internal auditability - proof of transactions
- High assurance security in data centers and the cloud
- Multi-tenancy capability of blockchain identities on a per partition basis

Industry-leading Blockchain Partners

Gemalto has partnered with industry-leading blockchain and cryptocurrency partners to provide enterprise-grade solutions for securing transactions. Together with partners such as Symbiont and Ledger, Gemalto is protecting the way industries are conducting business, bringing efficiency and establishing trust.

Gemalto – A Secure Model for Your Blockchain Solution

Blockchain technology is purpose-built for specific applications, but does come with its tradeoffs and risks. Contact Gemalto to determine how we can bring trust and security to your blockchain solution, and ensure against unauthorized access of your cryptographic keys with FIPS 140-2 Level 3 validated HSMs, flexible HSMs for custom FMs, and highly secure authentication solutions.

About Gemalto's SafeNet Identity and Data Protection Solutions

Learn more about Gemalto here: www.gemalto.com/companyinfo/about

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free