cpl.thalesgroup.com

THALES

Thales Brings Trust to Blockchain

Blockchain is one of those industry buzzwords that you seem to hear more and more, but what exactly is it and can you trust it? Many enterprises are implementing blockchain without truly embracing its complete capabilities, and although blockchain is based on sophisticated math and is secure at its foundation with its decentralized approach, there are ways to fool the blockchain to gain advantage.* Let us take the mystery out of blockchain and its use cases, and demonstrate how Thales can keep your transactions secure.

What is Blockchain?

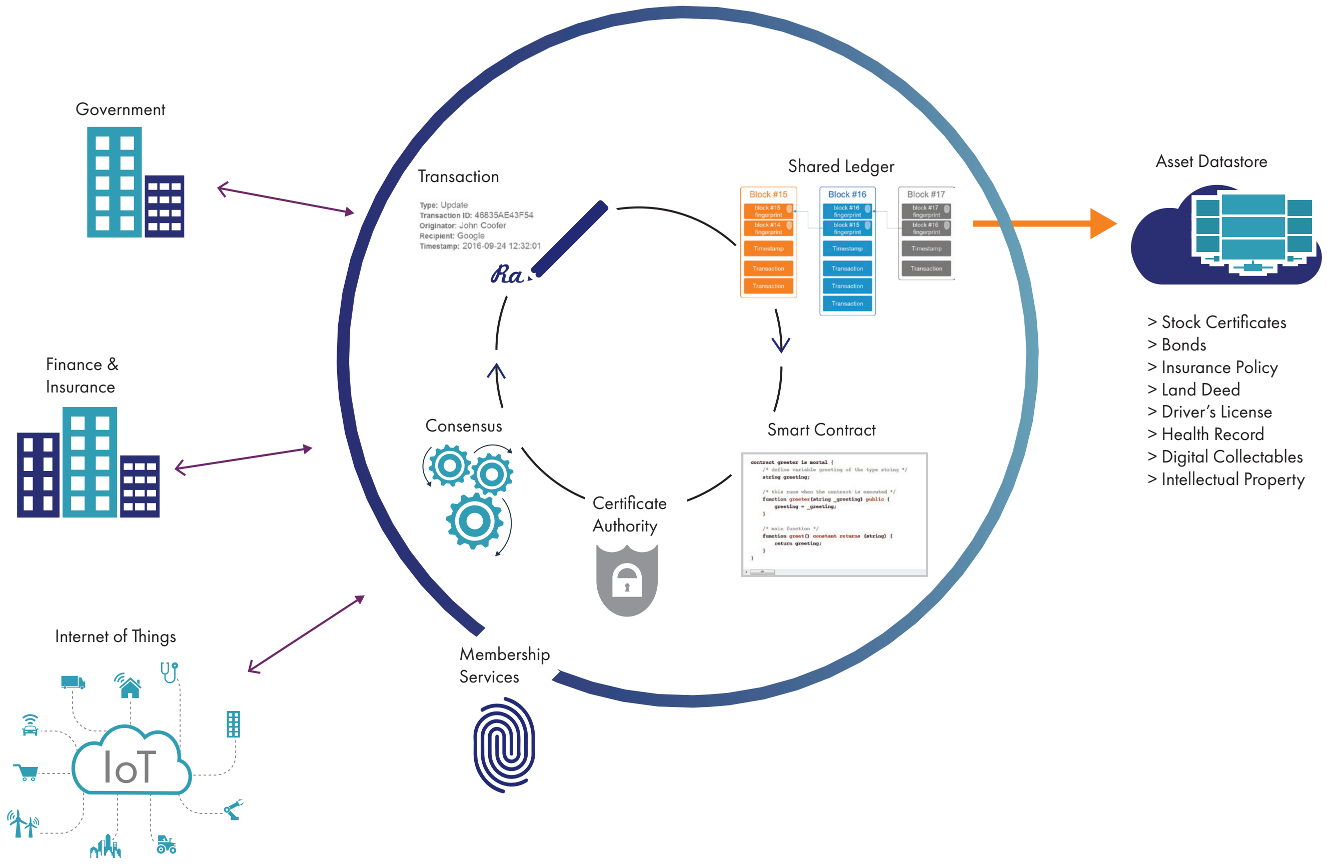
A blockchain is a distributed ledger technology that preserves a continuous chain of records called blocks. Each block is timestamped and linked to previous blocks, using cryptography to verify all records. Unlike traditional approaches, blockchain eliminates the need for centralized control – instead 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.

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

* Gartner Newsroom

Blockchain as an Infrastructure



Type: Update
Transaction ID: 46835AE43F54
Originator: John Coofer
Recipient: Google
Timestamp: 2016-09-24 12:32:01

```
contract greeter is mortal {
    /* define variable greeting of the type string */
    string greeting;

    /* this runs when the contract is executed */
    function greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
```

> Stock Certificates
> Bonds
> Insurance Policy
> Land Deed
> Driver’s License
> Health Record
> Digital Collectables
> Intellectual Property

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 2000 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.

Thales - Brings Trust to Blockchain

Thales 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

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

Thales 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 Trusted Access (STA) delivers fully-automated, highly secure authentication-as-a service with flexible token options. STA is tailored to the unique needs of your organization, substantially reducing the total cost of operation.

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

Thales Luna Hardware Security Modules (HSMs) ensure absolute trust by securing cryptographic keys and identities in a hardware root of trust. Cryptographic keys kept in software are at risk of theft which compromises the entire blockchain ledger.

Thales Luna Network HSMs

Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Luna Network HSMs - high-assurance, tamper-resistant, network-attached appliances offering market-leading performance.

Luna Network HSMs help secure blockchain solutions in a number of ways:

- Secure generation of cryptographic keys including RSA, Elliptic curves (secp256k1, Ed25519 and others)
- Secure storage of private keys in FIPS 140-2 Level 3 hardware
- Signing and verifying transactions
- Hierarchical deterministic wallet support using BIP32
- Strong authentication to generate and use keys

Luna Network HSMs are also programmable using Functionality Module (FM) capabilities to securely perform custom cryptography, or add custom blockchain algorithms.

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

Thales ProtectServer HSMs

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

Thales Luna Cloud HSM

In addition to our on-premises HSM solutions, Thales also offers a Luna Cloud HSM solution through Data Protection On Demand (DPoD). DPoD offers an as a service billing model with no hardware to deploy and maintain.

Securing Communications

Thales 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.

Industry-leading Blockchain Partners

Thales has partnered with industry-leading blockchain and cryptocurrency partners to provide enterprise-grade solutions for securing transactions. Together with partners such as IBM, R3, Ethereum, HyperLedger, Ledger, BitGo, Symbiont, ConsenSys Quorum, and more, Thales is protecting the way industries are conducting business, bringing efficiency and establishing trust.

Thales – A Secure Model for Your Blockchain Solution

Blockchain technology is purpose-built for specific applications, but does come with its tradeoffs and risks. Contact Thales 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 with custom FMs, and highly secure authentication solutions.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us