Bringing security to the world of blockchain

With technology from Infineon

www.infineon.com/blockchain

Management Summary

Blockchain marks a new way of documenting data on the Internet. Sometimes referred to as Internet 3.0, it powers cryptocurrencies like Bitcoin and Ether. Beyond fintech services, it can be used to develop applications in areas as diverse as logistics, energy supply, social networks, messaging, gaming, online marketplaces, storage platforms, identity and voting systems, prediction markets, online shops and much more.

The disruptive nature of blockchain is attributable to its core mechanism. Decentralized by design, and often hosted by millions of computers simultaneously, blockchain databases create a secured infrastructure by protecting data against manipulation and making it accessible to anyone. While this infrastructure provides inherent security for the technology, it also creates new pain points in relation to human or device interaction. To interact with a blockchain, the user's private key is both the identity and the security credential. If this key is stolen, the potential damage is are immense. Within a decentralized environment, there is no regulatory third party or intermediary with oversight, such as a bank or government agency. In a typical blockchain architecture, information is irrevocable, and key management is completely in the hands of the user.

Infineon's extensive security expertise provides the layer of security required to protect private blockchain keys. The integration of hardware-based security into blockchain applications, such as tokens, hardware modules and smartcards, makes private keys much more robust against attacks.

This paper outlines blockchain technology and explains how developers can design applications with built-in key protection, enabling end-users to have the best experience when working with the blockchain.

Contents

1. Blockchain: What is it and why is it so disruptive?

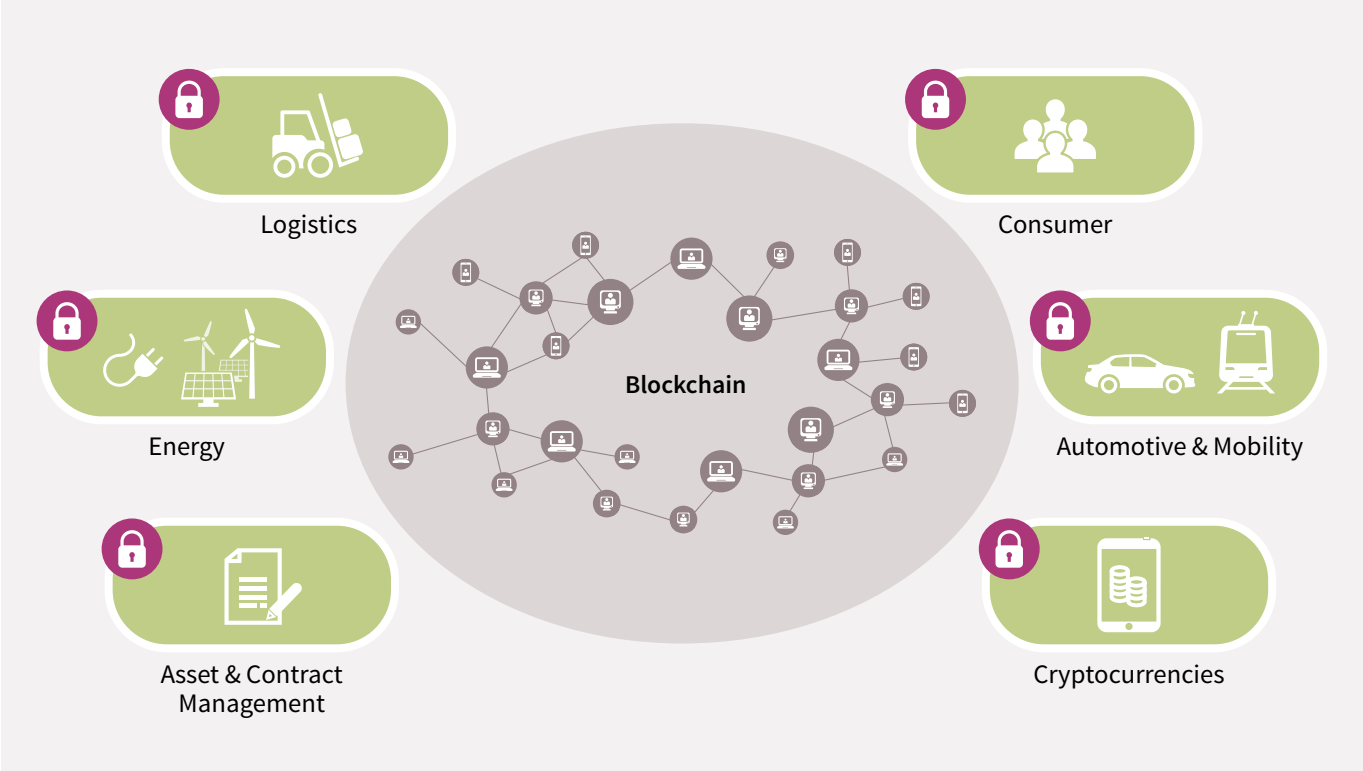
Blockchain technology creates a distributed database containing information that can be simultaneously used and shared within a large publicly accessible network. This network exists in a state of consensus and reconciles every transaction that happens in the network. At regular intervals, a set of transactions is grouped together and referred to as a "block". Once a valid block is generated, it is added and linked to the previous block of the continuously growing data chain – the blockchain.

By allowing digital information to be distributed but not altered, blockchain technology creates a digital ledger of transactions that can be programmed to record virtually everything of value, for example, financial transactions.

Looking beyond the hype, it is clear that blockchain is a disruptive technology that is here to stay, not least because of its broad deployment scenario.

Wide and growing number of use cases

Blockchain is predicted to have a significant impact on many industry segments. It is perhaps best established in the banking, financial and fintech sectors. However, it is suited to any industry that relies on accurate, secured, and protected data for trusted transactions between various market players. Hence it is also making rapid inroads into industries such as automotive, energy, logistics, healthcare and the public sector. New applications built around blockchain are also emerging for social networking, messaging, gaming and online trading – fueled largely by growing concerns among users about online privacy.
Another interesting target application is identity management, an area where conventional security implementations are still prevalent. For identity management, blockchain can be used as the foundation of an authentication system or of a smart contract solution.



Choosing the right blockchain

Bitcoin and other cryptocurrencies are based on a public blockchain, which implies network neutrality as well as open, permissionless read/write. As a result, it uses anonymous or pseudonymous identities and offers limited scalability in terms of speed and block creation. For private institutions such as banks, this may be a drawback.

Often referred to as distributed ledger technology (DLT), this permissioned blockchain network type is generated with pre-approved participants. Thus the validators could be, for example, members of a consortium who can regulate the access rights to the ledger. This blockchain type is typically much faster and all the identities are known to the consortium.

If the blockchain is in the control of just one single source or organization, it is referred to as a private blockchain. Although this system is completely centralized, it can leverage some of the advantages of blockchain technology such as tamper-resistant data and the ability to trace database errors.

	Public Blockchain	Private Blockchain	Permissioned Blockchain
Access	Anyone	Single organization	Multiple selected organizations
Participants	Permissionless Anonymous	Permissioned Known identities	Permissioned Known identities
Security	Consensus mechanism Proof of work/proof of stake	Pre-approved participants Voting/multi-party consensus	Pre-approved participants Voting/multi-party consensus
Transaction Speed	Slow	Lighter and faster	Lighter and faster

Source: blog.xsolus.com/different-types-of-blockchain-networks

2. Security matters

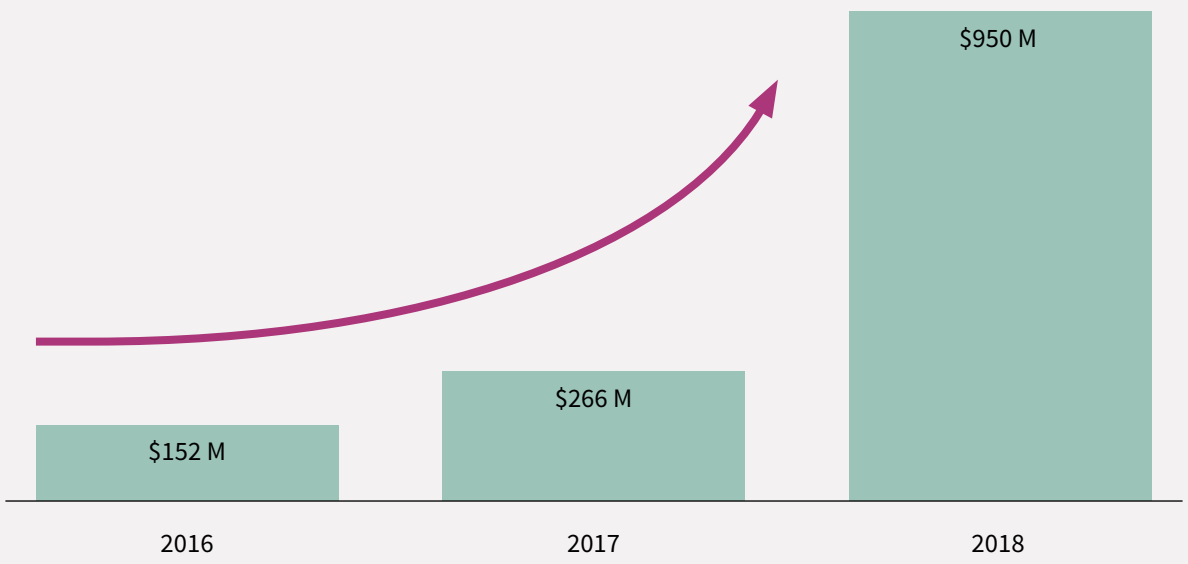
Without a regulatory third party or intermediary, the integrity of the blockchain user's digital identity is even more important than in traditional architectures.

The distributed nature of the technology may come with inherent security, but it poses real challenges when it comes to securely interacting with the system.

For example, generating transactions is an extremely sensitive process, because it uses the private key to add new valid data into the blockchain. As these data represent assets, e.g. cryptocurrencies or identities, the highest available protection is needed.

The graphic below shows the rapid rise in cryptocurrency theft from currency exchanges.

3.6 x more Crypto Stolen from Exchanges and Infrastructure in 2018 versus 2017



Source: CipherTrace Cryptocurrency Anti-Money Laundering Report Q4 2018

"Many exchanges have only been operational for two years or less. They have not invested in the security technologies and practices needed to safeguard IT systems, employees, and critical data. These cryptocurrency companies are at risk of having a simple file of cryptographic private keys stolen that can give the hackers $30 M to $500 M in profit. Yet these companies are immature in their security team funding, training and implementation."

Dave Jevans, Co-Chair of the Cryptocurrency Working Group / APWG

3. The role and functionalities of hardware-based security

Protecting private keys is the most reliable way to increase a blockchain system's security. A successful blockchain system needs highly reliable methods of strong key protection. Key security can be implemented at various levels depending on the level of protection required:

Level 1: Storing the blockchain user credentials on a personal device, such as a desktop, laptop or a mobile phone. While this practice may be convenient, it exposes the user to widely used software attacks.

Level 2: A slightly better security level is achieved by applying a TEE (Trusted Execution Environment) on the device microcontroller, which allows the separation of security software from other, less secure software stacks and therefore provides better protection of credentials against attacks.

Level 3: The highest possible security level protects the blockchain from micro-architectural[1] as well as physical attacks. This level of security can only be achieved when a dedicated security microcontroller is used for the operations and credential storage.

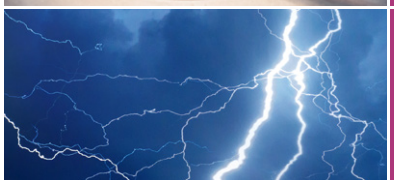
Physical attacks are increasingly common in blockchain environments. They can be divided into three different categories: observing, manipulation and semi-invasive attacks, as outlined in the following.

Observing side channels like power profiles, timing of the system and electromagnetic radiation can be used to expose the secrets stored inside a microcontroller.

Probing with needles on the silicon can be used to read out information from the chip.

Inducing faults into the chip during operation can generate errors in the output that help to calculate the secrets stored inside.

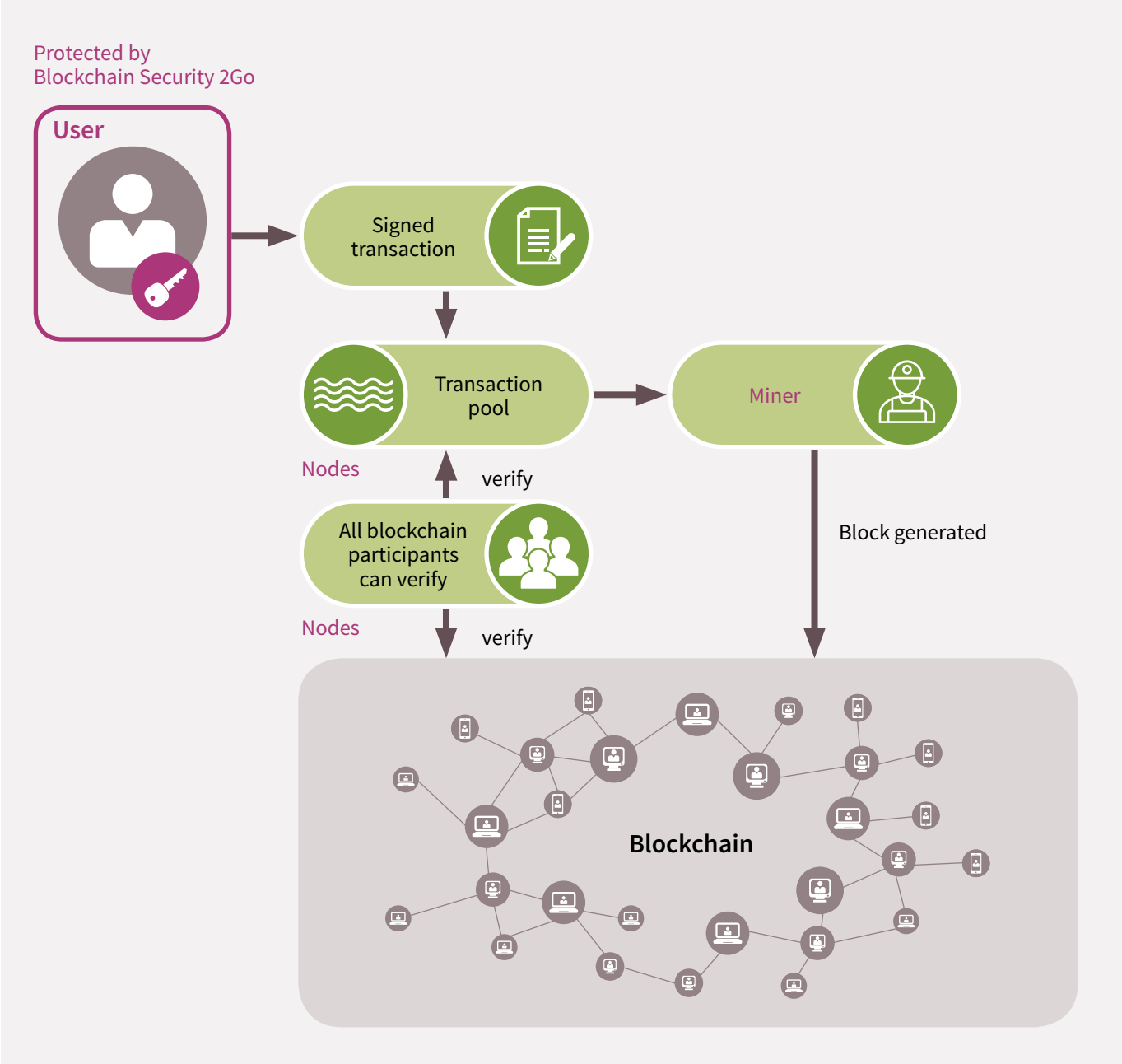
A security controller has dedicated countermeasures integrated to protect against these attacks and keep the credentials secret.

	Observing	› Power analysis › Electromagnetic analysis › Timing attack
	Manipulating	› Micro-probing (needles) › Circuit manipulation › Focused ion beam
	Semi-invasive	› Laser fault induction › Power supply glitch › Irradiation

[1] https://arxiv.org/abs/1706.05973

4. How to design security into a blockchain system

In blockchain systems, you can access and control an account once you gain access to the confidential private key. The security of a blockchain system thus hinges on the extent to which private keys can be protected.
For system integrators, a successful blockchain application starts with a good idea. However, the concept and implementation phase of this idea are often hampered by the lack of available tools to easily implement security right from the beginning. Integrators looking to implement a higher level of (hardware-based) security based on a security controller might find this task challenging and it may call for specialist expertise.



Closing the knowledge gap with Infineon's starter kit

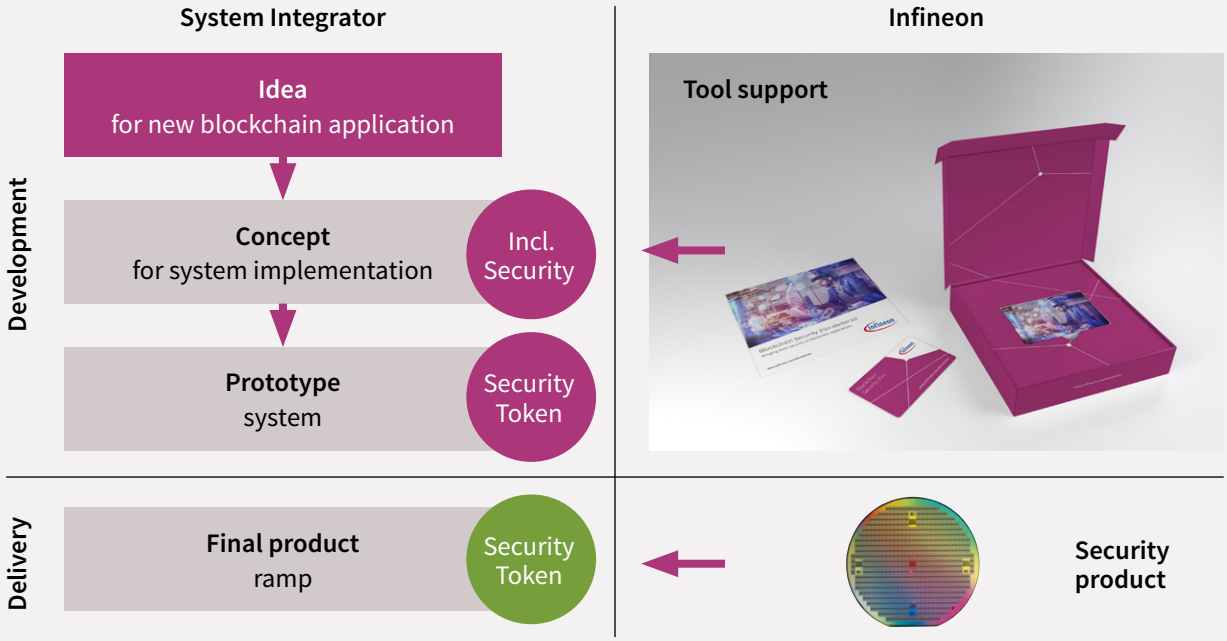
Infineon's Blockchain Security 2Go starter kit helps blockchain system integrators contemplating a new blockchain application to easily build in the most robust hardware-based security right at the concept phase.
Blockchain Security 2Go cards feature hardware-based protection mechanisms to generate and store private keys in a secured way.

Infineon's Blockchain Security 2Go starter kit is readily available from any Infineon distributor. In contrast to typical hardware-based security products, it can be bought without any legal formalities (such as a Non-Disclosure Agreement) and includes just a few security controllers. This lowers the hurdle for a system integrator looking to get hands-on hardware security at an early development stage.

Additionally, Infineon supports system integrators during the early prototype build phase.
There are open-source usage examples and libraries for smartphones (Android) and PCs (Python) publicly available that provide a good starting point for fast integration of hardware-based security. This is supported by the knowledge sharing of the rapidly growing open-source community involved in applying the starter kit for various different application domains.

The starter kit offers a simple but powerful interface for key management and signature creation. With this approach, integrators have a high chance of avoiding security issues in relation to key management, which often entail late and costly redesigns.

Support for secure blockchain system design



Where to buy

Infineon distribution partners and sales offices:
www.infineon.com/WhereToBuy

Service hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

- Germany ..... 0800 951 951 951 (German/English)
- China, mainland ..... 4001 200 951 (Mandarin/English)
- India ..... 000 800 4402 951 (English)
- USA ..... 1-866 951 9519 (English/German)
- Other countries ..... 00* 800 951 951 951 (English/German)
- Direct access ..... +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than "00" to access this international number.
Please visit www.infineon.com/service for your country!

Mobile product catalog

Mobile app for iOS and Android.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Order number: B181-I0841-V1-7600-EU-EC-P
Date: 06 / 2019