Blockchain & Security

Pierre Rouillac
V1.0

- restricted -

Agenda

1. What is Blockchain systems about?
2. Blockchain and security

Copyright © Infineon Technologies AG 2019. All rights reserved.

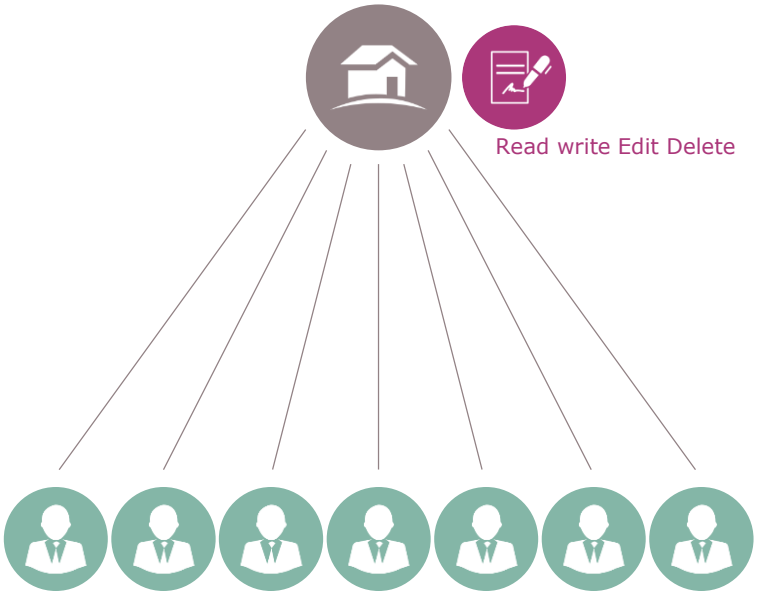
Agenda

1. What is Blockchain systems about?
2. Blockchain and security

Copyright © Infineon Technologies AG 2019. All rights reserved.

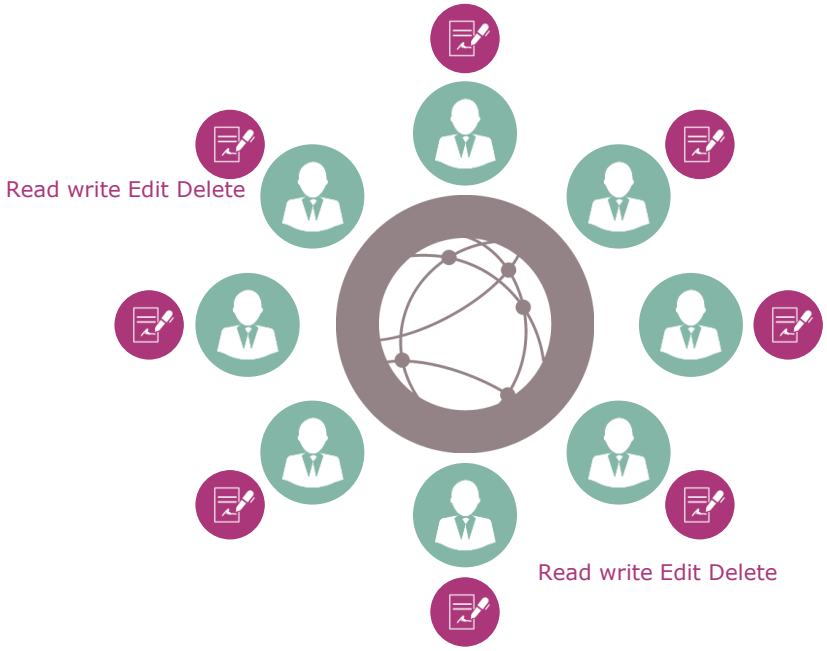
There are 2 kind of systems: Centralized and decentralized

A unique entity manages information



Centralized System

Information are shared by anyone



Decentralized System

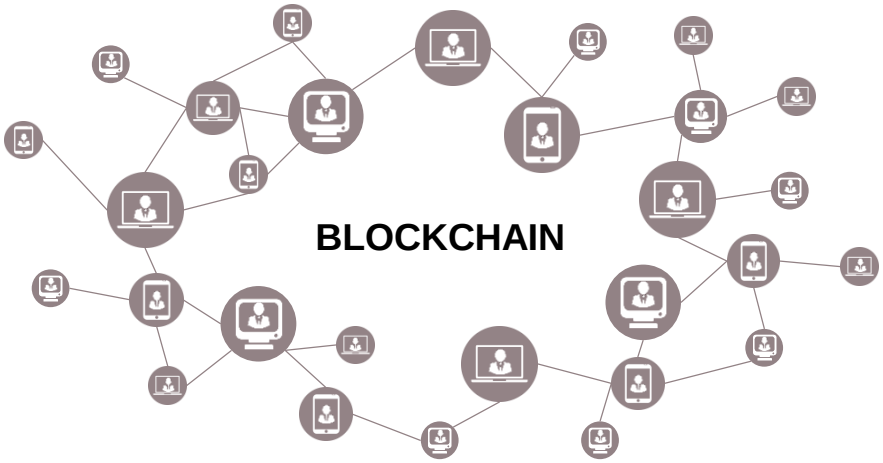
Protection of user credentials is essential

Copyright © Infineon Technologies AG 2019. All rights reserved.

Blockchain is a decentralized system

It maintains a continuously growing list of data

The records are hardened against tampering and revision



Cryptographic proof instead of central trust

Typically no central authority

Nodes don't have to trust each other

Copyright © Infineon Technologies AG 2019. All rights reserved.

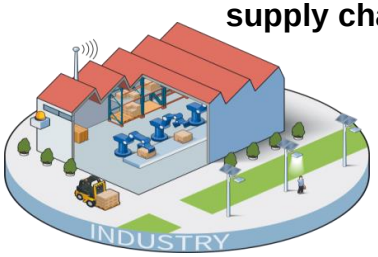
one of the most popular use case is Bitcoin…



Copyright © Infineon Technologies AG 2019. All rights reserved.

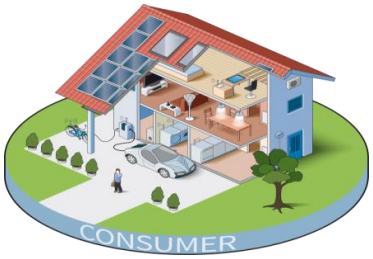
… but Blockchain can be used in many different areas!

Asset management / supply chain



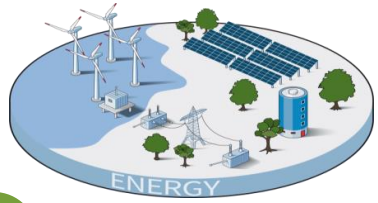
Logistics

Insurance and Healthcare

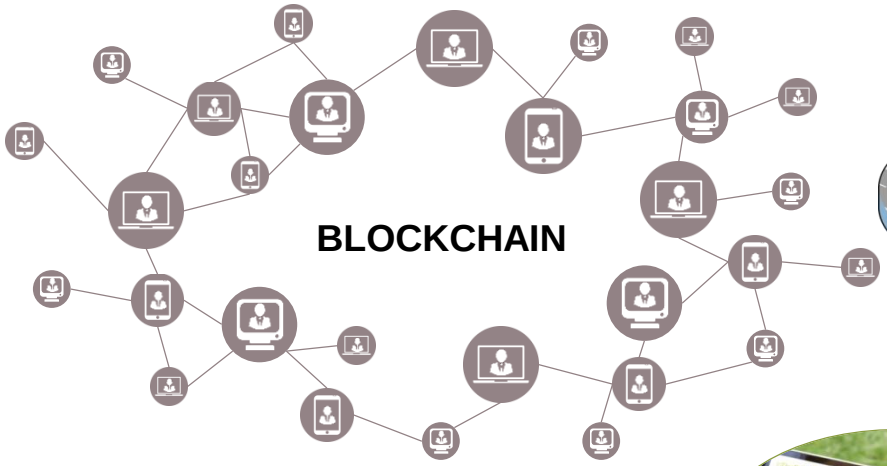


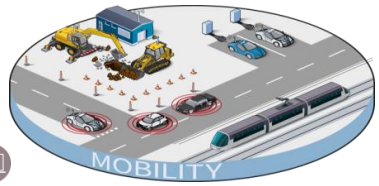
Consumer

Streaming application



Energy





Automotive & Mobility

Asset & Contract Management



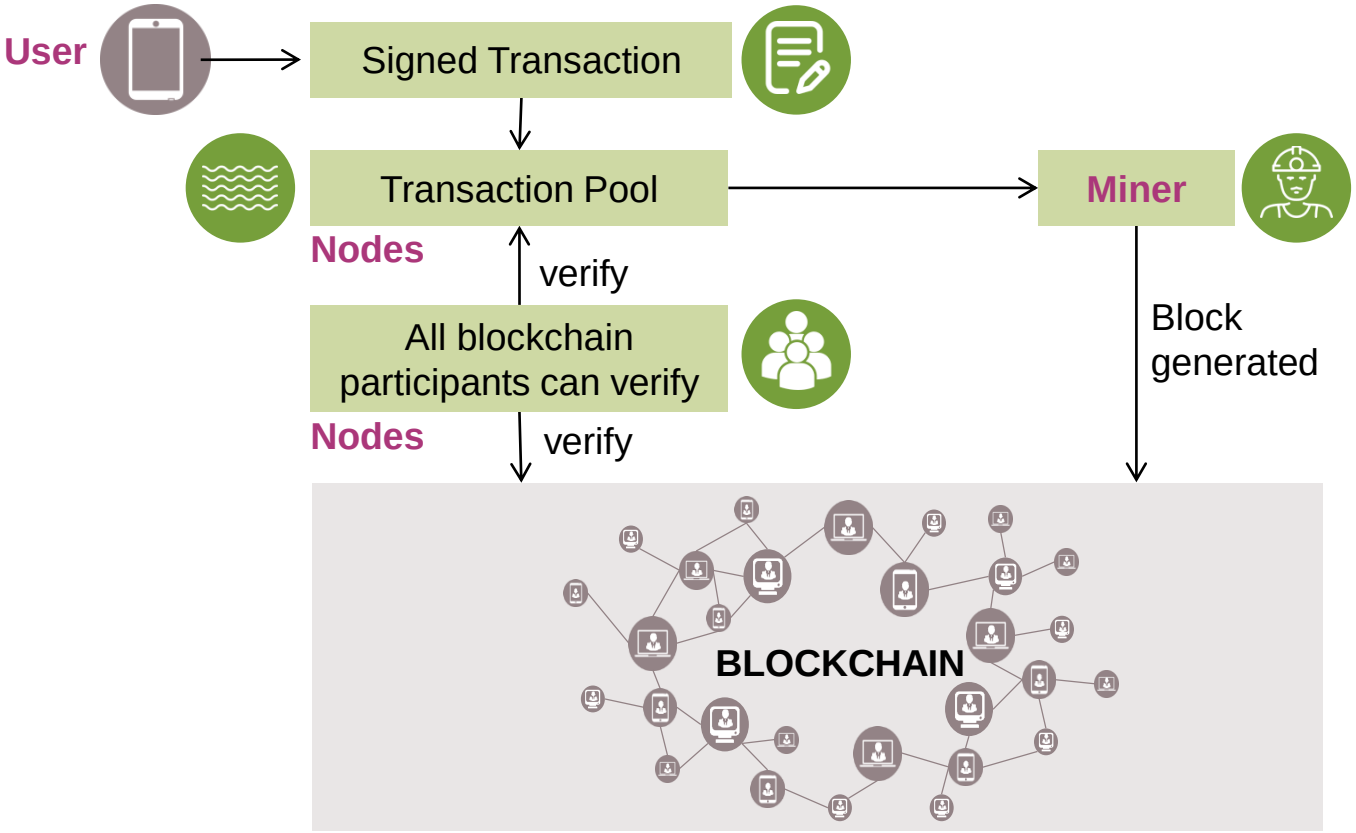
Electronic voting systems



Crypto Currencies

Copyright © Infineon Technologies AG 2019. All rights reserved.

Blockchain basics and environment



Copyright © Infineon Technologies AG 2019. All rights reserved.

Agenda

1. What is Blockchain systems about?
2. Blockchain and security

Copyright © Infineon Technologies AG 2019. All rights reserved.

Blockchain authentification is using

Public keys

used to

derive addresses and verify signatures



Private keys

used to

generate signature / sign transactions

Copyright © Infineon Technologies AG 2019. All rights reserved.

Security Risk



Public keys

&

Private keys

Can be attacked

Private key can be stolen

→ **attacker has full access to all assets**

One can lose his private key

→ **all assets are lost**

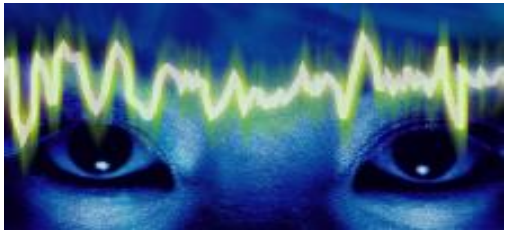
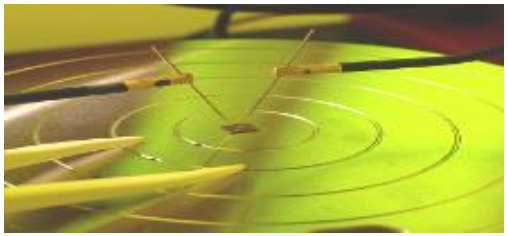
Blockchain transactions **cannot be undone**

Private key storage requires best possible protection

→ **Hardware based Security is important**

Copyright © Infineon Technologies AG 2019. All rights reserved.

Physical attack types and examples

	Different types of attacks	Examples
	Observing	› Power analysis › Electromagnetic analysis › Timing attack
	Manipulating	› Micro probing (Needles, FIB) › Circuit Manipulation
	Semi-invasive	› Overclock › Glitch in the power supply › Induction of local heating, UV light, or similar…

Copyright © Infineon Technologies AG 2019. All rights reserved.

Why hardware-based Security

Hardware security controler is the most secure solution to store credentials against attacks

	Software	Trusted Execution Environment	Security controller
Software attacks	⚠	🔒	🔒
Micro-architectural attacks	⚠	⚠	🔒
Physical attacks	⚠	⚠	🔒

Security Controller



Integrity Guard

Prepared to reach the highest security level

Copyright © Infineon Technologies AG 2019. All rights reserved.

If a customer is looking for :

A **decentralized** system

A highly **secured** solution based on **hardware**

A system involving a **big number** of participants without a **pyramidal** organization

An **enormous** potential for many use cases

Blockchain

An **quick** to understand solution

A **simple** solution with basic features

An **open-source** application examples

An access to the blockchain **community**

An “**all included** pack”

An **easy** to buy solution (no NDA, affordable, small volumes)

Blockchain Security 2Go Starter kit

On sale at :

www.infineon.com/blockchain

Copyright © Infineon Technologies AG 2019. All rights reserved.



Part of your life. Part of tomorrow.

Infineon