CHALLENGES AND RISKS OF BLOCKCHAIN TECHNOLOGY

Christian Sprecher
Ulrich Gallersdörfer

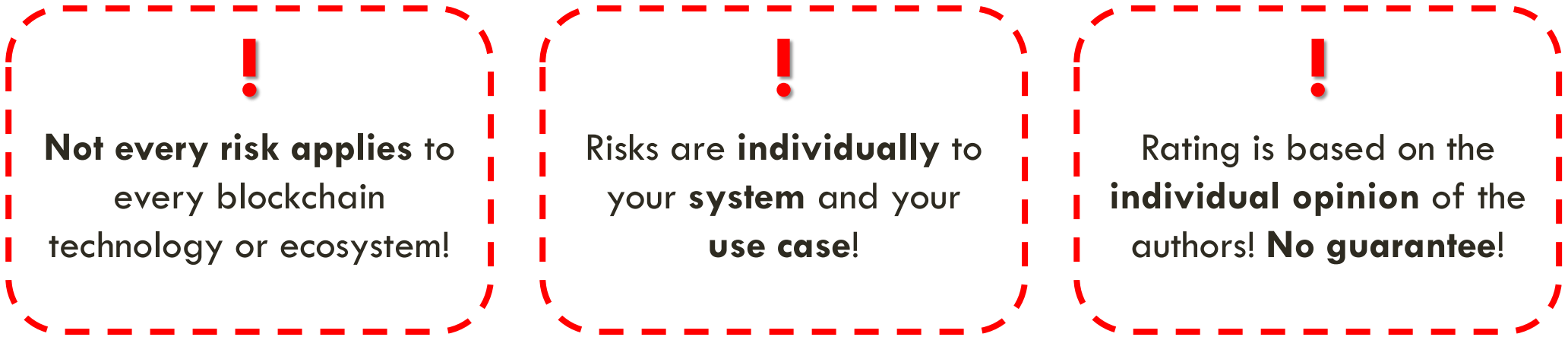
24.02.2017 @ IRIS 2017

PEOPLE

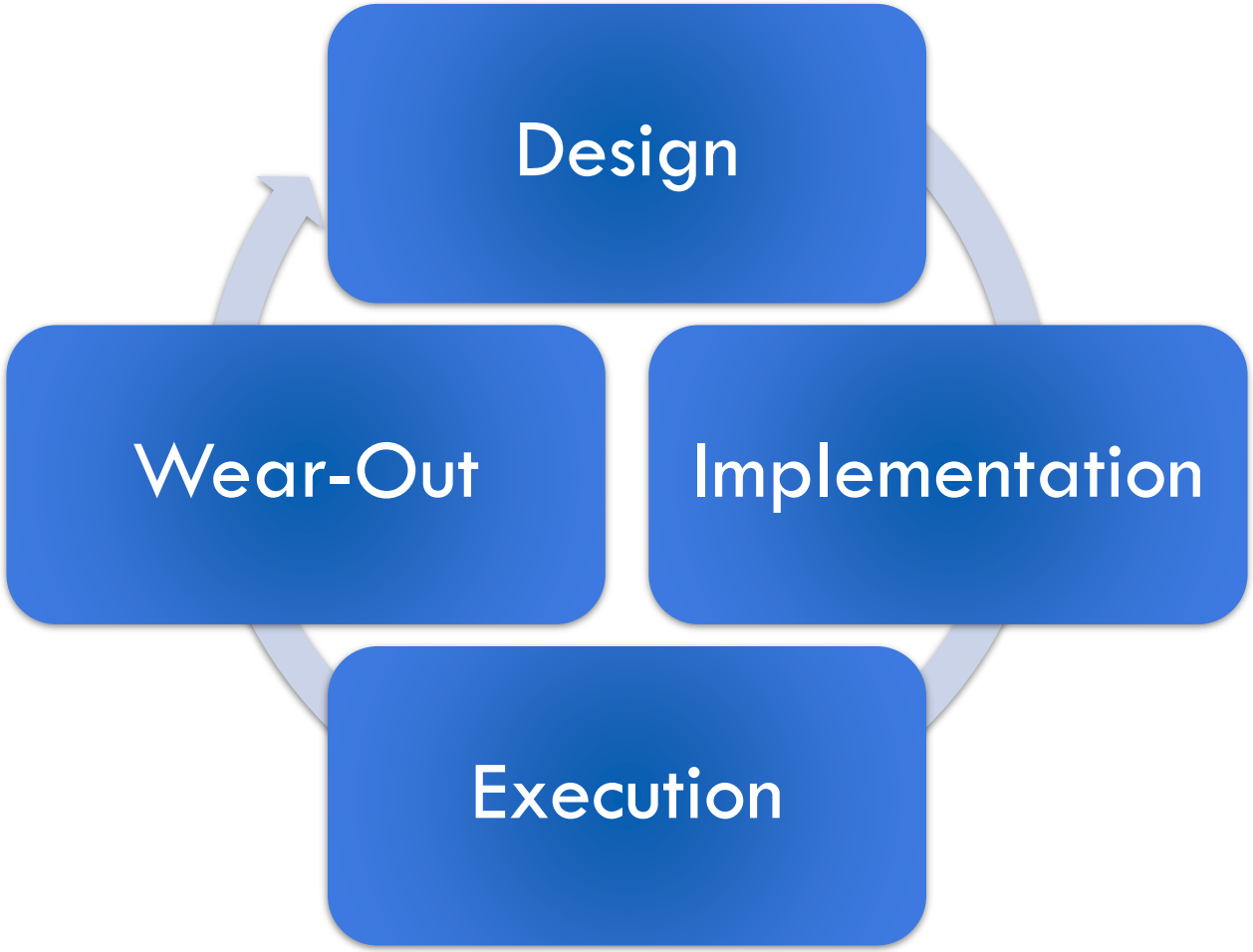
Christian Sprecher	Ulrich Gallersdörfer
CTO weblaw.ch	Master Student at TUM

OVERVIEW

We are going to discuss different **risks** and **challenges** of blockchain technology in **general.**

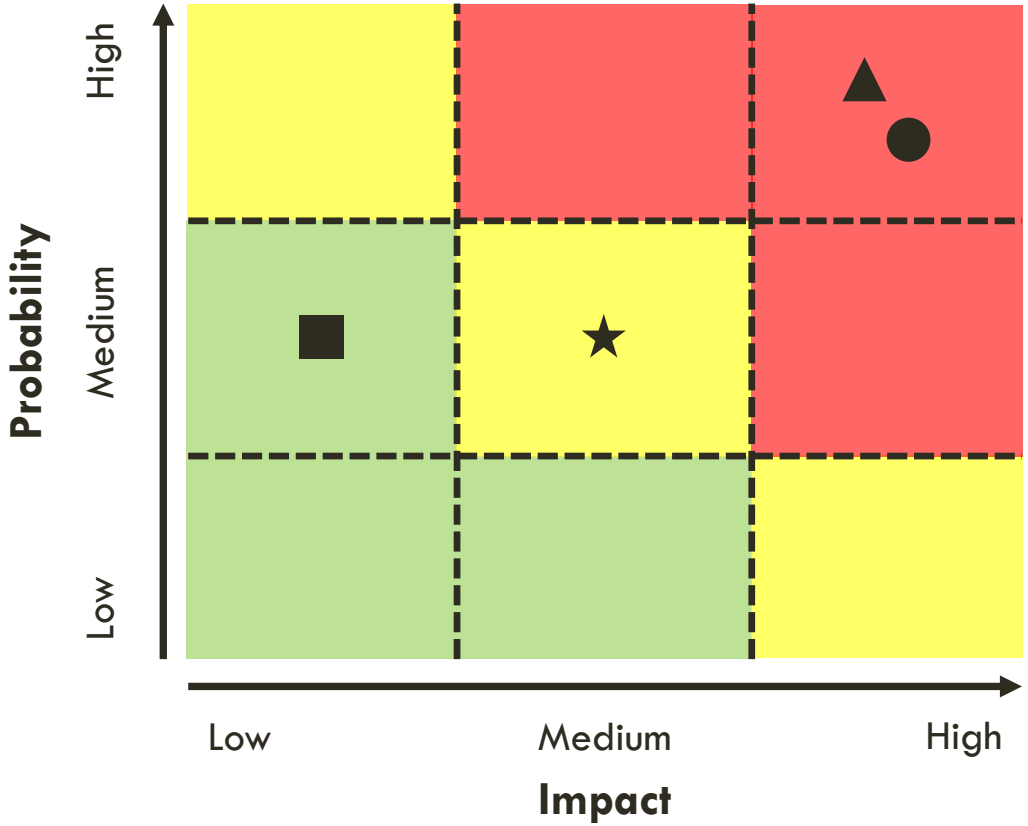


LIFECYCLE OF A BLOCKCHAIN (SIMPLIFIED)



1. AT DESIGN

- ■ Favoring Early Adopters
- ● **Scaling**
- ▲ **Private Key Security / Finality**
- ★ Pseudonymity



1. AT DESIGN (ONLINE EXPLANATION)

Favoring Early Adopters

It is the nature of a blockchain system, that early adopters have more advantages than late adopters. This can manifest in lower prices for coins or a lower effort to participate in the network. Blockchains have to be designed in such way that late adopters have enough incetives to participate.

Scaling

The speed of the network to process transactions is independent from the used computation power. That said, a laptop can process an equal number of transactions as the whole Bitcoin network, assuming that it uses the same blockchain design. Speed improvements can only be made with design changes.

Private Key Security / Finality

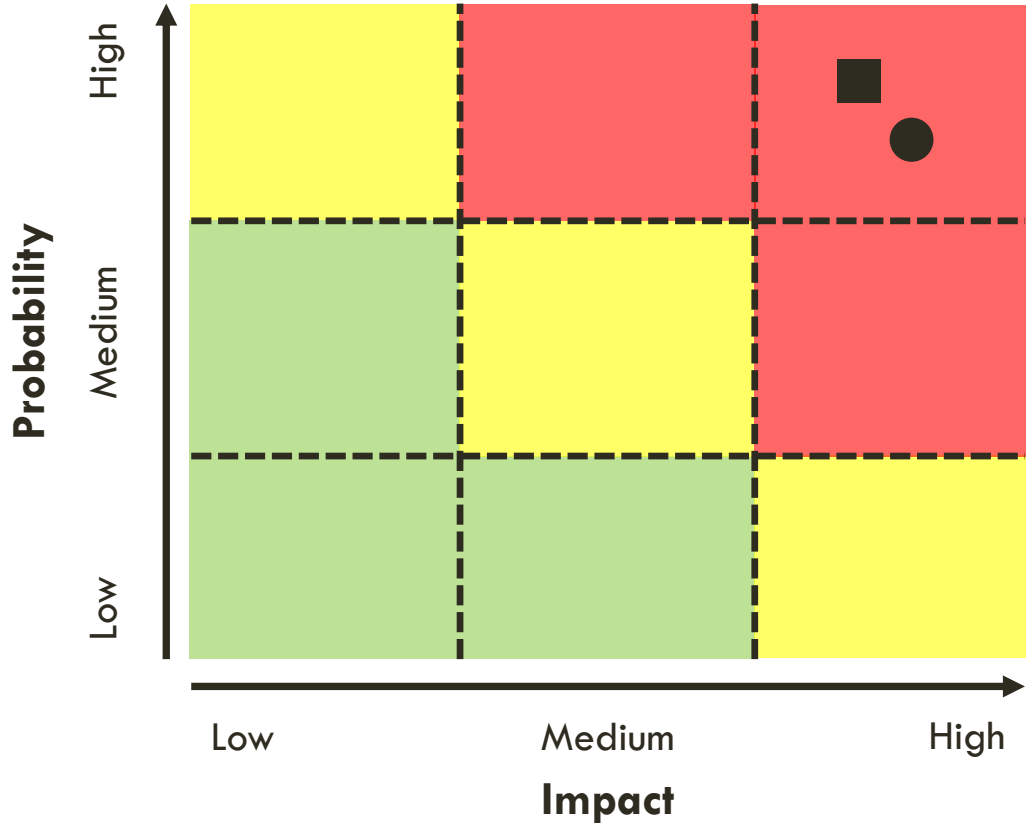
The Security of stored assets are only guaranteed by keeping the key secret. If someone gets hold of the key or it is lost, the corresponding asset is not accessible anymore. The blockchain is not designed to revert transactions that happened because of fraud.

Pseudonymity

The system itself is not anonymous as often proposed. Every user has to operate under public keys, how many is up to him. With bundled transactions it is possible that public keys can be linked together, such that it is sure that the same person acts under these different identities. If the real identity is uncovered of one key, all the activity can be traced back.

2. AT IMPLEMENTATION

- **Bugs in Implementation**
- **Durability of Crypto Algortihms**



2. AT IMPLEMENTATION (ONLINE EXPLANATION)

Bugs in Implementation

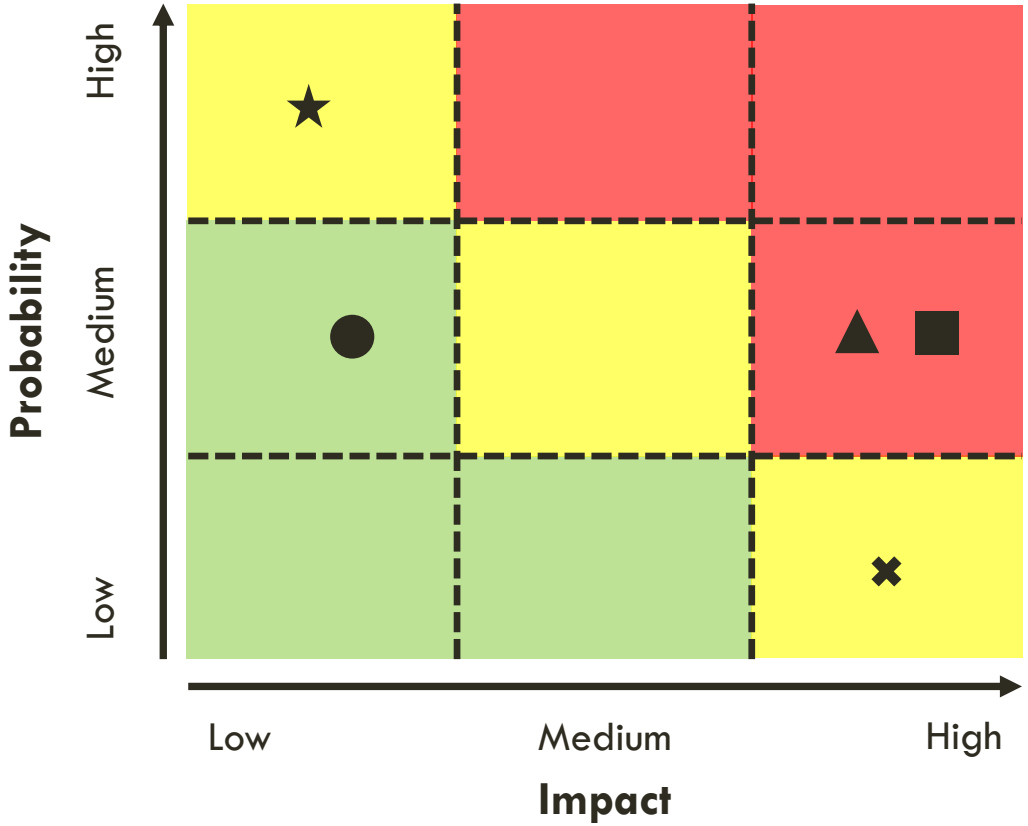
Blockchain is based on developed software as any other network. This results in equivalent problems: bugs. There are two problems about that: First, a bug in the blockchain is very hard to fix, because changes in the underlying software usually create a fork. That means, the network splits up in two „chains“, one with the old software and one with the new software, because they do not accept the blocks from each other. The second problem is, that bugs in a blockchain usually lead to security holes in the system.

Durability of Crypto-Algorithms

Another problem could rise up in the future: The durability of crypto-algorithms. A Blockchain usually depends on two main crypto-algorithms: one for public/private-key-cryptography, that ensures that only people who own the assets (know the private key) can move them. Another for linking the blocks together, so called hash-functions. The latter appears to be more vulnerable in general, but the impact is usually smaller. Blockchains are upgraded to always use the most recent hash-functions to ensure the integrity. A much bigger problem is the use of the public/private-crypto algorithms, because if they get vulnerable (e.g. by quantum computing), the migration process is much more complex. We do not know of a real world case where this happened, but it has to be assumed that most of the assets will be lost.

3. AT RUNTIME

- ■ „51-% Attack“
- ● „Selfish Mining“-Attack
- ▲ **Centralization of Mining-Power**
- ★ Waste of Energy
- ✖ „Death Spiral“



3. AT RUNTIME (ONLINE EXPLANATION)

"51%-Attack"

Blockchains are assumed to be a very resistant system. But it is possible that the system could be attacked if one node in the system has a mining capacity of more than 50 percent. With that, he is able to control the history and blackmail other participants. He is not able to create money out of thin air.

"Selfish-Mining"-Attack

An attacker can gain an monetary advantage over the network. He needs at least 25% of the network capacity, but the attack does only do low damage and is easily detectable.

"Death Spiral"

A "Death-Spiral" leads to the death of a blockchain. This is usually the case when more and more miners leave the network because of negative profit. The cause of this could be a hack or some other negative news.

Centralization of Mining Power

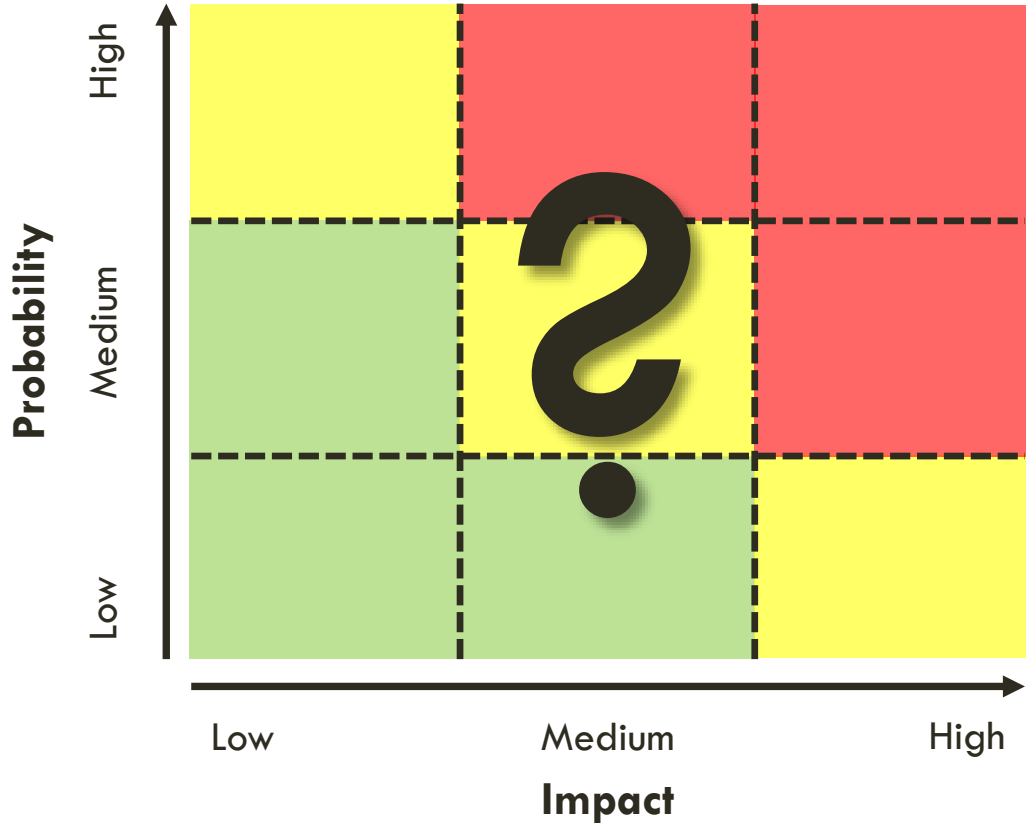
The network, when it grows, gets more and more centralized out of two reasons. The first reason is increased storage need, because the blockchain grows. The Bitcoin blockchain is around 110 gbyte big and grows about 3 gbyte per month. The second reason is that it only pays off to mine if the server capacities are big enough. For normal people the energy consumption is more expensive than the reward.

Waste of Energy

The concept of creating new blocks (called Proof of Work or PoW) consumes a lot of computation power and with that a lot of electricity. The computation power is used for this process and the results do not have any other good than for the sake of the blockchain.

4. AT WEAR-OUT

- What happens to old or broken Blockchains?
- What happens to your assets?



4. AT WEAR-OUT (ONLINE EXPLANATION)

What happens to old blockchains?

It is not known what happens to old blockchains. Unless the last node stops working, the network remains still functional. That means a blockchain could live long after being declared irrelevant, but is not used anymore. The assets on it won't be worth anything, unless they are tied to real world objects.

One way for old blockchains could be that they are getting upgraded to add new functionality or fix remaining bugs. This is unlikely, because certainly users will migrate to newer systems, but it is not impossible.

The aspect we want to convey is that this system does not last forever. Have a backup plan for the case that the platform you chose fails.

LESSONS LEARNED

Understand the **technology**(!) and its **implications**!

The trust is established by the code. **Do you trust the coders?**

Think about how you want to **keep your private keys private**!

Have an **exit plan** for the case that your chosen **platform fails**!

THANK YOU FOR YOUR ATTENTION!

Christian Sprecher
Ulrich Gallersdörfer