Deloitte.

Blockchain security

Protecting the distributed ledger

Blockchain security

Protecting the distributed ledger

A Blockchain, or distributed ledger, is a technological protocol that enables data to be exchanged directly between different contracting parties within a network without the need for intermediaries. Each transaction is communicated to all network nodes, and once verified and confirmed, is added to an immutable transaction chain.

Numerous industries are currently researching and piloting Blockchain applications, see our recent white paper "The Blockchain (R)evolution –The Swiss Perspective" (1) for a general overview of Blockchain applications in the Swiss market. What most of these new applications have in common is that they need to process and store sensitive data. In the healthcare industry, for instance, these are patient medical records, medical metadata, clinical trial information and PII (Personally Identifiable Information). As a consequence, there is a rising number of inquiries and concerns from our clients about the security aspects of Blockchain and its ability and limitations in protecting such critical data. Based on our experience, three aspects contribute to making Blockchain security difficult to manage:

1. Immaturity and complexity of the technology

Due to the different consensus algorithms available (e.g. proof of work or proof of stake), the Blockchain types (e.g. permissioned or permissionless), and the complex underlying cryptographic protocols, it is difficult for security practitioners to fully understand data flows and potential security weaknesses. In addition, multiple Blockchain platforms and implementations exist and applications must be evaluated for their suitability for integration with a specific Blockchain system.

2. Lack of standards and regulations around Blockchain technology

As of today, Blockchain technology is unregulated, resulting in legal uncertainties and grey areas. An interesting example of the lack of controls and laws regulating Blockchain networks is the DAO hack (2) where a smart contract (3) vulnerability led to the network losing 60 million US dollars (4).

3. Widespread belief that a Blockchain is secure by design

Blockchain technology is built upon public-key cryptography and primitives such as digital signatures and hash functions, which may give a false impression of security. The fact that all cryptographic protocols have their limits and that holistic security includes not only technology, but also people and processes, is often overlooked in a Blockchain security analysis.

To overcome these difficulties, we advise clients to take a risk-based approach to Blockchain security, which ensures that security controls are selected in line with business needs and business use cases. This approach can be summarised as follows:

- **Understand criticality of data and processes**
  The first step is to understand the sensitivity of the data that is being stored and processed in a Blockchain. By understanding regulatory implications and performing a business impact analysis, the importance of confidentiality, integrity and availability of data can be determined.

- **Create a threat model**
  Secondly, traditional threats related to public key infrastructure and application development, such as key compromise and code bugs, must be factored into the analysis. On top of these, Blockchain-specific attack vectors relevant to the given application need to be identified. These include consensus hijack, Distributed Denial of Service (DDoS), permissioned Blockchain exploitation, smart contract exploitation and wallet hacking (5). Based on these, risk scenarios can be listed and evaluated for likelihood and impact.

- **Select security controls**
  The final step is the selection of security controls that address the identified risks. A number of traditional good security practices can be deployed. These include robust key management, code review, data encryption, access control, and security monitoring. In addition, there are techniques specific to Blockchain technology that can be set up, such as secure wallet management, permissioned chain management, and secure smart contract development. Finally, it is important to keep in mind that people, processes and technology are equally important to ensure that Blockchain applications are properly protected. For instance, the impact of the aforementioned DAO hack could have been contained if proper governance structure and incident response process had been put in place.

If you would like to have an initial conversation about Blockchain security and Deloitte's approach, please get in contact with our team.

Authors:

Patricia Egger
Senior Consultant
paegger@deloitte.ch
+41 58 279 7641

Dusko Karaklajic
Senior Manager
dkaraklajic@deloitte.ch
+41 58 279 7386

Contacts:

Klaus Julisch
Partner
kjulisch@deloitte.ch
+41 58 279 6213

Florian Widmer
Partner
fwidmer@deloitte.ch
+41 58 279 6910

Deloitte.