Contribution ID: **24** Type: **Roundtable Member**

IT security and consensus mechanisms in private blockchains

Wednesday, 7 November 2018 09:05 (5 minutes)

In 2017, a study by the Pacific Northwest National Laboratory explored the potential of blockchain (distributed ledger) technology for safeguards applications. Starting from an analysis of the IAEA's requirements for new technologies, this study concluded so-called consortium systems (we shall use the more common term *private blockchains*) might improve on solutions currently used. This paper aims to highlight which issues need to be considered when evaluating the benefits and risks inherent in private blockchains. Special attention will be given to IT security matters.
Since blockchain solutions store information in a distributed fashion, a process for ensuring consistency and validity of the data copies, called *consensus mechanism*, lies at their core. Whereas bitcoin's proof-of-work is often berated due to its energy consumption and limited throughput, the use of private blockchains allows for much more efficient procedures. It is crucial, however, to understand that these rely on certain assumptions about the underlying network and the participants involved in the blockchain. The most important of these assumptions concerns the fault-tolerance the procedures can ensure. While it is not hard to design a consensus mechanism that works well in propitious circumstances, making it resilient to faulty behaviour, which may stem from technical failures but also be deliberately induced by an attacker, is a much more challenging task.
Fortunately, a number of research works has adressed just this question. This paper will provide a high-level overview of the available techniques and the security guarantees they offer. It will stress which matters need to be accurately modelled before choosing a blockchain solution. In a somewhat broader sense, it will also clarify certain popular misconceptions about blockchain technology in general.

Which "Key Question" does your Abstract address?

TEC4.1

Which alternative "Key Question" does your Abstract address? (if any)

TEC4.2

Topics

TEC4

Primary authors: Dr BERGHOFF, Christian (Bundesamt für Sicherheit in der Informationstechnik); Dr GEBHARDT, Ute (Bundesamt für Sicherheit in der Informationstechnik)

Presenter: Dr BERGHOFF, Christian (Bundesamt für Sicherheit in der Informationstechnik)

Session Classification: [TEC] Blockchain and Safeguards

Track Classification: Leveraging technological advancements for safeguards applications (TEC)