BLOCKCHAIN *Blues* - the *END* of eID cards?

By Markus Hoffmeister and Klaus Schmeh, cryptovision

By design, the blockchain is a decentralized technology. It creates a distributed database containing information that can be simultaneously used and shared within a large publicly accessible network. The blockchain network lives in a state of consensus and reconciles every transaction that happens in regular intervals. Each group of these transactions is referred to as a “block”, hence the technology’s name. By allowing digital information to be distributed but not modified, blockchain technology creates a digital ledger of economic transactions that can be programmed to record not just financial transactions, but virtually everything of value.

> *“A blockchain solution can link a public key with an identity in a similar manner to a public key infrastructure (PKI) – although without needing a central entity, through the avoidance of a central entity, you naturally have fewer possibilities for influence – with all the pros and cons associated with this.*
>
> *-Benjamin Drisch, cryptovision*

☐ What are the security implications?

With blockchain databases not being stored in any single location, the information is much harder for a hacker to manipulate. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet. In other words, the blockchain’s aim is to take trust away from human intermediaries and put it into mathematics and computing, which are a lot less susceptible to errors. It is a mechanism to bring everyone to the highest degree of accountability.

Yet the same thing that makes blockchain attractive - its distributed nature - also makes it a potential security threat. Vulnerabilities occur when the blockchain interfaces with humans or, in the case of IoT, with devices. When using blockchain, the user's private key is the identity and the security credential, which is generated and maintained by the user instead of third-party agencies. For example, when creating a storage wallet, the user must import his/her private key. An attacker could steal the user's private key using various attacks. Since the blockchain is not dependent on any centralized third-party trusted institutions, it is difficult to track the attacker's behaviour and recover the modified blockchain information.

This situation poses an important question for the smart card industry: what role will smart cards or other secure elements play in blockchains? Currently, all a user can do is use a self-issued smart card or other hardware device to store his private key, as a sort of cold crypto-wallet. This results in better protection than software wallets or hosted cryptocurrency exchanges, but is still far from perfect. It is therefore an interesting option to use a private key stored on a trusted identity card (i.e. a national eID card) for participating in a blockchain.

Blockchain for Identity and Data Management

The global blockchain identity management market is expected to reach USD 7308.4 million by 2025, from USD 57.6 million in 2017, growing at a CAGR of 83.2% during the forecast period of 2018 to 2025.

Data Bridge Market Research 2018

What are the implications of this development for the conventional digital identity markets and its stakeholders? Blockchain technology is currently promoted as the silver bullet for distributed applications of all kinds. Beyond the most cited application of BitCoin in the fintech sector, identity management is a growing segment. Here, the blockchain can be used to build the groundwork of an authentication system or of a smart contract solution. Having a secure identity to authenticate oneself is crucial for all online interactions. Absolutely no one would argue while the use of username / password is prevalent that there is a need for innovation to enable secure, convenient online identity management. Distributed ledgers could fill this need by offering enhanced methods for proving who you are, along with the possibility to digitize identity documents.

However, conventional identity systems are not being replaced just yet: Developing digital identity standards on the blockchain is proving to be a highly complex process. Besides technical challenges, a universal online identity solution requires cooperation between private entities and government agencies. Add to that the need to navigate legal systems in different countries and the problem becomes exponentially difficult.

Is blockchain replacing conventional PKI and eID systems?

"A blockchain solution can link a public key with an identity in a similar manner to a public key infrastructure (PKI) – although without needing a central entity, through the avoidance of a central entity, you naturally have fewer possibilities for influence – with all the pros and cons associated with this."

Benjamin Drisch, cryptovision

The implementation of a public key infrastructure (PKI) and a blockchain is an interesting debate within the industry. While the outcome is yet to be determined, it is apparent that blockchain technology can benefit from PKI and other identity technologies, rather than replacing them. Blockchain leverages digital signatures and hash functions, as the main cryptography for all transactions. This is exactly what a PKI provides. If the PKI is a part of an eID system, the private key is even protected to the highest level. It goes without saying that a digital currency, like BitCoin, profits from this.

The benefit of a key being stored on an eID card is less clear when it comes to blockchain-based authentication. As an eID card is an authentication solution in itself, it can be questioned whether a blockchain-based authentication system is even necessary when such a card is available. In addition, the involvement of a card issuing authority contradicts the main benefit of a blockchain: to establish a trusted infrastructure without involving a trusted third party. At this point it is important to note that not requiring a trusted third party is not the only advantage of a blockchain. Other purported benefits include fault tolerance, high availability and lower operation costs.

Conclusion

It will certainly be a major research goal for years to come to evaluate whether the benefits of an eID in a blockchain environment are real and if they outweigh the natural drawbacks of a blockchain. If these questions will be answered in a positive way, an eID card appears to be the perfect means for storing a private key used in a blockchain – as long as the existence of a trusted third party is accepted. Not only keys, but also identities can be shared between a blockchain and an eID infrastructure. All this means that eID cards might become important building blocks of blockchain systems and that a convergence of the two technologies can be expected. In the end, the major question is whether the blockchain will ever become as important as the current hype suggests. This remains to be seen. ☒

cryptovision

cryptovision's signature solutions work well for signing transactions within the blockchain. cryptovision has implemented a smart card solution that allows the user to conveniently sign payment instructions within the blockchain currency Ether. Since a smart card is used as a key store, the key is much better protected than in a conventional blockchain wallet. The cryptovision solution makes it possible to store the signature key outside the card for backup purposes.

cryptovision's Certificate Lifecycle Management solutions work well with various blockchain-based PKI components. For example, cryptovision's CA software CAmelot supports blockchain-based directory services, CRL distribution points, OCSP responders, CA certificate distribution points, and identity management systems, as long as they can be addressed through standard PKI interfaces.