DIGITAL CURRENCIES
Governance Group

ZERO-KNOWLEDGE PROOF

DCGG Briefing Paper

December 2021

The exponential growth of Internet usage and increased access to digital products and services have proportionately increased the need for users to share personal information online. Whereas big data and new technologies have improved access to services on digital platforms, they have also brought about certain risks. In order to gain full access to products and services, users may often relinquish their privacy, which can be associated with risks of exposure to security breaches and misuse of sensitive data. The concerns of individual rights and data ownership have guided research into new methods, tools, and mechanisms aimed at realising the full potential of the digital economy without the risks to data privacy.

What is Zero-Knowledge Proof?

Zero-Knowledge Proof (ZKP) allows users to take full advantage of the data-based economy whilst securing their privacy. A ZKP is a digital protocol, through which one party can 'prove' to another party that sensitive information exists, without actually sending that information over. In other words, ZKP allows digital authentication without disclosing sensitive personal data. Thus, ZKP prevents the possibility of any information, either from the sender's or receiver's end, from being compromised.

How DOES IT Work?

The ZKP technology, illustrated by the example below, indicates how information can be verified without revealing the contents of this information, thus transforming the way data is collected, used and transacted with. A transaction that employs ZKP demonstrates how the 'tester' can prove something true to the 'verifier' without revealing any other specifics about the transaction. In other words, through a series of probabilistic assessments, ZKP protocols can supply pieces of unlikable information, which are utilised to validate an assertion. Generally, a ZKP is designed to cover the following criteria:

1. Completeness: it should demonstrate to the "verifier" that the "tester's" knows what they claim they know;
2. Soundness: if the data is false, it cannot persuade the "verifier" that the "tester's" data is correct;
3. Zero-knowledge-ness: it should not disclose anything else to the verifier.

ADVANTAGES

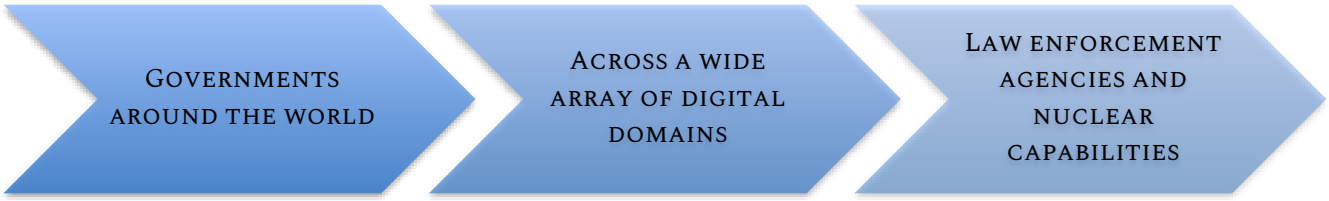
- The need for passwords is eliminated and also the use of other type of sensitive data
- Helps eliminate the risks that are involved in the password-only authentication
- Users can share some of the transaction details if they would like
- Bolsters the security of a person's online payments

DISADVANTAGES

- In case the originator of the transaction forgets his password, all the information related to the transfer will be lost forever
- These types of transactions take longer to compute due to its complex nature
- Information needs to be numerical, otherwise some translation is needed. This makes it difficult for data storage and sending secure messages

Application

ZKP can be utilised across a wide array of digital domains. The ZKP technology allows for developing digital identification mechanisms that do not obligate users to reveal personal sensitive information. Another prominent use case is when ZKP is used by government agencies around the world to verify the origin of information without disclosing how or from where they obtained this information. In terms of law enforcement, ZKP allows agencies to determine if an individual has a valid driver's license without requiring any other information from that individual besides their ID number. Another use case, which can gain prominence is when it is used by governments to estimate the nuclear capabilities of certain militaries without the need to inspect their inventories.



DCGG's Position

- GDPR

In May 2018, the European Union's General Data Protection Regulation (GDPR) came into force. It introduced stringent requirements in order to highlight the right of people and businesses to have their personal information erased ("right to be forgotten") or the right to rectification (right to have personal information completed or corrected,). This has put a burden on companies that need to collect and store

PII (Personally Identifiable Information), PHI (Protected Health Information) or any other sensitive data, in order to comply with GDPR. This has put the question whether blockchain-based systems comply with GDPR and its requirements.

In principle, there is no rift between the goals of GDPR and the principles behind blockchain technology. Most GDPR requirements can be applied to blockchain applications. As an example, GDPR requires the entity that operates the applications to be a data controller. This requirement is met by many blockchain-based applications since they are operated by an identified entity that posts data on a blockchain ledger on behalf of their users. Many believe that ZKP can be a significantly useful technique that can keep blockchain applications compliant with the GDPR. Experts argue that the most effective way to protect information is to not have it at all and zero-knowledge systems that do not have access to the customer's information will give an advantage to companies in their quest for GDPR compliance. There is a case to be made for securing breach notification exemptions for zero knowledge systems – as a breach can only access evidence that data exists.

Similarly, in the context of The Digital Markets Act (DMA), where major digital platforms are identified as 'Gatekeepers' and prevented from harvesting user personal data and combining it with other sources, ZKP technology can play an important role and contribute to easing the compliance procedures.

- ## Encryption

As a form of encryption, ZKP comes against certain policy developments in this space.

The EU institutions recognize that encryption plays a fundamental role in ensuring strong cybersecurity and the effective protection of fundamental rights of citizens. However, that it can also be used to conceal crime from law enforcement and the judiciary, making crime detection, investigation and prosecution more difficult. As a part of the EU Security Union Strategy, the European Commission has pledged to work with Member States toidentify legal, operational, and technical solutions for lawful access to electronic information in encrypted environments which maintain the security of communications. Practical steps under way include a decryption platform in Europol to help law enforcement to gain lawful access to encrypted information on devices seized during the course of criminal investigations.

This is consistent with a Resolution passed by the Council of the EU in November 2020, which focused on the challenges of ensuring public security in light of digitalisation, and in particular the exploitation of encrypted solutions for criminal activity. The Council resolved that it is essential for competent authorities to be able to access electronic evidence to conduct successful investigation and to protect victims and help ensure security. However, the Council also acknowledged that the principle of security through encryption and security despite encryption must be upheld in its entirety and should be promoted and developed. The resolution called for a review of the divergent regulatory frameworks to allow competent authorities to carry out operational tasks effectively (i.e. finding a balance between allowing authorities to access encrypted data, upholding fundamental rights and preserving the benefits of encryption).

- ## e-Evidence

Separately, the e-Evidence Regulation, proposed in April 2018 aims to enhance cross-border gathering of electronic evidence. Under it, service providers must ensure common lines of transferring data, so that the exchange of information is done in a secured way. It also includes increase involvement from of host Member State (MS) authorities in the data access orders issued by the authorities of other MS. Furthermore, online service providers must provide the requested subscriber, content, traffic, or metadata within 10 days upon receiving the order and within 16 hours in emergency cases.

ZKP can actually have a useful role in gathering of e-evidence and encrypted data by EU and national authorities if the proper approach is taken in its implementation.