



DIGITAL CURRENCIES

Governance Group

BLOCKCHAIN-BASED INNOVATIVE SOLUTIONS

DCGG BRIEFING PAPER

This paper presents three blockchain-based innovative solutions, which can find useful application in the European Union (EU) and drive positive change by harnessing the benefits of new technologies, while mitigating risks to consumers, financial stability and the environment. It firstly outlines the **Zero-Knowledge Proof** as a technology used to protect sensitive data; it then describes the positives of **Online Dispute Resolution** platforms as digital arbitration mechanisms; and lastly, it discusses the promise of a **sustainable future for blockchain transactions**.

ABOUT DCGG

Digital Currencies Governance Group (DCGG) is an international trade association and consultancy, created to strengthen the voice of the digital assets industry. We provide practical insights and state-of-the-art expert knowledge to inform legislators and regulators on opportunities and policies concerning digital-assets. DCGG seeks to facilitate an open dialogue and encourages communication between political representatives and digital currency experts to ensure that legislation supports both political objectives and innovation in the digital-asset space.

ZERO-KNOWLEDGE PROOF (ZKP)

1. What is Zero-Knowledge Proof?

A Zero-Knowledge Proof (ZKP) is a digital protocol, which allows digital authentication without disclosing sensitive personal data. By verifying information without revealing its contents, the ZKP technology can transform the way data is collected, used and transacted with. Through a series of probabilistic assessments ZKP protocols can supply pieces of unlikable information, which are utilised to validate an assertion. In other words, ZKP enables users to take full advantage of the data-based economy whilst preventing the possibility of any information from being compromised.

A number of advantages is brought about by the ZKP: the need for passwords is eliminated as well as the use of other type of sensitive data; it helps eliminate the risks associated with password-only authentication; users can share some of the transaction details if they would like; it bolsters the security of online payments.

2. Use Cases

The ZKP technology can find use cases across a wide array of digital domains, government agencies, law enforcement bodies, and even militaries in terms of nuclear capabilities. This is all possible thanks to the innovative technology, which allows for developing digital identification mechanisms that do not obligate users to reveal personal sensitive information

3. Application of ZKP in EU Legislation

The ZKP can find practical application in EU regulations - ZKP can be a significantly useful technique that can keep blockchain applications compliant with the GDPR. 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. Similarly, in the context of The Digital Markets Act (DMA), where major digital platforms are prevented from harvesting user personal data, ZKP technology can play an important role and contribute to easing the compliance procedures. Furthermore, as a form of encryption, ZKP can play a fundamental role in ensuring strong cybersecurity and effective protection of fundamental rights of EU citizens. Lastly, ZKP can have a useful role in gathering e-evidence and encrypted data by EU and national authorities under the e-Evidence Regulation.

ONLINE DISPUTE RESOLUTION

1. What is Online Dispute Resolution?

Online Dispute Resolution (ODR) platforms are decentralised open-source applications, used to arbitrate disputes in multiple types of contracts. They are built on top of the blockchain, whereby a selected panel of jurors decides on a matter and sends back a decision. Such platforms work as decentralised third parties, which are able to solve every kind of dispute by a fully automated arbitration process and rely on game-theoretical economic incentives.



2. Use Cases

The ODR mechanism works in the following way: a party registers to a smart contract operating on a blockchain for a given service. In case a dispute arises, the funds for the service are held until an online arbitration is carried out. Then an arbitration is organised by the ODR platform, whereby jurors are invited to participate in a hearing. For the arbitration process, jurors are randomly drawn from all users who have indicated their availability to serve as jurors. To indicate their availability, potential jurors purchase tokens that are specific to the ODR platform and stake them. The selected jurors rule disputes in order to collect arbitration fees and receive fees only if they had voted for the option voted by the majority. If not, they do not receive fees and lose tokens.

The underlying idea is that jurors are incentivised to vote honestly given the risk to lose tokens. Among such ODR platforms are Kleros, Mattereum Protocol, Rhubarb Fund and Aragon Network. They are capable of supporting a large number of applications in e-commerce, finance, insurance, freelancing, token listing, content moderation, travel, international trade, consumer protection, intellectual property and academia among multiple others.

3. Application of ODR in EU Legislation

ODR platforms seek to remove dispute resolution from centralised authorities and organisations by creating a streamlined, technologically based solution that can dramatically reduce costs and delays, as well as provide disputing parties with a fair and considered decision. Importantly, this technology holds the prospect of creating jobs, promoting democracy and bolstering technological innovation. DCGG believes that existing legislative requirements as stipulated by the Markets in Crypto-Assets Regulation (MICA) and the Digital Operational Resilience Act (DORA) can impose burdensome obligations on innovative technologies. In order to strengthen competition, stimulate innovation and give incentives for smaller companies to participate in the market, the EU legislator can set up a licensing scheme that reviews and authorises innovative technological ideas. By creating a friendly regulatory environment to forward-looking projects and easy market access, the EU can both invite and incentivise technological progress.

CARBON-NEUTRAL TRANSACTIONS ON THE BLOCKCHAIN

Blockchain and digital currencies are technologies with an incredible future that offer great possibilities for the digital economy. Since digital currency mining can be associated with a negative impact on the environment, members of the blockchain community have been working to address the issue by creating a sustainable solution that can be eco-friendly. Making transactions on the blockchain carbon neutral is a real prospect in the near future as a number of blockchain networks have committed to drive innovation with a negative carbon footprint. In the next 12 to 18 months technologists are expected to be able to offer a solution which improves carbon emissions by 80-85%. Blockchain leaders from the US and the UK have reported to be ready with a technology, which can achieve carbon offsetting with measurable and permanent results. DCGG believes that the EU should subsidise such innovative solutions and provide a favourable regulatory environment, which incentivises blockchain members to participate.

Given the EU's dedication to lay the foundations for a more sustainable Europe and fight climate change, supporting clean and forward-looking blockchain solutions can help the Union live up to its promise. Additionally, it can contribute for the EU to stay on the cutting edge of technology and be a leader of the digital economy.
