Berlin, August 11, 2023

How Blockchain Technology will Digitize the Euro

The European Central Bank (ECB) and the Eurosystem are planning to introduce the digital euro as early as 2026. It has not yet been decided on which technology the digital central bank currency will be based

Blockchain Bundesverband e. V. (Bundesblock) advocates that distributed ledger technology (DLT) in general and blockchain technology in particular should be used. Either as an underlying technology or with the possibility of interoperability. With this position paper, the Bundesblock wants to show the ECB, the Eurosystem and the public what benefits these technologies could have for the digital euro and how emerging risks can be minimized by using a decentralized infrastructure.

Authors (After naming the leads alphabetical order by first name)

Philipp J.A. Hartmannsgruber (Co-Lead), Board of Directors Bundesblock | PJAH Consulting

Sarah Rentschler-Gerloff (Co-Lead), Practice Partner DXC Technology Banking & Capital Market

Dirk Schuster, FGS Digital GmbH

Jan-Gero Alexander Hannemann, Head of the Bundesblock Working Groups DAO and Finance

Maren Frings, Digital Business Lead Finance, Automotive Industry

Wolfgang Lohmann, AUSY Technologies Germany AG

AGENDA

1. The ECB’s Digital Euro

The European Central Bank (ECB) and the Eurosystem are steadily pushing ahead with the introduction of the digital euro (Central Bank Digital Currency, or CBDC). On June 28, 2023, the European Commission published its legislative proposal on the digital euro, flanking the ECB's design decisions. The public still has until September 8, 2023 to provide feedback on the proposed legislation. After the legislation, it will be decided whether the digital euro will actually be introduced. However, many questions are still unanswered, such as how the digital euro will be designed in concrete terms and what technology will be used. From the point of view of Blockchain Bundesverband e. V. (Bundesblock), the advantages of blockchain or distributed ledger technology (DLT) should be used to reduce many risks, such as the restriction of privacy by a central system.

2. Advantages of Blockchain Technology for the Digital Euro

Blockchain technology is a decentralized and transparency-creating technology used to record and manage transactions and data. A blockchain is essentially a networked database consisting of a chain of information-storing data blocks.
Each block contains a list of transactions or data linked together by cryptography. The blocks are added chronologically, with each block containing a reference to the previous block, resulting in a chain of blocks - hence the name "blockchain".
The use of blockchain technology offers a number of advantages:

Decentralization: The blockchain enables decentralized data storage and management, where no central authority or intermediaries are required. This promotes trust, as control is not in the hands of a single party and manipulation is made more difficult.

Transparency: The blockchain is transparent because all participants have access to a copy of the database. Everyone can track and verify transactions and activities in real time. This increases trust and reduces corruption and fraud.

Security: The blockchain offers high security standards. The data in the blockchain is protected by cryptographic algorithms and is very difficult to change subsequently. Each block contains a hash value of the previous block, which ensures the integrity of the data. This makes the blockchain particularly resistant to hacking and forgery.

Increased efficiency: By using the blockchain, processes can be automated and inefficient intermediate steps eliminated. Financial transactions, for example, can be processed faster because third parties such as banks or clearing houses are bypassed. This can lead to cost savings and faster business processes.

Trust building: The transparency and security of the blockchain helps build trust between parties, especially in situations where trust has traditionally been a challenge. By being able to verify the data on the blockchain, companies and individuals can ensure that all information is accurate.

Innovation: Blockchain technology offers a platform for new business models and innovations. Tokenization of assets can create new financing opportunities. Smart contracts based on the blockchain enable automated and programmable contracts, which can improve the efficiency and transparency of business processes.

It is important to note that blockchain technology also brings challenges, such as scalability, energy efficiency and legal aspects. Nevertheless, the above advantages offer enormous potential for various industries and application areas.

3. Potentials

The planned digital euro in its current form holds potential when it comes to its use in various blockchain-based use cases. Below is a consolidated summary of the most important aspects:

Increased efficiency: The digital euro can lead to increased efficiency in various use cases. For example, e-commerce (online retail) payments could be processed faster and more seamlessly, improving the customer experience.

Transparency in use cases: Using blockchain technology can provide increased transparency in point-of-sale (PoS) and machine-to-machine (M2M) payments. Transactions can be publicly verified, which could lead to increased trust.

Security and data integrity: As already described in chapter 2, the integration of the digital euro into blockchain-based use cases can ensure enhanced security. The blockchain's data integrity and tamper resistance can help reduce fraud and manipulation.

Flexibility and scalability: The digital euro offers a flexible and scalable solution for pay-per-use (PPU) payments. By using smart contracts on the blockchain, payments can be automated and adapted to usage.

4. Challenges

4.1. General Challenges and Risks

However, there are not only potentials, but also certain challenges and risks with the digital euro (and in its integration into blockchain-based use cases).

Scalability: The scalability of the digital euro is a challenge, especially in use cases with a large number of transactions such as e-commerce. Standardized mechanisms must be developed to handle the increased demand and avoid bottlenecks. The scalability challenge is due to the diversity of options.

A decision in favor of a standardized method or a uniform technological solution would be necessary for this.

Data protection: The use of the digital euro in blockchain-based use cases may raise data protection issues. It is important to ensure that personal data is adequately protected and that applicable data protection regulations are complied with.
Blockchain technology is characterized by its transparency, as all transactions are recorded in a public ledger. However, this can jeopardize the privacy of users, as personal information can potentially be traced. The integration of the digital euro into the blockchain therefore requires mechanisms to preserve the anonymity of users and ensure the protection of personal data.

Offline capability: The offline capability of the digital euro poses a technical challenge, especially in use cases such as point of sale (PoS) or machine-to-machine (M2M) payments. Mechanisms need to be developed to ensure the integrity of offline transactions and minimize potential security risks.

Interoperability: Interoperability between the digital euro and various blockchain-based use cases requires uniform standards and interfaces. Integrating the digital euro into existing systems and platforms may pose technical and regulatory challenges. To ensure interoperability of the digital euro across different blockchain use cases, standardized interfaces should be developed to seamlessly integrate the digital euro into existing systems and platforms. To this end, industry-wide consortia could be formed to work together to develop and implement such standards. Collaboration between regulators, financial institutions and technology companies is critical in this regard to ensure a consistent approach and meet regulatory requirements.

4.2. Democratization

The introduction of the digital euro may pose various democratic challenges that need to be taken into account:

Data protection and privacy: The introduction of a digital euro will raise data protection and privacy issues. Since transactions are traceable on the blockchain, there is the potential for extensive monitoring of citizens' financial activities. It is important to implement mechanisms that ensure the protection of personal data and privacy.

Financial monitoring: The integration of the digital euro into blockchain-based solutions could improve the monitoring of financial transactions and make the fight against money laundering, terrorist financing and other illegal activities more effective. Nevertheless, it is of great importance to consider the potential risks of disproportionate surveillance of citizens.

It is essential to create an appropriate framework for financial surveillance that fully respects the protection rights and privacy of citizens. Transparent and proportionate implementation of surveillance measures is essential to avoid unnecessary restrictions on individual liberties.

The protection of our fundamental democratic values and civil rights must always be in line with the goal of preventing illegal activities and ensuring the security of society. State institutions should ensure that any form of surveillance is subject to clear legal requirements and effective control mechanisms to prevent abuse.

Promoting security and protection against criminal acts must never be done at the expense of individual freedoms and democratic values. A balanced approach that takes into account the common good and the fundamental rights of citizens is essential to maintain a democratic society in which every individual is respected and protected.

Digital divide: The integration of the digital euro may lead to a digital divide, as not all citizens have the necessary technological resources or expertise to make digital payments. This could lead to further marginalization of disadvantaged populations. It is important to ensure that no one is excluded from accessing financial services due to technological barriers. A technological barrier would sometimes be when individuals do not have access to digital devices and applications or cannot use them due to a physical discrepancy.

Technical dependency: The introduction of the digital euro requires a technical infrastructure to be provided by central banks, governments, financial institutions and technology companies. This could lead to dependency on specific companies or technology platforms, which could affect control over the monetary cycle. It is important to ensure that technology is open and interoperable to foster competition and innovation.

Citizen participation: Citizens should be appropriately involved in the development and implementation of the digital euro. Transparency, consultation and democratic processes should be guaranteed to ensure that the interests of the public are taken into account and that decisions are democratically legitimized.

Promoting **decentralization** and eliminating middlemen could lead to greater **transparency** and lower costs.
Transparent and traceable transaction histories on the blockchain could strengthen trust and integrity.

The democratic challenges associated with the integration of the digital euro require a balanced approach that balances the benefits of the digital euro with the protection of fundamental democratic rights and values.
Recognition of these challenges and the development of appropriate mechanisms are of great importance to ensure that the digital euro functions in accordance with democratic principles. Therefore, a commitment of acceptance of the digital

euro, as listed in the previous solution descriptions of the ECB and the European Commission in the legislative proposal, must be viewed critically.

4.3. Custody

Experience and established infrastructure: The custody of the digital euro by intermediaries such as banks would draw on their experience and existing infrastructure, even if this would require some adjustments both technologically and legally. This could ensure safekeeping of digital euro assets and give users confidence in the security of their assets. The integration of the digital euro into the two-tier banking system presents both challenges and risks, particularly with regard to the safekeeping of citizens' deposits. For banks and savings banks, this can lead to a challenge with regard to their existing business model; on the other hand, this challenge can give new market providers an opportunity with new business models.

Compliance with regulatory requirements: Banks and other intermediaries typically have extensive experience with regulatory requirements and compliance guidelines. The custody of the digital euro by these intermediaries could help ensure that the digital euro complies with applicable regulations and thus contribute to the security and stability of the digital euro.

Centralization and dependence on intermediaries: The custody of the digital euro by intermediaries would lead to centralization, as control over the assets lies with these intermediaries. This entails the risk of increased dependence on these institutions. In the event of operational failures, technical malfunctions or even systemic failure of the intermediaries, this could lead to significant problems and uncertainties. Blockchain technology could minimize these risks through decentralization.

Potential fee structures and access restrictions: There is a risk that intermediaries could introduce unfair fee structures for the custody of the digital euro or restrict access to the balances. This could limit the accessibility of the digital euro for certain user groups.

4.4. Privacy

The digital euro based on the UTXO (Unspent Transaction Output) process poses risks and opportunities for user and industry privacy. It can potentially lead to the disclosure of private transaction data, as transactions on the blockchain are publicly visible. Best protection procedures must be applied so that transactions cannot be linked to real identities.

On the other hand, the process provides transparency for the industry and enables efficient analysis and compliance. Security and anti-counterfeiting are further advantages. Striking the right balance between transparency and data protection is crucial to boosting trust in the digital euro and maximizing its benefits. Collaboration between regulators and technology developers is essential here.

Outlook and Facts

Currently, the EU considers a non-traceable digital currency a risk in terms of corruption, terrorist financing, money laundering and tax evasion. Therefore, there are restrictions:

According to the European Commission's legislative proposal, the digital euro is to exclude "full anonymity". At the same time, however, a high level of privacy is to be guaranteed. In principle, the central bank is not to have access to users' identities and information about their transactions. However, users of the digital euro must have an account with a payment service provider.

These accounts are subject to EU laws against fraud, terrorist financing and money laundering, as well as national laws. They must therefore disclose data about users' identities and their online transactions to investigating authorities upon request. Digital euro accounts are therefore similarly private to bank accounts.

It is important to note that the actual implementation of the digital euro and the implementation of the UTXO model will depend on the specific design decisions and objectives of the ECB. A careful balance between anonymity and regulatory requirements will be necessary to find an appropriate balance.

4.5. Programmability

Through programmability, the digital euro could make new functions and innovations available to users.

Benefits: Smart contracts can, for example, make it possible to automatically monitor predefined conditions and rules and automatically enforce transactions tied to them, thus improving the security of transactions. The automation of payment and business processes enables high efficiency and cost savings. The ability to manage digital identities and digital rights would enable improved authentication and access control.

Disadvantages: There is a general risk that transactions could be programmatically censored or restricted (including institutionally), for example by setting caps or even (geographic) restrictions on the purchase of certain goods or services. Complex smart contracts represent potential sources of error and could lead to problems in the smooth execution of transactions. The security of such smart contracts must be ensured to prevent misuse or data leaks. Standards and quality assurance measures will be required. A smart contract registry or building block for the financial industry is needed, with transparency and oversight managed by a consortium or institution. In addition, high technical understanding and expertise would be required for development, auditing, and legal processes.

4.6. Technical Aspects

Resources: The introduction and use of the digital euro requires a significant amount of resources. When designing for technical implementation, resource efficiency, especially energy efficiency, must be a key requirement. Efficient data processing and storage are required without compromising data integrity and

security. Furthermore, attention must be paid to indirect effects and impacts that can arise, for example, in interaction with third-party systems. One example is the premature obsolescence of functioning existing technology due to insufficient integration options.

Scalability: Practically unlimited scalability of the digital euro beyond the euro zone (> 340 million people) is essential for acceptance. Not only must it be possible to use it at any time, but a growing number of services between devices (for example, as part of the Internet of Things) requires stable and fast transaction options. Therefore, no bottlenecks and delays or strain on the network must be perceptible to ensure smooth functioning.

UTXO model: The development and introduction of a digital euro is to be based on the UTXO model. It is very efficient and allows good parallelizability in the processing of transactions. This requires special arrangements for the management of the entire set of UTXO, where connected systems must be supported accordingly to ensure smooth operation. The UTXO model, on the other hand, is more complex to program than other transaction models such as the account-based model. It requires a comprehensive understanding of transaction structures and processing. The technical complexity must not be perceptible to users.

Interoperability: Interoperability with other blockchain platforms and protocols is important, as is providing a good user experience. Addressing these challenges will require technical innovation, infrastructure investment, and collaboration between regulators, financial institutions, and technology companies. Facilitating the integration of financial services and decentralized applications could foster innovation and new business opportunities.
Compatibility issues with existing systems and infrastructures must be identified during the planning phase and taken into account during implementation.

5. Conclusion

The work of the ECB's project team - together with the Eurosystem - is progressing steadily. The European Commission is also intensively involved, in particular through its legislative proposal of June 28, 2023. A decision on the next phase of the ECB project is to be taken in the fall of 2023.

It is important that the digital euro is thought of as an overall construct that offers benefits to citizens, businesses, banks and central banks alike. Therefore, retail and wholesale CBDC must be in harmony. Blockchain technology may be applied to the latter. Since technical work has not yet begun on the retail CBDC, the Bundesblock believes that this should also take advantage of blockchain technology in order to be able to map new use cases. Only in this way can added value be generated that goes beyond what has already been possible for decades with commercial bank money or other developments from private industry. In 2024, the European Payments Initiative (EPI) will map the same use cases that are planned today with the digital euro at least two to three years earlier.

The risks associated with the introduction of the digital euro must be minimized. In particular, the privacy and data protection of users must be protected. Without the use of blockchain technology, the risks outweigh the opportunities of the digital euro. If the digital euro is not built on a decentralized infrastructure such as blockchain or distributed ledger technology, it should be rejected.