# The digital pound: A new form of money for households and businesses?

*Views from the Digital Currencies Governance Group*

## About DCGG

*Digital Currencies Governance Group (DCGG) is a trade association that represents digital assets issuers and service providers in the United Kingdom and the European Union. Our mission is to facilitate an open dialogue and encourage communication between policymakers and digital asset experts to support the design of a sound and proportionate regulatory framework that ensures safety for all market participants. Our Members include Tether - currently the largest stablecoin issuer worldwide, Ledger - a leading technology service provider for self-custody, Bitfinex - a crypto-assets exchange, ZKValidator (ZKV) - a leading proof-of-stake validator, and Iden3 - a solutions provider for self-sovereign identity management. Our team of former government officials, lawyers, and cryptoasset experts regularly engage with policy-makers and regulators both at the national and international level. For any general enquiries or to request further information, please do reach out to info@dcgg.co.uk*

### Introduction

The Digital Currencies Governance Group (DCGG) supports constructive, consultative processes with industry and relevant stakeholders in developing a sound approach to the creation of a Digital UK-issued Central Bank Digital Currency (the Digital Pound). DCGG notes that there is now room for the UK to achieve considerable progress in the digital assets landscape. There are opportunities for the country to attract both talent and capital to drive faster economic growth welcoming innovation and competition, whilst mitigating risks to consumers and stability of the financial system. This will only be possible if the Digital Pound is appropriately designed, consumer privacy-oriented and moving at a fast pace on the development of a CBDC will position the UK as a global leader on this matter.

We welcome the HM Treasury and Bank of England's initiative to consult with private sector representatives and industry experts on the potential design of the Digital Pound, which is a crucial step in the pipeline of this project. Our view is that the privacy component of the Digital Pound would be one of the main factors to be considered by users upon adoption, and we have put forward recommendations for

the use of Zero-Knowledge Proof to facilitate user protection, reduce data sharing burdens and make transacting with the Digital Pound more efficient.

## I. Digital Pound Consultation Paper

**1. Do you have comments on how trends in payments may evolve and the opportunities and risks that they may entail?**

In recent years, the field of payments has witnessed remarkable transformations driven by technological advancements and changing consumer preferences. Technology has significant capability to revolutionise the way people pay for goods and services. Automated Teller Machines (ATMs) provided convenient access to cash and expanded electronic payment options through providing greater forms of accessibility and convenience, while enabling transfers and withdrawals. The availability and connectivity of mobile phones and banking applications have similarly influenced the rise of digital payments and new trends in payments.

This is set to continue as technology continues to advance and become more integrated in the way that consumers interact and manage their finances. This includes:

1. **Contactless and Biometric Payments:** Near Field Communication (NFC), QR codes, and biometric authentication will further streamline the payment process, eliminating the need for physical cards or devices. Wearable devices may also become popular payment tools.

2. **Internet of Things (IoT) Payments:** As devices become increasingly interconnected, payments are expected to become integrated into everyday objects, such as smart appliances and vehicles. These devices could facilitate autonomous payments, enabling seamless transactions.

3. **Blockchain and Cryptoassets:** The benefits of blockchain technology are much discussed in how they can enhance security, transparency, and decentralisation in some instances. They also offer greater accessibility, lower fees, and faster, more borderless and secure transactions that can also embed smart contracts.

4. **Peer-to-Peer (P2P) Payments:** P2P offer convenience and simplicity, while digital wallets offered through messaging apps, or more securely via cold-storage wallets, will likely become more prevalent.

5. **Subscription and Recurring Payments (e.g. VRPs):** Through Open Banking, the subscription-based economy is expected to continue growing, driving the demand for recurring payment models that match consumers preferences.

6. **Central Bank Digital Currencies (CBDCs):** CBDCs have the power to revolutionise the financial system by embedding the stability and trust of central banks with the benefits of new technologies.

It is important that central banks, regulators and governments recognise the opportunities that new payment trends offer for consumers. These new forms of digital payments can offer greater opportunity for safeguarding consumers assets and finances. While these solutions will exist and develop within the market, it is important that they are encouraged, and that appropriate regulatory safeguards are put in place to encourage the development of secure solutions and products while not inhibiting innovation.

This is important with the development of a range of different forms of payment and data requirements facing consumers. New technologies, such as Zero-Knowledge Proofs, can play an important role in providing enhanced privacy, minimising data sharing and improving trust and security against authorisation attacks, while also embedding compliance with Data Protection regulations. It is important that such technologies are encouraged through providing clear regulatory frameworks, including guidelines and standards, encouraging private-public partnerships to identify barriers to adoption, and providing incentives and promoting research and development.

**2. Do you have comments on our proposition for the roles and responsibilities of private sector digital wallets as set out in the platform model? Do you agree that private sector digital wallet providers should not hold end users' funds directly on their balance sheets?**

DCGG supports the suggested roles and responsibilities of digital wallet providers in the platform model. believe that the private sector has already developed efficient solutions that ensure consumer protection and offer the functionalities listed in this consultation paper. Furthermore, the private sector is well-positioned to drive innovation, especially in the context of distributed ledger technology. This will enable the implementation of additional functionalities in digital wallets to meet user demands and align with the regulatory objectives of the Digital Pound.

In order to grant UK customers full control over their Digital Pound holdings (with appropriate limits), we agree that private sector digital wallet providers should not hold user funds. Moreover, this is a standard practice for our member wallet provider

Ledger, whose business model does not allow for holding or having any access to users' assets, granting them the necessary agency and privacy in relation to their funds, which is what we envision for the future Digital Pound infrastructure.

We also support placing liability for Anti-Money Laundering (AML) and Know Your Customer (KYC) checks on these providers in order to strengthen privacy safeguards and prevent illicit activity. With DLT-based solutions, information sharing becomes a fast and reliable process, allowing the detection of suspicious activity from a pass-through wallet within minutes. Any identified risks can then be promptly addressed by the competent authority to mitigate potential harm.

**Question 3. Do you agree that the Bank should not have access to users' personal data, but instead see anonymised transaction data and aggregated system-wide data for the running of the core ledger? What views do you have on a privacy-enhancing digital pound?**

DCGG fully supports the vision of a privacy-enhancing Digital Pound and acknowledges that users would feel more empowered to utilise the Digital Pound if their personal data is protected and transactions are secured. We believe that Personal Identity Providers (PIPs) should only disclose identity-related information to the relevant competent authority in limited circumstances of suspicious activity, as outlined in the consultation paper.

In today's increasingly digitised economy, customers are often required to provide personal data to numerous institutions, including for payment purposes. Therefore, we strongly endorse the adoption of Zero-Knowledge Proof (ZKP) technology to enhance the privacy component of the Digital Pound. With ZKPs, personal identity data points can be verified once through a Zero-Knowledge protocol and subsequently prove seamless by the PIP without the need to disclose personal information. Alternatively, in relation to Digital Pound holdings, ZKP provides the infrastructure for selective disclosure of information whereby some personal data can be proved without revealing its contents, e.g., a user can prove they have funds over a certain threshold without revealing the amount itself, and without the need for third-party verification. ZKPs would therefore provide the necessary privacy for Digital Pound users while also addressing concerns related to AML and Combating the Financing of Terrorism (CFT).

**Question 4. What are your views on the provision and utility of tiered access to the digital pound that is linked to user identity information?**

DCGG and its members fully support the concept of users having complete control over the extent of personal information they choose to share when transacting with

the Digital Pound, within the legal framework set by the government. We believe that the proposed 'tiered' access could be a valuable tool for promoting financial inclusion and facilitating access to the Digital Pound for UK customers who are new to the digital ecosystem, have limited trust, or prefer to share minimal personal identity-related information.

Zero-Knowledge Proofs would be particularly effective in a tiered access system to the Digital Pound. If implemented, mechanisms and thresholds could be established for different levels of ID-related information required for various payment amounts. This approach recognises that KYC procedures can be overwhelming or complex for segments of the population that are financially or digitally less integrated., ZKP protocols are well-suited to facilitate access with lower KYC requirements for making smaller payments, encouraging financial inclusion, and reducing barriers to entry.

To further incentivise financial and digital inclusion, under ZKP, users would only need to verify the required information once, significantly improving their overall experience with the Digital Pound. The same principle applies should users choose to conduct higher-value payments, where additional personal identity information that would be shared forKYC purposes, but only once for verification. ZKP protocols can be designed to facilitate a quick and efficient transition process for Digital Pound users based on their evolving needs and preferences.

Through the adoption of a tiered access system with ZKP technology, the Digital Pound can provide users with greater control over personal data sharing, flexibility, and improved accessibility for a wider range of individuals.

**Question 5. What views do you have on the embedding of privacy-enhancing techniques to give users more control of the level of privacy that they can ascribe to their personal transactions data?**

The success of the Digital Pound depends on a combination of trust, confidence, and several key functions it fulfils within the economy, including acting as a medium of exchange, and store of value and legal tender. Privacy is a key component to build trust and confidence in CBDCs to ensure consumers that their interactions with the Digital Pound are secure and autonomous, without being subject to monitoring and surveillance.

DCGG strongly supports embedding privacy-enhancing techniques to provide users with the necessary agency and control over their Digital Pounds. We believe the government is taking the right approach to not require any personal data records and allowing users to choose the extent of personal and transaction data they wish to share, based on their considerations and objectives. We see this as a strong factor

for adoption once the Digital Pound is launched as ZKP protocols can be applied in relation to personal transaction data as well, which allow users to selectively disclose information that can be proven and verified without revealing unnecessary personal details.

## II. Digital Pound Technology Working Paper

**Question 1. Do you agree that these six considerations are foundational technology considerations for CBDC? Are there additional or alternative technology considerations that the Bank should be focused on? (Section 3)**

DCGG views the proposed six foundational technology considerations in this technology working paper (i.e., privacy, security, resilience, performance, extensibility and energy usage) as sound and as an important basis for the future Digital Pound.

In particular, our perspective is that Zero-Knowledge Proofs are a useful technological tool for meeting these objectives, especially in relation to considerations on **privacy** (one-time verification of only necessary personal data when transacting with the Digital Pound) and **security** (encrypted personal data after one-off verification). The ZKP technology has received a large amount of academic contributions and industry funding and at this time is a viable, effective and usable privacy technology. Other emerging cryptographic techniques, such as Multi-Party Computation (MPC) and Fully Homomorphic Encryption (FHE) are on the horizon, but are at an earlier stage of development at this time. In both academia and in industry, we also see more experimentation in the combinations of ZKPs with MPC and FHE. But these also are at a much earlier stage. We recommend that the development of these solutions is closely monitored throughout the duration of the Digital Pound development in order to harness the benefits of these upcoming technologies.

**Question 2. Which privacy-enhancing technologies, or other privacy mechanisms, might support the proposed policy objectives, and how might they be used? (Section 3.1)**

DCGG supports the HMT and BoE's intention to potentially implement privacy-enhancing technologies (PETs) into the design phase to ensure the policy objectives of the Digital Pound are met and the future CBDC infrastructure meets consumer demands and promotes user protection, especially in P2B payments. As mentioned in our responses to the consultation paper, we consider the application of Zero-Knowledge Proof technology to be highly useful to facilitate data privacy protection for Digital Pound users. Not only do ZK protocols allow for one-time verification of necessary personal data, which can then be verified when needed without the need for multiple disclosure of full sets of personal information by the

user, increasing privacy and security, but these are also a useful tool for KYC verification, as well as information-sharing between PIPs and competent authorities when potential illicit activity (ML/TF) is flagged. This way, customers are granted a very high level of protection.

ZKP is a technology that has been around for 30 years, with very active academic contribution in the last 10 years and very active industry application in the last 5 years. Given the longevity of this technology, many ZK libraries have been developed and in order to mitigate potential software or protocol-level security risks within the Digital Pound ecosystem, DCGG recommends the deployment of protocol security audits and the implementation of the most used ZK libraries, which have been live and tested over a longer period of time. This will provide the necessary level of protection against software risks. Moreover, ZK experts are currently developing ZKP implementation in a modular upgradeable way, which essentially entails that a working ZKP protocol/system could be switched out for new, more efficient standards when they are introduced, allowing for alignment with technological innovation.

**Question 7. What are the most appropriate approaches or technologies for collecting and analysing aggregate transaction data? (Section 4.2)**

DCGG and its members understand the necessity of aggregate transaction data collection and analysis for the purposes of gaining in-depth insight into the extent and the ways users adopt the Digital Pound in their day-to-day lives. Yet, we would welcome further details from the HMT and BoE with regard to the analysis that is envisioned. In order to recommend potential approaches for data collection and aggregation, it is important for the private sector to understand what sort of subsequent analysis would be conducted and the overarching purposes of that analysis to make sure information collection and privacy protection are balanced. For example, ZK protocols could be a tool in the future for data processing that allows for cryptographic protection of personal user information, through the currently early-stage zero-knowledge machine learning technology. However, as a first step, we recommend that further clarity is provided in relation to the transaction analysis requirements.

**12. Is programmability and smart contract functionality an important feature of a CBDC system? If so, what is the best approach to enabling such functionality? (Section 4.7)**

We recognise the technological complexities that might emerge from implementing a smart contract functionality to the CBDC infrastructure. However, we anticipate that smart contracts would be a very effective tool to be considered for

implementation after the initial phase of the Digital Pound launch and wider adoption. Smart contracts' inherent automation functionalities can uncover a vast array of use-cases for the UK CBDC beyond the initial applications referenced in this paper. With regard to the risks outlined, we believe those could be addressed through sufficient testing against the backdrop of future policy objectives, as well as through requirements for security audits of protocols prior to launch. We encourage the BoE and HMT to continue consulting with the private sector to find ways to cooperate on an easy and effective way to implement into the design phase and harness the benefits of permissionless Blockchain infrastructures to strengthen the resilience of the Digital Pound in the future.

**Conclusion**

DCGG's members are highly dedicated to user privacy in the digital economy. The Digital Pound is a landmark project in the UK payments landscape, and we foresee widespread adoption, as long as the privacy component is comprehensively addressed in the design phase. Implementing privacy-enhancing technologies like Zero-knowledge proof in the architecture of the Digital Pound system will make the CBDC significantly more attractive to users and will bring immense competitive advantage to the UK.