Copper,
17A Curzon Street
Mayfair
London,
W1J 5HR

Digital Currencies Team
Bank of England
Threadneedle Street
London
EC2R 8AH

cbdc@bankofengland.co.uk

12th June 2020

Dear Digital Currencies Team,

Copper welcomes the opportunity to respond to the Bank of England's ***Discussion Paper: Central Bank Digital Currency Opportunities, challenges and design, March 2020.***

Copper is a recognised pioneer in providing secure digital infrastructure for institutional investors of digital assets. Our solutions enable clients ranging from funds, financial institutions and high-net-worth private traders, to acquire, store and trade more than 100 digital assets with absolute certainty that their capital is not at risk from hackers or other malicious players.

We applaud the Bank of England for its commitment to exploring the development of a CBDC, and its potential added value to the UK economy. In this letter, we provide our response to the points made in **Chapter 6.5, Security and use of cryptography** and to **Question 35** regarding what innovations should be factoring into a CBDC design. We discuss how multi-party computation (MPC) cryptography can enable the accessibility of a CBDC whilst ensuring robust protection and total autonomy over digital assets.

We take the view that the CBDC model described in Chapter 1, '*electronic form of central bank money that could be more widely used by households and businesses to make payments and store value*', is ambitious but achievable.

In response to question 35: ***What other future technology and digital economy innovations should we be factoring into the potential design of CBDC? How might these impact the future demands placed on CBDC, and potential approaches to designing a CBDC?***

Copper believes that for any CBDC to thrive in today's threat landscape, the most secure, versatile and scalable security solution would need to be factored into the design. Multi-party computation (MPC) is a powerful cryptographic tool that is setting a standard unlike any other in the safeguarding of digital assets.

The novel solution of MPC affords wallet holders robust protection from potential security breaches. Its highly specialised mathematical approach to private key management eliminates the need for a master private key. Instead, MPC distributes key shards among the devices of participating parties. As a whole key is never created in the first place, it therefore cannot be compromised.

Drawing on another protocol of secure computation called zero-knowledge proof, which works by verifying information between parties without revealing the information itself, a key shard can prove that it has the right to co-sign a transaction.

Because the key that executes the transaction is a collectively generated value, it means a single key never exists in whole, or lives on any one device. This renders an attack in key theft effectively impossible while also protecting against internal fraud and collusion – preventing any employee, or group of employees, from misusing the key.

MPC is fundamentally different from other known key management alternatives, where there is typically a reliance on a trusted third party with which data is centrally shared and stored in for some period of time.

Traditional cryptography requires the user to place trust in either their own computing device to securely store the private key (without ever being lost or compromised), or place their trust with a third party such as a hardware security module (HSM) to securely store the private key. Threshold cryptography eliminates this single point of failure by using MPC to transfer trust from a centralised to a decentralised model.

It is also worth noting that MPC systems provide the ability to maintain safe and secure cryptographic operations even if one or potentially more of the parties' devices become hacked or compromised. This allows for corrupt systems to be recovered, without the service disruption that exists with alternative protocols.

We conclude by reiterating that an MPC-based key management system would be an essential component in the technological architecture of a secure and accessible CBDC. An effectively implemented MPC system would meet the BoE's high requirements for confidentiality and integrity more than any other known key management alternative.

Copper recently engaged Professor William Knottenbelt, Professor of Applied Quantitative Analysis at Imperial College to conduct an independent assessment of MPC versus other private key management encryption protocols and/or others, with a view to assessing the robustness of each technique in the secure management of transactional data. We would be happy to share the results of this research paper with you, and have a discussion with Professor Knotttenbelt, when the research is complete in around two months.

We also agree with the BoE that proper interoperability for cross-border, multi-currency payments among upcoming CBDCs will require direct collaboration between issuing central banks and private sector firms. It is for this reason that Copper recently joined the Official Monetary and Financial Institutions Forum's (OMFIF) Digital Monetary Institute (DMI) as a founding member.

The team at Copper stands ready to help and support the BoE in its research into CBDCs, and are available for follow up questions or discussions.

Yours sincerely,
Dmitry Tokarev
Copper, Founder & CEO