BANK OF ENGLAND

Fintech Proof of Concept

Chain – exploring how distributed ledgers can be configured to enable privacy amongst participants whilst keeping data shared across a network

Background

In this Proof of Concept (PoC) with Chain, the Bank wanted to explore how distributed ledgers could potentially be configured to enable privacy amongst participants whilst keeping data shared across a network.

One of the Fintech Accelerator's first PoCs raised questions about whether confidentiality could be maintained in a distributed ledger system and the possible trade-offs between privacy, performance and resilience this brings. Questions relating to the technical issues around privacy were also identified in the digital currencies research questions published by the Bank in 2016.

The engagement with Chain helped the Bank to get a better academic understanding of how recent innovations in cryptography can ensure privacy in a distributed ledger system, and to consider some of the potential trade-offs that the solutions involved.

The Proof of Concept

The work undertaken with Chain was an academic, rather than a practical, exercise and did not develop testable technology. However, the exercise did explore some of the key questions that could arise from ensuring privacy on a distributed ledger system.

The scenario considered for this exercise assumed the transfer of ownership of a fictional asset amongst several participants, including a central authority and a regulator. The central authority would have the ability to issue new units of the assets as well as retire units, and grant access to participants to use the ledger, and the regulatory authority would have the ability to view all transactions. The Bank's key objectives were to:

- Explore how DLT based systems could be configured to ensure that no party (except for the regulator) was able to infer details about transactions which they were not counterparty to, including ensuring that participants in the consensus process did not have full visibility of transaction details;
- Understand how the choice of privacy solution affected the performance of the system as well as the trade-offs, risks and challenges this presents.

For the purposes of this exercise, the Bank's preference was to explore solutions that used cryptographic techniques to ensure privacy amongst participants whilst keeping data fully distributed across all participants and thus maximising resilience benefits. Experiments by other central banks[1] have also touched upon some of the trade-offs implied by alternative approaches to privacy in DLT.

[1] For example, see Bank of Canada's Project Jasper and Monetary Authority of Singapore's Project Ubin.

Reflections and next steps

In this cryptographic approach to privacy, an attacker would need to obtain the private keys to every transaction in order to decrypt all of the data. Whilst this may be unlikely[2], a risk will always remain that future breakthroughs in cryptography or computing power render the entire scheme vulnerable and may provide retroactive access to information, regardless of the soundness of the encryption techniques today.

The discussion with Chain highlighted that many of the key challenges and risks would depend on decisions around process flows and the structure of the network as much as on the specifics of the technical solution itself. For example, Chain's confidentiality scheme hid asset identifiers and amounts for all transactions and allowed unblinding through the sharing of blinding keys. The overall resilience of the system would be affected by the approach chosen by the regulatory node and whether they would be required to proactively participate in the signing of transactions as they occur or just observe and rely on actions and incentives outside of the technical solution.

The exercise helped confirm thinking on the range of the potential approaches to the privacy challenge in DLT. Many of the alternative approaches involve scenarios where data is not fully distributed amongst all participants in the network; instead data is only shared between those participants directly involved in each transaction; this type of approach has obvious advantages in achieving privacy, but also potentially weakens some of the prospective resilience benefits of DLT. On the other hand, cryptographic privacy solutions which keep data shared across all participants are still in the very early stages of their development, and examples of their deployment at scale are limited.

Overall, it appears *theoretically* possible to configure a distributed ledger system in such a way that transactions remain private whilst keeping all data shared across the network, and at the same time maintaining a regulatory view of all transactions. However, the trade-offs would still need to be further explored, especially with respect to scalability, speed of transaction processing and risks around the security of the cryptographic techniques employed.

[2] Individual transaction data could be compromised by obtaining individual keys but the likelihood of *all* keys being obtained is much lower.