New Development Bank

Project Khokha – South African Reserve Bank

ITU Focus Group on Digital Currency including Digital Fiat Currency

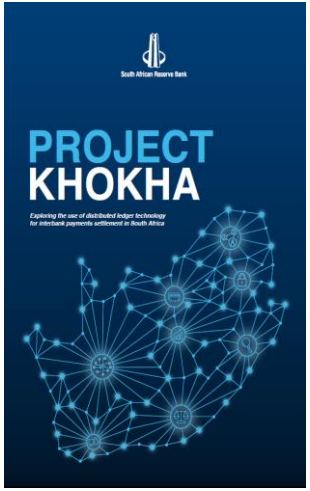
June 12, 2019 Geneva, Switzerland

Srinivas Yanamandra

Chief - Compliance

New Development Bank

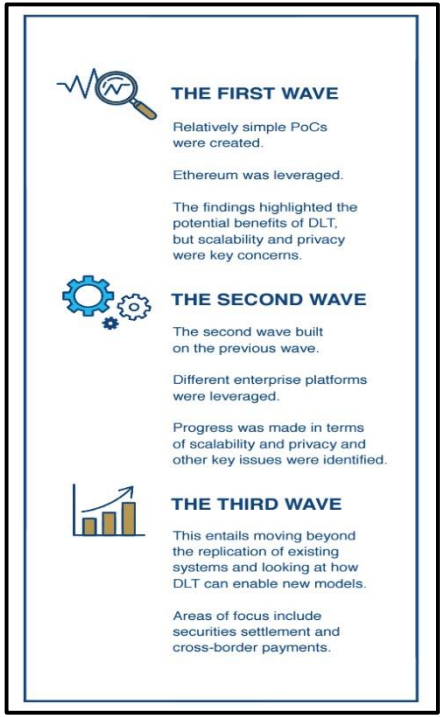
Shanghai

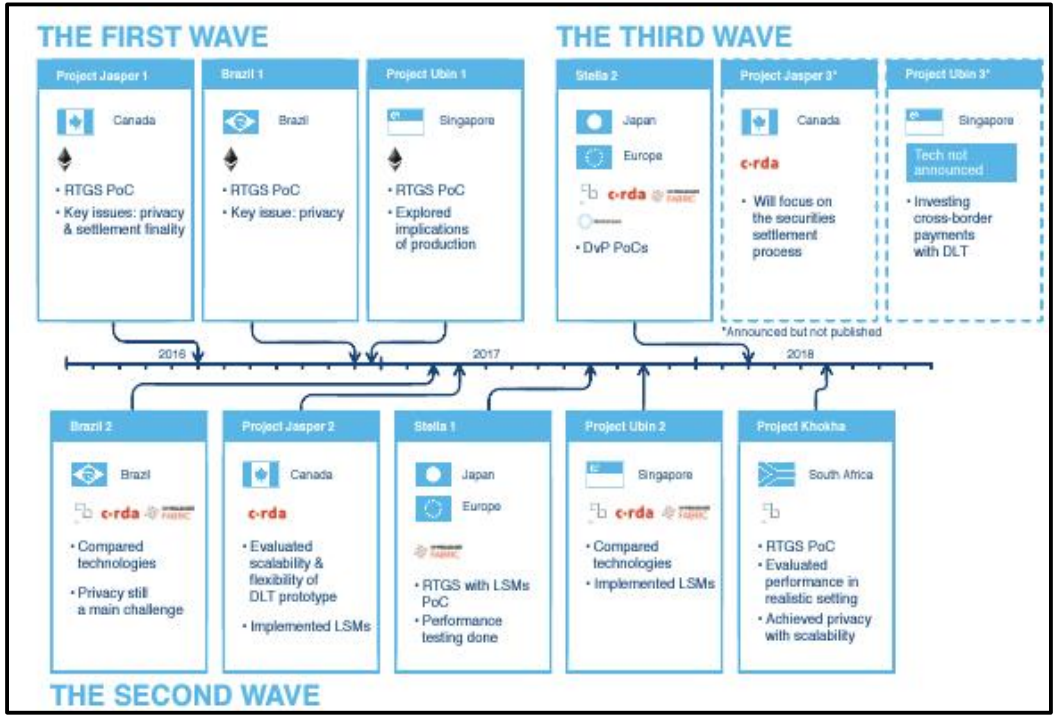


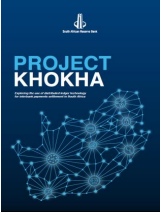
Disclaimer: *The views expressed herein are based on the Project Khokha report released available in public domain. Views expressed herein does not necessarily reflect the views of NDB or of SARB*

Background and context

The three different waves of experiments with CBDCs







Evolution of CBDC experiment at SARB

For exploring the DLT innovation in the context of payment & settlement systems

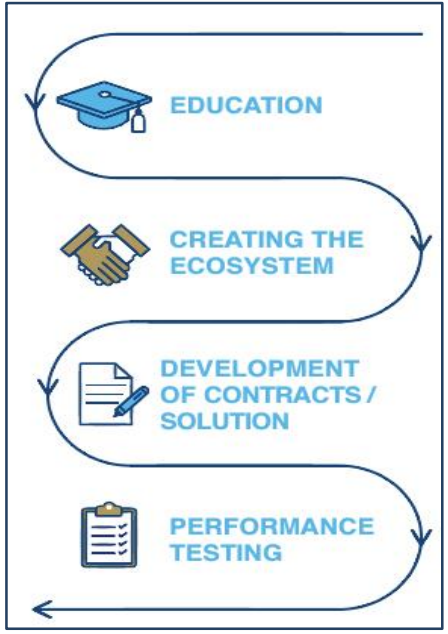
Laying down the foundation

Project Khokha is a collaborative initiative using distributed ledger technology.

Project Khokha is seen as an initiative in collaborating for innovation, therefore both the process as well as the outcome of the project contribute to the SARB's goals. The decision was made to assess the use case for DLT in wholesale payments and interbank settlement and thus build on and extend the work done in other parts of the world. The SARB engaged ConsenSys as the technical partner on the project and worked with a consortium of banks made up of Absa, Capitec, Discovery Bank, FirstRand, Investec, Nedbank and Standard Bank.

PROJECT KHOKHA IS SEEN AS AN INITIATIVE IN COLLABORATING FOR INNOVATION.

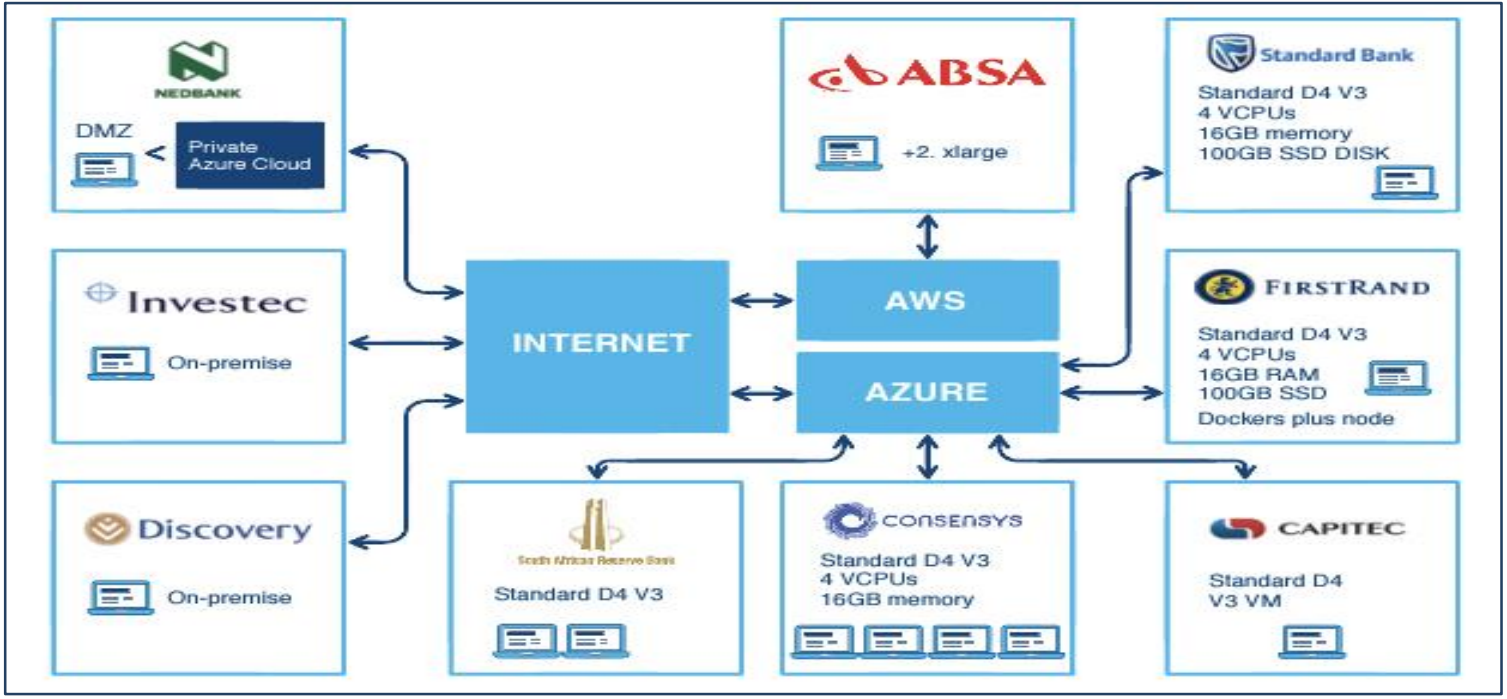
Identification of the Project

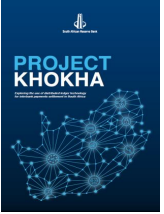


Gearing up the eco-system

An overview of Project Khokha

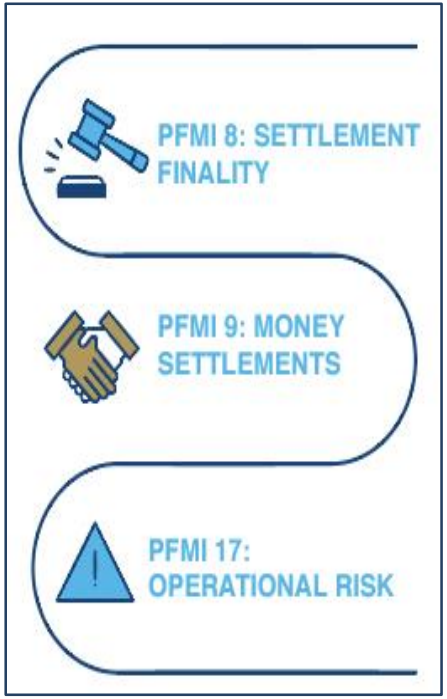
With participation from financial institutions / technology vendor





Statement of hypothesis / performance standards

Against which the pilot project has been tested



The Experiment

Iterations and project highlights

PRIVACY & TRANSPARENCY

Both transaction-level privacy and network-wide transparency are supported. It is customisable to requirements. For this project, Whisper peer-to-peer messaging, Pedersen commitments and range proofs were the mechanisms used to enable privacy.

PERFORMANCE & THROUGHPUT

Quorum has been designed to achieve realistic throughputs associated with the financial services industry. This is partially enabled by including options for consensus mechanisms. The mechanism used here was Istanbul Byzantine Fault Tolerance (IBFT).

PERMISSION & GOVERNANCE

Quorum supports blockchains around permissioned groups of participants, with transaction validation and block creation distributed throughout the network.

Project undertaken in four iterations

1. Straightforward transfer between two banks
2. Very similar to the current process (bank A effectively sent a payment instruction that the SARB executed)
3. Amounts and balances were shielded (Network only seeing the Pedersen commitment for each transaction - SARB still approved the transfer)
4. Amounts and balances are shielded - visible only to the two parties to the transaction and the SARB (Network only sees the Pedersen commitment and the nodes on the network approve the transaction via range proofs.)

Istanbul Byzantine Fault Tolerance - first time in CBDC experiments

Pedersen commitments used to enable confidentiality

Whisper messaging is used at start-up for SARB oversight

Conclusions and implementation considerations

Conclusions

- Project Khokha has been declared successful as it has achieved its stated objectives
- BIS benefits and risks framework has been useful for analysis.
- Existing industry groups helped to lay the foundation for collaboration on Project Khokha.

Implementation considerations for production readiness

- Additional work on integrating with bank systems at deployment level
- Several DLT issues to be resolved at technology level
- Macroeconomic considerations of DLT-based real-time gross settlement at higher level

Thank you!