Effective date: 1 April 2024

GUIDELINES FOR FINANCIAL INSTITUTIONS
GUIDELINES NO. TRS/G-4/2024/1

GUIDELINES ON BLOCKCHAIN PLATFORM

1. INTRODUCTION

1.1. Brunei Darussalam Central Bank (BDCB) has been closely monitoring the domestic and global developments of Blockchain technology. BDCB views Blockchain technology as potentially beneficial to the financial sector in Brunei Darussalam especially in enabling near real-time transaction, advanced security, and improved transparency. However, proper governance is important to oversee the risks, operation resiliency and financial consumer protection.

1.2. These Guidelines are issued for banks and financial institutions (FIs) that wish to adopt Blockchain platform for their critical systems, service delivery, or in handling consumer personal data. These Guidelines focus on the implementation of Blockchain platform only, instead of the use case. Nevertheless, specific use case relating to Blockchain technology can be referred to applicable Notices or Guidelines relevant to the type of financial services involved.

1.3. These Guidelines are issued pursuant to section 32 of the Brunei Darussalam Central Bank Order, 2010 ("BDCB Order") and are aimed at banks and FIs licensed, registered, or regulated under the following:

1.3.1. Banking Order, 2006;

1.3.2. Islamic Banking Order, 2008;

1.3.3. Insurance Order, 2006;

1.3.4. Takaful Order, 2008;

1.3.5. Finance Companies Act, Chapter. 89;

1.3.6. Securities Markets Order, 2013;

1.3.7. Money-Changing and Remittance Businesses Act, Chapter 174;

1.3.8. Moneylenders Act, Chapter 62;

1.3.9. Pawnbrokers Order, 2002; and

1.3.10. Payment and Settlement Systems (Oversight) Act, Chapter 251

1.4. These Guidelines are also applicable to:

1.4.1. Operators of payment systems that have been approved to operate in Brunei Darussalam under the Notice on Requirements for Payment Systems (Notice No. PSO/N-1/2020/1);

1.4.2. Perbadanan Tabung Amanah Islam Brunei established under the Perbadanan Tabung Amanah Islam Brunei Act (Cap. 163); and

1.4.3. Any other entity or person specified by the BDCB, that are licensed, approved or regulated by the BDCB under any written law and directions issued thereunder.

1.5. These Guidelines should be read with:

1.5.1. Notice No. TRS/N-1/2023/2 on Technology Risk Management (hereinafter referred to as "Notice No. TRS/N-1/2023/2");

1.5.2. Guidelines No. TRS/G-2/2022/1 on Technology Risk Management (hereinafter referred to as "Guidelines No. TRS/G-2/2022/1"); and

1.5.3. Guidelines No. TRS/G-3/2022/2 on IT Third Party Risk Management (hereinafter referred to as "Guidelines No. TRS/G-3/2022/2").

1.6. These Guidelines should also be read with the following:

1.6.1. Notice on Application for Approval of Outsourcing Arrangement for Insurance Companies and Takaful Operators (Notice No. TIU/N-1/2019/11);

1.6.2. Notice on Early Detection of Cyber Intrusion and Incident Reporting (Notice No. FTU/N-1/2017/1 and TRS/N-1/2020/1);

1.6.3. Notice on Market Conduct (Notice No. FCI/N2/2021/1);

1.6.4. Notice on Outsourcing for Capital Markets Services Licence Holders (Notice No. CMA/N-1/2020/15);

1.6.5. Guidelines on Outsourcing Arrangement for Insurance Companies and Takaful Operators (Guidelines No. TIU/G-1/2019/10);

1.6.6. Guidelines on Outsourcing for Banks;

1.6.7. Guidelines on Standard Technology Risk Management for Money Changer and Money Remittance Businesses (TRS/G-1/2019/1);

1.6.8. Any other notices, directives or guidelines, which the BDCB may issue from time to time.

1.7. These Guidelines are not exhaustive and subject to revision from time to time as deemed necessary by the BDCB.

1.8. These Guidelines take effect on 1 April 2024.

2. DEFINITIONS

2.1. For the purposes of these Guidelines, the following terms have the following meanings except where the context otherwise requires –

2.1.1. "Administrator" refers to a role in the blockchain platform that is responsible for administering and managing the blockchain platform and nodes;

2.1.2. "Blockchain platform" refers to common IT system and infrastructure of blockchain technology that can be set up to run specialised services or applications;

2.1.3. "Blockchain technology" refers to IT solutions that use Distributed Ledger Technology, in which the database is decentralised so that no centralised intermediary is required;

2.1.4. "Consortium" refers to group of organisations (i.e. FIs, counterparties) that are accountable for decision-making related to the blockchain platform, and responsible for general oversight of the management and operation of the blockchain platform;

2.1.5. "Counterparties" refers to entity that provide services to the banks and FIs mainly through mandate, trust, cooperation or membership. This includes, but is not limited to, government agencies, regulators, and financial market infrastructure (e.g. SWIFT and payment settlement system). This does not include service providers or vendors.

2.1.6. "Critical system" refers to any system that supports the provision of banks or FIs services, where failure of the system can significantly impair the banks' or FIs' provision of services to its customers or stakeholders, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements;

2.1.7. "Emerging risks" refers to new or unforeseen risks that have not been detected, which can be due to insufficient use-case and testing;

2.1.8. "Financial Institutions" or "FIs" have the same meaning as section 2 of the BDCB Order, 2010;

2.1.9. "Group" refers to parent and subsidiary offices or branches that belongs to same corporate group as the bank and FI;

2.1.10. "Kill-switch" refers to a mechanism to abruptly stop a process or transaction during an emergency;

2.1.11. "Node" refers to an entity or individual authorised to join a blockchain network and to become part of a blockchain platform;

2.1.12. "Off-chain" refers to transactions, data or components that are outside of blockchain;

2.1.13. "Off-chain components" refers to external components, including but not limited to payment exchange system, external database, administrator console, or user interface website that resides outside of blockchain;

2.1.14. "On-chain" refers to transactions, data or components that are inside of blockchain;

2.1.15. "On-chain components" refers to components that are within the blockchain, which are commonly the nodes, ledger, and algorithm;

2.1.16. "Operator" refers to a node in a closed, private or permissioned blockchain that is responsible for running blockchain's software, and certifying transactions by writing new blocks and broadcasting them to the network;

2.1.17. "Operator role" refers to a role assigned to personnel of the Operator that are responsible for running the software or service in the blockchain, and to certify and broadcast transactions in the blockchain platform;

2.1.18. "Participant" refers to a node in a closed, private or permissioned blockchain that are granted access to shared ledger and store copies of it;

2.1.19. "Service provider" refers to an individual or entity that provides a service to the banks and FIs, including a member of the Group to which the banks and FIs belongs, e.g., Head Office, parent insurer, another branch or related company, whether it is in Brunei Darussalam or elsewhere;

2.1.20. "Smart Contract" refers to an algorithm that runs when predetermined conditions are met, and is intended to be used to automate agreement process;

2.1.21. "Vendor" refers to an external individual or entity that offers solutions to the banks and FIs directly or through suppliers and service providers.

2.2. Any expression used in these Guidelines, except where expressly defined in these Guidelines or where the context requires otherwise, have the same meaning as in the BDCB Order, 2010.

3. PROJECT MANAGEMENT

3.1. There should be strong justification to move critical systems, service delivery or consumer personal data to a blockchain platform. The goals and requirements of the move should be defined and incorporated into the banks or FIs' overall IT strategy.

3.2. Banks and FIs should conduct sufficient feasibility studies before implementing and moving to the blockchain platform. The feasibility studies should include considerations on existing resources and capabilities of the banks and FIs. Banks and FIs should also refer to Paragraph 4.3 of Guidelines No. TRS/G-2/2022/1 on System Acquisition.

3.3. Implementing or migrating to the blockchain platform should be managed based on the banks' and FIs' project management framework and outsourcing framework. Banks and FIs should refer to Paragraph 4.2 of Guidelines No. TRS/G-2/2022/1 on Project Management, and Paragraph 4 of Guidelines No. TRS/G-3/2022/2 on IT Outsourcing.

4. GOVERNANCE

4.1. Banks and FIs should be mindful of inadvertently introducing digital financial services or new form of financial services that require license or approval from BDCB when implementing the blockchain platform. Therefore, Banks and FIs should refer to applicable BDCB Legislations, Notices and Guidelines that govern similar financial services. Banks and FIs should consult BDCB for any financial-related services that do not require a specific license yet, or not being addressed explicitly in any Notices or Guidelines.

Individual or Group Blockchain Platform

4.2. Banks and FIs should assess and designate Administrator, Operator and Participant roles in the blockchain platform.

4.3. Third-party service providers or vendors of the blockchain platform should not be assigned as Administrator, Operators or Participants of the blockchain platform. The role of third-party service providers or vendors of the blockchain platform is to support and maintain the blockchain platform at infrastructure and system level only.

4.4. An Administrator role should only be handled by key senior personnel of the bank and FIs, who are deemed as fit and proper by the board of directors and senior management of the bank and FIs. The following criteria should be considered to determine the fitness and propriety of a key senior personnel handling the Administrator role:

4.4.1. Competence and capability

4.4.2. Honesty, integrity, fairness and ethical behaviour; and

4.4.3. Financial soundness.

4.5. The board of directors and senior management of the banks and FIs should be held accountable and responsible for the oversight and any decisions relating to the Administrator and Operator roles of the banks' and FIs' blockchain platform.

4.6. An Administrator of the blockchain platform should conduct on-going due diligence on all Operators and Participants, and be able to monitor and manage Operators and Participants, including removing them from the blockchain platform when required.

4.7. A blockchain platform should be made closed, private or permissioned-based, where an Administrator should be able to restrict Operators and Participants to specific target groups such as Group, or counterparties.

4.8. There should be requirements established for an Operator and Participants before they can enter the blockchain platform, which should include but is not limited to the following:

4.8.1. IT and information security policies or guidelines;

4.8.2. Terms and Conditions;

4.8.3. Privacy policy; and

4.8.4. Legal or regulatory requirements (e.g. AML and CFT).

4.9. The Operator and Participants should enter into an agreement on the use of blockchain platform, that includes complying to paragraph 4.8.1 to 4.8.4 above.

4.10. For blockchain platforms operated by banks or FIs within their Group only, an Administrator role should only be assigned to key senior personnel from the head office or headquarter level. Depending on the governance structure of the banks or FIs, Operator's role(s) should be restricted to the services or functions required for the blockchain platform's intended use cases.

Consortium-based Blockchain Platform

4.11. For blockchain platforms that are jointly operated with other banks and/or FIs, or counterparties, a blockchain consortium should be established. The consortium should designate key senior personnel from one bank or FI to become an Administrator. Notwithstanding Paragraph 4.3, the consortium may designate a trusted counterparty rather than a bank or FI to become an Administrator.

4.12. For banks and FIs that wish to join a counterparty's blockchain platform and subsequently become part of the counterparty's consortium, there should be at least one local bank or FI, the board of directors and senior management of the bank and FIs that make up the Consortium shall assess that the representative is deemed fit and proper.

4.13. The banks and FIs should ensure that controls stated in this Paragraph 4.2 to 4.10, or equivalent are considered by the consortium.

4.14. The consortium may assign more than one Operator, depending on the size and intended use cases of the blockchain platform, but there should be policies and controls in place to ensure that the Operators act according to decisions or agreement of the consortium.

5. TECHNOLOGY RISK MANAGEMENT

5.1. Banks and FIs should be mindful of emerging risks associated with the use of blockchain platforms, that may not be identified in any existing technology. Therefore, it is important to continuously assess and monitor the risks as blockchain platforms become more developed.

5.2. Banks and FIs should identify and assess all components in on-chain and off-chain, and understand how the transaction flows within the components.

5.3. Servers, computers, or devices that host, run or are part of the blockchain platform on both on-chain and off-chain should be maintained and securely configured. This should be outlined in policies or guidelines stated in Paragraph 4.8.1 above.

5.4. Banks and FIs should assess and determine appropriate integration methods when connecting to an off-chain external system with the Blockchain platform. The external system and the integration component may be subjected to common application vulnerabilities and should be addressed accordingly.

5.5. Personal data should be stored off-chain for blockchain platform hosted by a third-party vendor or owned by a counterparty, while unique reference to the personal data can be stored on-chain when pseudonymised. In any case, banks and FIs should ensure personal data is handled safely based on Paragraph 10.1 of Guidelines No. TRS/G-2/2022/1.

5.6. When a process in the Blockchain platform is automated using certain algorithms such as smart contract or blockchain transaction verification, the banks and FIs should be able to demonstrate to BDCB, customers and stakeholders the processes that takes place in a transparent manner. Automated process is considered as using Artificial Intelligence, so the banks and FIs may refer to Paragraph 4.13 of the Guidelines No. TRS/G-2/2022/1.

5.7. Further to Paragraph 5.6 above, an Administrator of a Blockchain platform should be able to intervene in any automated processes in the Blockchain platform at any time. This includes the use of a "kill-switch" at off-chain administrator console to temporarily stop all processes or transactions with minimal impact as much as possible.

5.8. In addition to the types of testing outlined in Paragraph 4.9 of Guidelines No. TRS/G-2/2022/1, banks and FIs should also conduct performance and readiness testing such as performance tests and stress tests, depending on the volume of transactions and number of nodes in the Blockchain platform, to ensure the Blockchain platform is stable.

6. BUSINESS CONTINUITY

6.1. Banks and FIs should establish incident management processes specific to the use of Blockchain platforms that take into consideration of the on-chain components and off-chain components. The incident management process should be incorporated with the incident reporting requirements as stated in Notice No. FTU/N-1/2017/1 and TRS/N-1/2020/1.

6.2. Banks and FIs should also ensure that there are incident reporting processes between all Participants and Operator(s) in the Blockchain platform. This should be outlined in policies or guidelines established under Paragraph 4.8.1 above.

6.3. Banks and FIs should establish business continuity plans (BCP) and disaster recovery plans (DRP) for business operations or data that can be impacted when there are disruptions or downtime on the Blockchain platform.

6.4. Banks and FIs should prepare an exit strategy, that consists of a response plan to be executed in case of prolonged failure in the Blockchain platform, or sudden termination by the Administrator.

6.5. Banks and FIs should establish a data backup process for on-chain data in the Blockchain platform, and off-chain data in the off-chain component.

6.6. The Blockchain platform should continuously be monitored by the Administrator and Operator. If there are any issues that may affect the Blockchain platform, nodes, data and/or other components, all Operators and Participants should be alerted.

7. LOGS AND RECORDS

7.1. Banks and FIs should ensure that processes or activities carried out on the Blockchain platform are recorded. This information should be stored based on applicable legislation or regulation pertaining to data and logs retention and audit.

7.2. Banks and FIs should be able to access transactions and relevant activity logs of the Blockchain platform such as through compliance management portal or log collection server at off-chain. Otherwise, the banks and FIs should ensure that the information can be requested from the Administrator or consortium when required.

7.3. Banks and FIs should be able to generate or request regulatory reports for compliance or data reporting purpose, such as Anti-Money Laundering reporting requirement and statistical data when requested by BDCB.

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 6 Sya'ban 1445H / 16 February 2024M