2024-03-04

Database Privacy: Design of User Privacy Preserving Central Bank Digital Currency: A Case of Tanzania

Minja, Godbless

Indian Society for Education and Environment (iSee)

https://doi.org/10.17485/IJST/v17i14.3193

INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Database Privacy: Design of User Privacy Preserving Central Bank Digital Currency: A Case of Tanzania

Godbless G Minja[1]*, Devotha G Nyambo[1], Anael E Sam[1]

1 The School of Computational and Communication Sciences and Engineering, The Nelson Mandela African Institution of Science and Technology, P. O. Box 447, Tengeru, Arusha, Tanzania

OPEN ACCESS

Received: 20-12-2023

Accepted: 07-03-2024

Published: 03-04-2024

Citation: Minja GG, Nyambo DG, Sam AE (2024) Database Privacy: Design of User Privacy Preserving Central Bank Digital Currency: A Case of Tanzania. Indian Journal of Science and Technology 17(14): 1439-1449. https://doi.org/10.17485/IJST/v17i14.3193

* **Corresponding author**.

godblessminja@gmail.com

Funding: MoEST – HEET Scholarship (UDOM)

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: This work aims to contribute towards Tanzanian Central Bank Digital Currency (CBDC) users' privacy preservation. It proposes the design of a privacy preserving CBDC which might be issued by Tanzania's Central Bank (CB), the Bank of Tanzania (BoT), which is currently in CBDC research phase. The work also aims to contribute to literature, the CBDC research being done by BoT, other CBs and CBDC stakeholders around the world. **Methods:** By using the Design Science Research (DSR) methodology, a privacy preserving CBDC design suitable for Tanzania was proposed, demonstrated and evaluated. This is the result of existing literature showing that different countries have different CBDC designs due to their differences in contexts and purposes for CBDC issuance. This consequently emphasized the fact that a CBDC design should not be treated as a one-size fits all solution. **Findings:** As opposed to the existing general and other country specific CBDC designs, we proposed a privacy preserving CBDC design suitable for Tanzania by consulting literature and taking into consideration the Tanzanian context. The design appears to be promising Tanzanian CBDC users' privacy preservation though further work needs to be done. The work should not only be on practical evaluation of the proposed design but also on other factors impacting the success of CBDC projects. This will consequently further increase the success probability of CBDC projects, hence the potential for practical realization of CBDC project benefits. **Novelty:** Existing literature has shown that, considering the countries' differences in context and CBDC issuance purposes, CBDC design should not be treated as a generic solution thereby obliging the need for country-specific CBDC designs. Consequently, the privacy preserving CBDC design suitable specifically for Tanzania consists of and provides an outline of privacy preserving interactions among the identified key Tanzanian CBDC participants or actors. The actors are the BoT, the intermediaries (i.e., other banks and payment service providers), Tanzania's National Identification Authority (NIDA), financial transactions violation detection engine, and the expected CBDC users.

Keywords: Digital currency; database privacy; central bank digital currency; privacy

1 Introduction

A digital currency is a currency form that exists only in electronic or digital form, and can be used to make online payments. Digital currencies are often divided into two categories; cryptocurrencies and central bank digital currencies (CBDCs). Cryptocurrencies use cryptography for security, and are created and managed by a decentralized network of computers. Examples are Bitcoin (BTC), Ethereum (ETH) and Dogecoin [1],[2]. On the other hand, CBDC is a digital version of a country's official currency with cash-like attributes that is issued and regulated by the country's central bank (CB). Examples are Bahamas' Sand dollar, Nigeria's eNaira and China's eCNY. CBDC has drawn the attention of more than one hundred countries, representing over 95 percent of the global gross domestic product (GDP). Additionally, CBDC has a number of potential benefits such as improving monetary policy conduct, enhancing efficiency of digital payment systems, lowering transaction charges and increasing financial inclusion [1],[2]. In connection with those concepts, database privacy is the protection of sensitive personal information such as names, addresses, phone numbers, emails, postal and physical addresses, financial and medical records stored in a database from unauthorized access, use or disclosure [2]. It includes implementation of measures and practices to ensure that such data remains confidential and is accessible only to authorized individuals and entities. Additionally, database privacy provides protection from harms such as identity theft, reputational damage, regulatory and legal damages, and financial fraud among other privacy compromise consequences [2]. Since CBDC is a digital currency, it will collect, store and process certain personal information of its users thereby making it possible to expose users' wealth, interests and health (i.e., through users' transactions data and patterns), hence making privacy concerns inevitable [3]. Furthermore, privacy preservation in a country's CBDC is a concern since it is one of the features provided by the country's physical fiat currency (i.e., cash). This concern has also been highlighted by various CBDC stakeholders who include the general public, economists, computer scientists and engineers, national and international financial organizations, and scholars among others [4]. Existing literature has also shown that countries differ in contexts and CBDC issuance purposes thereby emphasizing that CBDC design should not be considered as a universal solution, hence requiring a country-specific CBDC design approach [5],[6],[7]. Additionally, considering the degree of attention drawn on CBDCs, their potential benefits, and the risks associated with the raised CBDC privacy concerns, the design of a privacy-preserving CBDC will contribute to increasing the success probability of a CBDC project. Consequently, this work aims to propose a privacy preserving CBDC design suitable for Tanzania. It will provide a description of privacy in CBDCs, the important design considerations for a privacy preserving CBDC as extracted from existing literature, and the proposed Tanzanian privacy preserving CBDC design. It also includes the proposed design's demonstration and evaluation, and eventually a conclusion with suggestions of future related research work areas.

Privacy in a CBDC can be defined as ensuring that the users' data is used only in steps strictly necessary for the specific purpose of determining whether a transaction is lawful, and if this is the case, executing it. It is also recommended to be 'privacy by default' implying that privacy should be ensured without the need of any intervention by users [8]. Privacy in CBDC can also be defined as the degree to which a user's CBDC balance or holdings and transactions data are hidden from CBDC participants, which include payer's and payee's bank or other payment service provider (PSP), government institutions, the general public and other PSPs [9]. Additionally, it is important to note that providing access to digital financial services (in this case, a CBDC) in the absence of government oversight risks facilitating criminal activities such as the financing of

illegal activities like terrorism, tax evasion and other related regulatory violations. This signifies the fact that anti money laundering (AML), combating the financing of terrorism (CFT), anti-tax avoidance (ATA) measures and other related law enforcement requirements will have higher priority and importance over users' privacy and data protection as can be seen in Figure 1 [5]. Consequently, it has been argued that CBDCs should be implemented to provide some form of privacy instead of cash-like privacy so as to satisfy AML, CFT, ATA, and the respective privacy and data protection laws and regulations [9]. As an example, the digital Yuan, eCNY has implemented five levels of privacy in which privacy is tied to balance, transfer and activity limits, with two of the levels not requiring a user's identity but rather just the user's email address or a phone number [10]. Furthermore, as a result of countries' differences in contexts and CBDC issuance purposes, different privacy preservation approaches have been applied by the countries in their respective CBDC (such as the eNaira, the eCedi and the Sand dollar) designs [5], [6], [7]. In summary, this emphasizes that privacy preservation in CBDCs is challenging as opposed to the case in physical fiat currencies (i.e., cash), and that CBDC design should not be treated and implemented as a generic solution, thereby making country-specific CBDC designs inevitable.

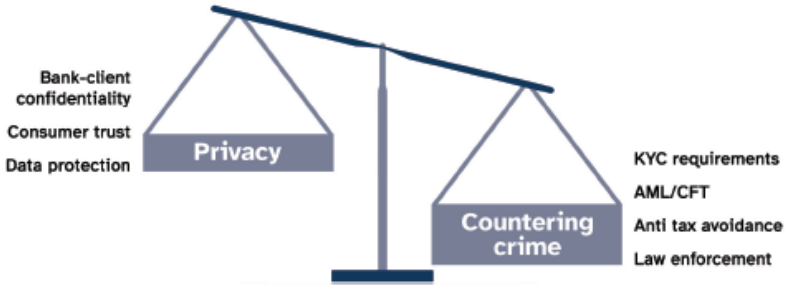

Fig 1. Balancing user financial privacy preservation and measures against crime [5]

2 Material

Privacy preservation concerns in CBDCs have been worked on to varying degrees by various stakeholders in academia and industry as will be outlined in this section. In summary, most of the explorations have been general or specific to certain countries thereby making them unsuitable for Tanzania's specific context considering the differences among countries' contexts and CBDC issuance purposes. This eventually makes it necessary to explore the available relevant CBDC work in existing literature and propose a privacy preserving CBDC design suitable specifically for Tanzania's context.

Literature has shown that CBDC implementations differ among countries due to their differences in contexts and CBDC issuance purposes, among other factors, which should be taken into consideration to ensure successful CDBC projects. Context includes a country's existing payment and technological infrastructure, which if well-developed and efficient will ease CBDC implementation as opposed to if it is less developed, and the country's financial capacity which if strong the more favorable contrasting to if it is weak. Context also includes the socio-economic status of a country's citizens who are the expected CBDC users, whose levels of access to smartphones and the Internet are crucial to CBDC adoption success, among other factors. On the other hand, the CBDC issuance purpose includes one or more of the CBDC issuance benefits [1], [2]. The purposes include improving monetary policy conduct thereby enhancing the CB's control over money demand and supply situation, improving digital payment systems' efficiency by making them faster and more accessible, and lowering transaction fees especially for small value payments. Other purposes include increasing financial inclusion thereby making financial services more accessible to citizens that lack access to traditional banking services, and countering the impact of private digital currencies (i.e., cryptocurrencies) like BTC and ETH. Furthermore, cryptocurrencies are decentralized therefore beyond government's control and are attractive to some users hence posing risks such as price volatility and use for illegal activities [2], [11]. Apart from such factors, privacy preservation features of a CBDC are crucial as cash-like privacy is among the features desired by the expected CBDC users and other stakeholders. Privacy is important as similar to the use of cash in which it is hard to track the spending habits of a user, the use of a digital currency risks the exposure of a user's spending habits, hence making it inevitable to have appropriate private preservation measures in place. Furthermore, existing literature has also shown how challenging it is to preserve users' privacy in CBDCs considering the regulatory requirements for AML, CFT, ATA, and the respective country's privacy and data protection laws and regulations [2], [4], [11].

Existing literature has also shown that several considerations have to be made in the design of a privacy preserving CBDC. The considerations include the choice of the CBDC operational model or architecture, and the CBDC infrastructure as can be

seen in Figure 2, the CBDC approach or model and the use of design principles. CBDC operational models or architectures include the one-tier architecture in which the CB does the user facing operations, and the two-tier architecture in which the intermediaries (such as other banks and other PSPs) handle the user facing operations as can be seen in Figure 3. The CBDC infrastructure refers to the modality used for transactions' data recording which include the use of a centralized database, a decentralized ledger or a no ledger system. The CBDC approach or model has two categories, the account-based CBDC which is more centralized, secure and easy to track, making it regulatory compliance compatible, and the token-based CBDC which is more decentralized, relatively less secure and difficult to track, making regulatory compliance incompatible. Moreover, the use of design principles refers to the use of principles such as the Privacy by Design (PbD) principle. An additional consideration is the choice of appropriate technologies and protocols to implement the CBDC design, which includes the choice and use of privacy preserving technologies and ledger technologies, among others [3], [4], [6].

In the initiatives to create a privacy preserving CBDC several initiatives have been made by various countries. The CBDC projects outlined in the subsequent parts of this section provide an overview of the related works from existing literature which include CBDCs by the Chinese, Bahamian, Ghanaian and Nigerian CBs.

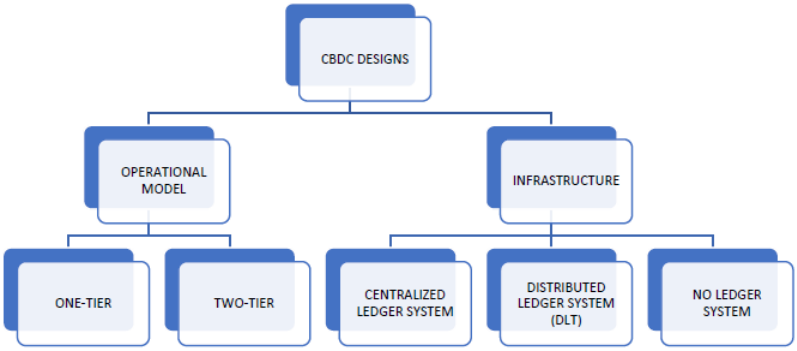

Fig 2. CBDC design: Operational models (i.e., architectures) and infrastructures [4]

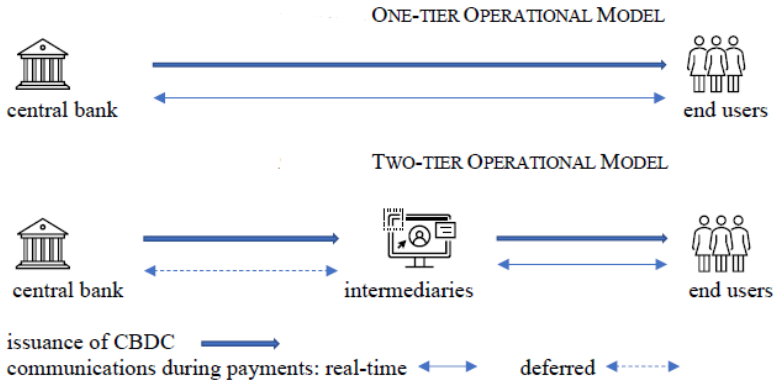

Fig 3. CBDC architecture [4]

The Chinese CBDC (i.e., the eCNY) is one of the earliest CBDCs to be launched. The eCNY uses the two-tier architecture in which the CB issues CBDC and the intermediaries distribute it to users as can be seen in Figure 4. It also uses the centralized database infrastructure to keep track of the CBDC transactions, meanwhile using controlled anonymity in which the stakeholders (such as the CB, other banks, other intermediaries and third parties) have limited CBDC users' information. The controlled anonymity is implemented by separating the CBDC users' identity information (which is stored by the telecommunication companies) from other stakeholders (which store only the necessary and required CBDC transaction data). This implies that these stakeholders cannot fully identify the CBDC users. For instance, the CB only has users' phone numbers as the users' identity information whereas more such information like the names and addresses are held by the telecommunication companies, collected during users' registration with these respective companies. Additionally, eCNY is account-based, making it relatively more secure and easier to track the transactions, and is loosely coupled with users' bank accounts, implying that

the country's visitors and the unbanked citizens can open an eCNY wallet without having a bank account so as to access basic eCNY features[5],[12]. Nevertheless, literature appears to lack substantial details on eCNY design, particularly technological specifications. However, despite the eCNY implementation appearing successful in China, its design might not necessarily be suitable for Tanzania, considering the two countries' differences in contexts and CBDC issuance purposes.

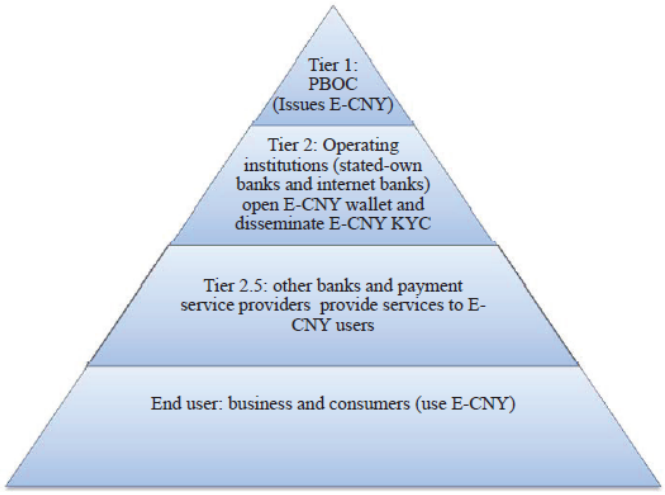

Fig 4. eCNY architecture[5]

The Bahamian CBDC (i.e., the Sand dollar) was the first nationwide deployed CBDC launched in October 2020. Its design consists of the two-tier architecture and a distributed ledger technology (DLT) infrastructure. Also, the Sand dollar design ensures that transactions are not anonymous meanwhile protecting users' confidentiality, and includes an AML/CFT engine owned by the CB of Bahamas. The engine is used by the intermediaries to screen the CBDC transactions for AML/CFT compliance as can be seen in Figure 5. Furthermore, the CBDC has multi factor authentication and data encryption on the eWallet, and rigorous cyber security assessment of the CBDC system (which includes the CB, intermediaries, eWallets and apps). On the other hand, it also comprises a Know-Your-Customer (KYC) database which is owned by the CB and used by the intermediaries[5] [7]. Nevertheless, this KYC database handling approach appears to risk users' privacy compromise as it creates the possibility of public surveillance and data abuse by the CB and the government of Bahamas. Considering the unique context of Bahamas and its CBDC issuance purposes, the Sand dollar design appears to be suitable for Bahamas and therefore cannot be suitable for Tanzania. Consequently, it is necessary to propose a privacy preserving CBDC design suitable specifically for Tanzania.

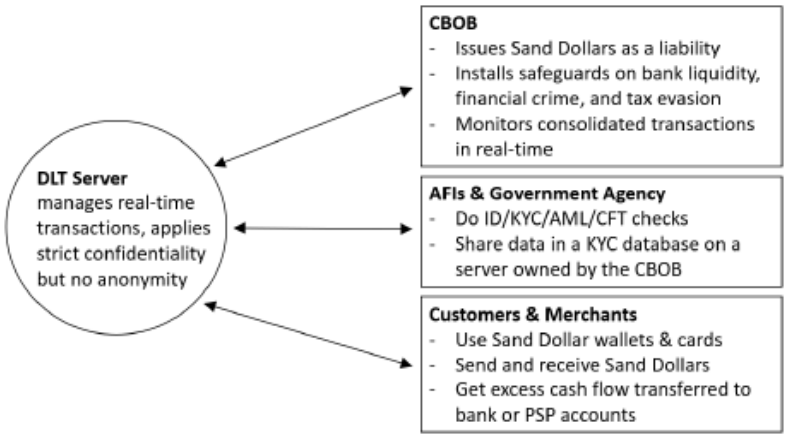

Fig 5. The Sand dollar operations[5]

In Africa, Ghana's token-based CBDC (i.e., the eCedi) was piloted in 2022 but has not been launched. The eCedi was designed to have a two-tier architecture and aims to ensure user privacy and AML/CFT compliance according to the country's privacy and data protection laws and regulations as can be seen in Figure 6. Additionally, the intermediaries will be responsible to monitor transactions for AML/CFT violations and report them to respective authorities, and the country has an AML Act that provides a framework for an optimal AML compliance meanwhile creating a balance with users' privacy preservation. Though the eCedi appears promising, the technology design details and the outline of its actors' interactions are lacking. In summary, the eCedi monitoring and reporting approach is aimed at promoting financial inclusion and users' privacy preservation, among other goals[7],[9]. On the other hand, in October 2021 Nigeria launched an account-based CBDC (i.e., the eNaira) with a two-tier architecture (as can be seen in Figure 7) and a distributed ledger technology (DLT) infrastructure. The used DLT is the hyperledger fabric which is a customizable and permissioned blockchain platform with robust security architecture, developed by the Linux foundation. Furthermore, the eNaira's design chose the account-based CBDC approach so as to facilitate compliance for AML/CFT through the intermediaries (as they directly interface with the users) thereby ensuring the integrity of the CBDC. To protect privacy, the eNaira design made a balance in which it ensures a certain degree of users' privacy preservation meanwhile ensuring compliance with AML/CFT according to the country's AML/CFT guidelines, privacy and data protection laws and regulations[1],[6],[13]. In summary, the Ghanaian and Nigerian CBDC designs among other factors took into consideration the respective countries' contexts and CBDC issuance purposes thereby necessitating the proposal of a privacy preserving CBDC design suitable specifically for Tanzania.

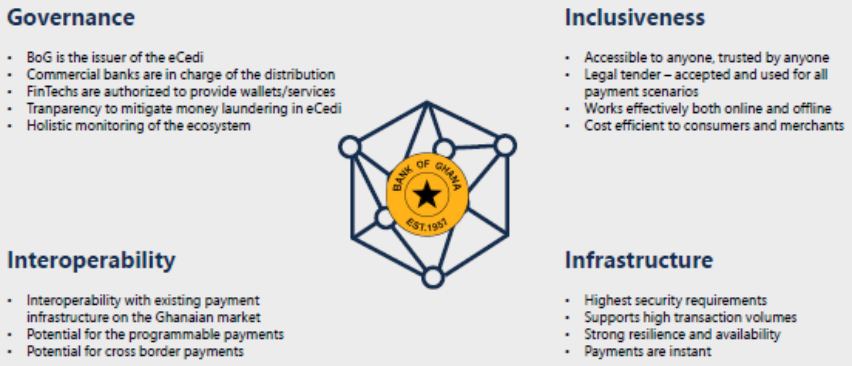

Fig 6. Design of the eCedi[7]

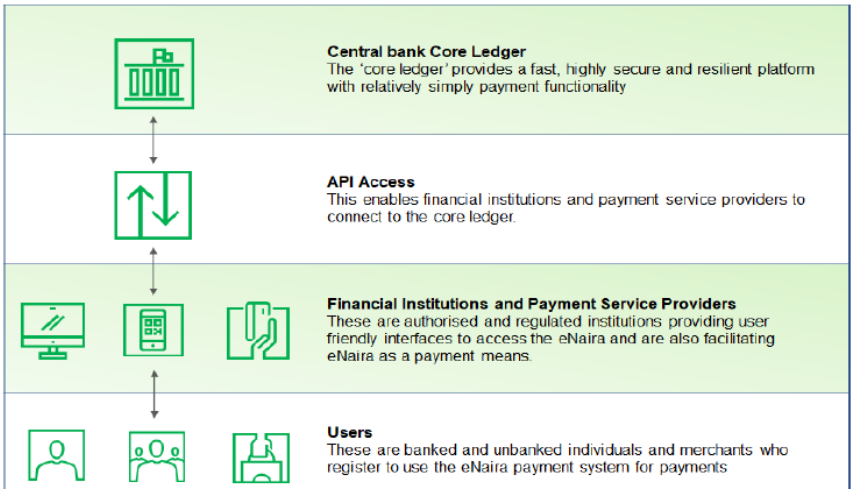

Fig 7. Architecture of the eNaira[6]

Drawing from existing literature, it is evident that each reviewed country has a different specific CBDC design further emphasizing the fact that a CBDC design should not be treated as a universal solution. Furthermore, the eCNY, Sand dollar,

eNaira and the eCedi designs among other factors took into consideration the respective countries' contexts and CBDC issuance purposes. Additionally, Tanzania's context is different from the contexts of all the reviewed countries, and Tanzania's purposes for CBDC issuance might also differ from theirs. The contextual differences include differences in levels of technological development, financial capacity, cultural preferences and regulatory environments, whereas purposes for CBDC issuance can be to benefit from one or more of the CBDC issuance advantages. Consequently, it is inevitable to consider Tanzania's context when proposing the design of the country's CDBC, specifically a privacy preserving CBDC design.

3 Method, Results and Discussion

Considering the goal of this work, the Design Science Research (DSR) methodology was used to propose the design of a privacy preserving CBDC suitable specifically for Tanzania's context. Considering that Tanzania's CB, the Bank of Tanzania (BoT) is in its CBDC research phase, apart from other CBDC stakeholders, the BoT can significantly benefit from this work[14]. The DSR methodology was selected as it emphasizes the creation and evaluation of artifacts ensuring that they are effective, usable and contributing to knowledge, an emphasis which properly fits the goal of this work[15]. The DSR process has six steps, which are problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation and communication; with four entry points which can be seen in the DSR process model as shown in Figure 8[15].

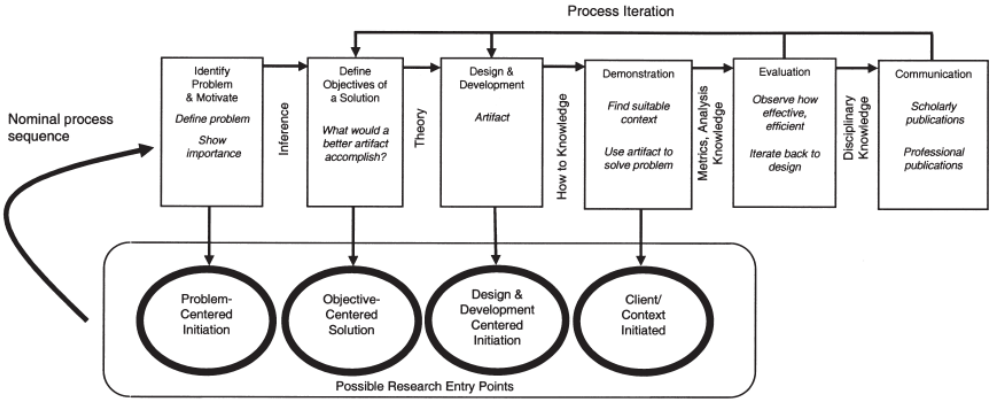

Fig 8. DSR methodology process model[15]

Findings/Results: It is worth noting that when comparing the contexts of Tanzania with those of the studied developing countries such as Nigeria, Ghana and Bahamas, Tanzania's payment and technological infrastructure is less developed, its financial capacity is weaker, and its citizen's socio-economic status is lower compared to those countries[1],[2]. Consequently, based on the DSR methodology's steps, a privacy preserving CBDC design suitable specifically for Tanzania's context was eventually proposed, demonstrated and evaluated, and the results are as further described in the subsequent subsections.

3.1 Step 1: Problem identification and motivation

Through literature review of related CBDC research and development work, including that conducted by countries like China, Bahamas, Ghana and Nigeria, around the world, the absence of a privacy preserving CBDC design suitable specifically for Tanzania was identified as the problem. Furthermore, the challenging trade-offs between the need for users' privacy preservation and the requirements for AML/CFT compliance also contributed to the problem identification. Also, the solution to the problem is expected to increase the likelihood of a successful adoption of the resulting CBDC. Consequently, this will enable the practical realization of the associated CBDC adoption benefits which include increasing financial inclusion, improving monetary policy conduct, lowering transaction charges and enhancing efficiency in digital payment systems. Additionally, this work chose the problem-centered entry approach as literature has shown that privacy in CBDC solutions is one of the major concerns that significantly determine the success or failure of a given CBDC project[15],[16],[17].

3.2 Step 2: Objective for a solution

As existing literature has shown that privacy is one of the major concerns raised by CBDC stakeholders, the objective for a solution was to propose a privacy preserving CBDC design suitable specifically for Tanzania's context. The proposed design aims

to addresses users' privacy preservation requirements meanwhile managing privacy's challenging trade-offs with AML/CFT compliance requirements. This is expected to facilitate a smooth adoption of the CBDC that might be issued by the BoT consequently increasing its success probability, and hence the practical realization of the associated CBDC benefits in Tanzania.

3.3 Step 3: Design and development

This section presents a proposal of a privacy preserving CBDC design suitable specifically for Tanzania's context. Based on the designs created by other researchers, CBs, other stakeholders, and the reviewed privacy preservation technologies and protocols, a suitable design is produced under the consideration of a number of relevant factors including architecture, infrastructure and CBDC approach. This is further outlined in the subsequent parts of this subsection with the resulting proposed privacy preserving CBDC design as shown in Figure 9.

3.3.1 Architecture

The two-tier CBDC architecture is the one that appears suitable for Tanzania's context as it is supported by the currently existing digital payment systems environment. This is supported by the fact that using the one-tier architecture will require BoT to perform all the customer facing operations such as KYC, AML, CFT and handling of deposits and withdrawals. This will require BoT to have a larger and sufficient number of branches and employees to perform the said operations. This will also result into bank disintermediation and might potentially negatively impact BoT's efficiency in overseeing its current main responsibilities such as monetary policy, payments and settlement systems, currency and financial sector supervision[18]. On the other hand, in the two-tier architecture the BoT will be responsible for CBDC issuance to the intermediaries (i.e., banks and other PSPs). The intermediaries (apart from performing operations like KYC, AML, CFT, handling of deposits and withdrawals) will be responsible for distributing the CBDC to the customers (via their mobile money wallets and bank accounts) who can then use the same to make payments[1],[2] as can be seen in Figures 3 and 9.

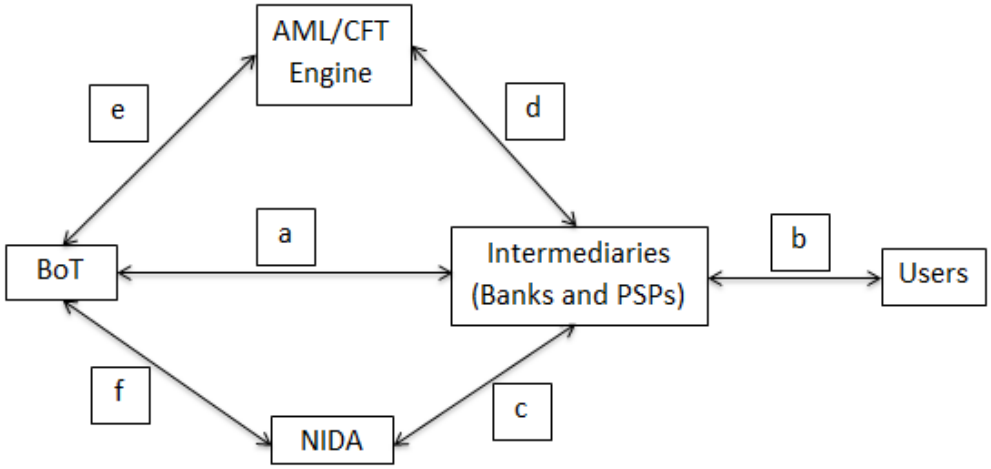

Fig 9. The proposed privacy preserving CBDC design suitable specifically for Tanzania's context

Key:

- a: BoT issues CBDC to the intermediaries (i.e., banks and other PSPs).
- b: The intermediaries distribute CBDC to the users, who will use web and mobile applications to perform transactions in their interactions with the intermediaries.
- c: Intermediaries interact with NIDA as they perform KYC during the registration of their customers (i.e., users).
- d: As the users perform transactions, the intermediaries interact with the AML/CFT engine to detect any AML/CFT violations in the transactions.
- e: The BoT interacts with the AML/CFT engine to obtain the list of blocked transactions.
- f: The BoT can interact with NIDA to obtain the identity data of the parties involved in the blocked transactions for further appropriate processing.

3.3.2 Infrastructure

Considering the need for privacy, the pros and cons of the available infrastructure options (i.e., centralized database, distributed ledger, and no ledger systems), the distributed ledger appears to be the suitable CBDC infrastructure for Tanzania. The suitable distributed ledger option appears to be the permissioned distributed ledger, known as the hyperledger fabric. This ledger is also used by Nigeria's CB and is under consideration for use in CBDCs by other countries like Malaysia, Singapore, Thailand, Canada, France and Hong Kong. This option (i.e., the hyperledger fabric) has a number of benefits, such as scalability, customizability, transparency, interoperability and reliability (as a DLT eliminates the single point of failure vulnerability). Despite such benefits, the option has a number of challenges that include cost, the technology's complexity and skills requirement (as it is a complex and new technology to Tanzania). On the other hand, the centralized database option is scalable and familiar (making it relatively cheaper and easier to implement) while it also reduces transparency and security as it creates a single point of failure thereby risking privacy compromise [(1),(2),(6)]. Additionally, as a permissioned blockchain (i.e., only authorized participants can join it, hence it is not open to the public), the hyperledger fabric increases security and preserves CBDC users' privacy by the use of private transactions and zero knowledge proofs (ZKP). A private transaction is the one in which only the sender, receiver and authorized nodes can see a transaction's details (thereby hiding transaction details from the public and the unauthorized parties) while ZKP allow users to prove that they possess certain information (such as in identity verification) without revealing the information [(1),(2)]. Conclusively, as the goal is privacy preservation in the CBDC, the DLT (in this case the hyperledger fabric) appears to be the suitable option as Tanzania's CBDC infrastructure.

3.3.3 Central bank digital currency approach

The account-based CDBC appears to be the one suitable for Tanzania as it resembles the current banking system except that it will use a digital version of the Tanzanian Shilling (TZS) instead of cash. Through this approach BoT and associated stakeholders will benefit from the account-based CBDC features which include traceability and stability thereby making provision for KYC, AML, CFT and ATA. This is unlike the token-based CBDC approach where it is difficult to track transactions, is subject to instability due to speculations and volatility, and eliminates the intermediaries. In summary, the token-based CBDC approach will make it challenging for KYC, AML, CFT and ATA [(1),(2)].

3.3.4 User identification, privacy and data protection laws and regulations

As an initiative for easy identification of CBDC users, the National Identification Numbers (NIN) as provided by Tanzania's National Identification Authority (NIDA), can be used. Nevertheless, to prevent the risk of public surveillance and data abuse by the government, relevant privacy and data protection laws and regulations should be in place to restrict access to the data handled by NIDA, the BoT and the intermediaries (banks and other PSPs). These will provide user privacy and data protection guidelines for the parties involved in the Tanzanian CBDC ecosystem thereby ensuring users' privacy preservation. This is similar to what has been done in Nigeria, Ghana and China [(5),(6),(7),(12)]. Additionally, an AML/CFT engine will be required to screen the CBDC transactions for AML/CFT compliance, somehow similar to the Sand dollar implementation [(5)]. Additionally, the engine can use artificial intelligence (AI) to classify each transaction as either normal or suspicious. Furthermore, a transaction classified as suspicious is expected to raise an alert which is to be reviewed by a human who will confirm or block the transaction and submit the blocked transactions to the respective authorities for further procedures and investigations [(19),(20)].

3.4 Step 4: Demonstration

User privacy is preserved in the proposed CBDC design through the use of the proposed options described in subsection 3.3 as will also further be described in this section. The use of the two-tier architecture and the hyperledger fabric infrastructure ensures that only authorized participants join the blockchain network. Furthermore, the use of private transactions ensures that only the sender, receiver and authorized nodes have access to a transaction's data, and the use of ZKP ensures that verification can be done with the users without the users revealing the actual information. Also, the use of the account-based CBDC approach facilitates AML/CFT compliance and raises the level of security thereby contributing to user privacy preservation. Additionally, the enacting of the necessary privacy, and data protection laws and regulations will make user privacy protection a legal requirement for the involved CBDC participants. Consequently, since the users' identification data will be handled by NIDA, and the transactions' data will be handled by the BoT and intermediaries, access to such data by the relevant AML and CFT authorities will only occur in instances of associated alerts (via the AML/CFT detection engine) and with reasonable evidence of AML/CFT violations. This will preserve users' privacy and avoid the risk of public surveillance and data abuse by the Tanzanian government.

3.5 Step 5: Evaluation

As the objective was to propose a privacy preserving CBDC design suitable specifically for Tanzania's context, the proposed design promises to address the said objective. This is evaluated through identification of the parties that will have access to the CBDC data and the reasons for which they access the data thereby providing a means to determine the extent to which privacy will be preserved by the design [(4)]. Privacy is preserved as user identity data is handled only by NIDA and is shared with the intermediaries and BoT only in KYC operations and legal investigations to obtain further information of parties involved in suspected violations (as detected by the AML/CFT engine), respectively. Also, through the use of private transactions only the sender, receiver and authorized nodes can view the transaction data thereby contributing to users' privacy preservation. Furthermore, through the use of ZKP the CBDC users will be able to provide necessary proof without the need to reveal the details of the information for which they provide proof, thereby also contributing to users' privacy preservation. Additionally, through the use of the permissioned blockchain (i.e., the hyperledger fabric), only the authorized nodes can participate in the blockchain network thereby restricting access to the transactions' data and consequently contributing to users' privacy preservation. Conclusively, this CBDC design promises to preserve users' privacy for the Tanzanian context.

It is also worth noting that this work stems from the fact that the existing literature lacks a privacy preserving CBDC design suitable specifically for the Tanzanian context. Furthermore, considering the proposed design's presentation, demonstration and evaluation and acknowledging that CBDC privacy is one of the most demanded features by users (with reference to cash's features), the design presents an insightful finding and a contribution to the body of knowledge. Consequently, this aims to contribute towards the practical realization of CBDC benefits in Tanzania, such as enhancing financial inclusion, lowering transaction fees (especially for low-valued transactions) and improving the efficiency of digital financial systems. On the other hand, the CBDC designs of Tanzania, Nigeria and Bahamas are similar in architecture and infrastructure (i.e., all use two-tier and DLT respectively). Furthermore, the designs of Tanzania and Nigeria are also similar in approach (i.e., both use account-based) whereas that of Ghana is token-based but uses the two-tier architecture. Nevertheless, the proposed CBDC design has several limitations, especially considering its specificity to the Tanzanian context. This implies that the findings are mainly applicable to the Tanzanian context and cannot be generalized for other countries' contexts without some sort of customization. Additionally, the proposed design has not considered the Tanzanian existing relevant regulatory and legal frameworks and challenges, and has not been implemented and tested in a real world setting, thereby limiting its demonstration and evaluation in a production environment. The design also lacks the inclusion of interdisciplinary perspectives and considerations for user adoption and acceptance. These consequently suggest future research to cover such CBDC design aspects to contribute to the body of knowledge.

3.6 Step 6: Communication

As a user's spending habits have the potential to reveal the user's interests, wealth and health among other things, which are directly linked to the user's privacy, implementing measures to protect the user's privacy in a country's CBDC is inevitable. Furthermore, existing literature has shown that failure to preserve CBDC users' privacy or at least ensure a certain level of privacy (as it might be impossible to provide exactly cash like privacy) will risk the adoption success of the CBDC. This will consequently risk the practical realization of the associated CBDC benefits. As a result this work, proposed a privacy preserving CBDC design suitable specifically for Tanzania's context, thereby increasing the success probability of the potential Tanzanian CBDC. Consequently, this will increase the chances for the practical realization of the associated CBDC project benefits in Tanzania. Such benefits include increasing financial inclusion, lowering transaction charges, improving monetary policy conduct and enhancing efficiency in digital payment systems. Conclusively, the authors' findings are as communicated through this work.

4 Conclusion

Since literature has shown that different countries have different contexts and CBDC issuance purposes thereby requiring them to have specific CBDC designs, it is also inevitable for Tanzania to have a specific CBDC design, in this case for users' privacy preservation. Consequently, this work proposed a privacy preserving CBDC design suitable specifically for Tanzania's context, thereby promising database privacy for the potential Tanzanian CBDC. Furthermore, given the fact that, AML/CFT requirements outweigh those of users' privacy preservation, there had to be a certain level of balance to ensure that the two concerns are addressed simultaneously. This also required the design to include an AML/CFT detection engine for analyzing every CBDC transaction for signs of AML/CFT violations. Additionally, the use of private transactions, ZKP, a permissioned blockchain and the enacting of relevant and supportive privacy and data protection laws and regulations will be necessary to

eventually provide CBDC user privacy preservation. Nevertheless, further or future research work needs to be done, including the development and evaluation of the proposed design, as well as its adoption and acceptance by the users. Furthermore, future work includes CBDC development considering the existing relevant regulatory and legal frameworks and challenges in Tanzania, the inclusion of interdisciplinary perspectives, and research on other factors impacting the success of CBDC projects.

References

1) Google's Bard, Various relevant questions. 2023. Available from: https://bard.google.com/.
2) OpenAI' ChatGPT, Various relevant questions. 2023. Available from: https://chat.openai.com/.
3) Auer R, Bohme R, Clarke J, Demirag D. Mapping the Privacy Landscape for Central Bank Digital Currencies: Now is the time to shape what future payment flows will reveal about you. *Queue*. 2022;20(4):16–38. Available from: https://doi.org/10.1145/3561796.
4) Jiang J. Privacy Implications of Central Bank Digital Currencies. Seton Hall University School of Law. 2023. Available from: https://scholarship.law.ufl.edu/facultypub/1222/.
5) Chen J, Nesterov IO. Central bank digital currencies: Digital Yuan and its role in Chinese digital economy development. *RUDN Journal of Economics*. 2023;31(1):120–133. Available from: https://journals.rudn.ru/economics/article/view/34247/21951.
6) eNaira Design. 2021. Available from: https://enaira.gov.ng/design-paper/.
7) Design Paper of the Digital Cedi (eCedi). 2022. Available from: https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf.
8) Auer R, Bohme R. The Technology of Retail Central Bank Digital Currency. 2020. Available from: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm.
9) Darbha S, Arora R. Staff Analytical Note 2020-9. 2020. Available from: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/.
10) Privacy and CBDCs - DEA Working Group Paper. 2023. Available from: https://blog.digital-euro-association.de/privacy-and-cbdcs-dea-working-group.
11) Mng'ong'ose W. Digital Currencies and the Challenges for Central Banks: Case of Tanzania. Bank of Tanzania Academy. 2022. Available from: https://academy.bot.go.tz/wp-content/uploads/filr/1890/DIGITAL%20CURRENCIES%20PRESENTATION.pdf.
12) Wang H. How to Understand China's Approach to Central Bank Digital Currency? *Computer Law & Security Review*. 2023;50:105788. Available from: https://doi.org/10.1016/j.clsr.2022.105788.
13) Mnyawi R, Kombe C, Sam A, Nyambo D. Blockchain-based Data Storage Security Architecture for e- Health Care Systems: A Case of Government of Tanzania Hospital Management Information System". *International Journal of Computer Science and Network Security*. 2022;22(3):364–374. Available from: http://dx.doi.org/10.22937/IJCSNS.2022.22.3.46.
14) Public Notice: Bank of Tanzania (BoT) Progress on Central Bank Digital Currency. 2023. Available from: https://www.bot.go.tz/Adverts/PressRelease/en/2023011413181519.pdf.
15) vom Brocke J, Hevner A, Maedche A. Introduction to Design Science Research. In: Design Science Research. Cases. Progress in IS;Springer, Cham. 2020;p. 1–13. Available from: https://doi.org/10.1007/978-3-030-46781-4_1.
16) Eurosystem report on the public consultation on a digital euro. 2021. Available from: https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf.
17) Alberola E, Mattei I. Central bank digital currencies in Africa. 2022. Available from: https://www.bis.org/publ/bppdf/bispap128.pdf.
18) Core Functions, Bank of Tanzania (BoT). 2023. Available from: https://www.bot.go.tz/.
19) Alhajeri R, Alhashem A. Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management*. 2023;15(04):284–305. Available from: https://doi.org/10.4236/iim.2023.154014.
20) Pavlidis G. Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*. 2023;26(7):155–166. Available from: https://www.emerald.com/insight/content/doi/10.1108/JMLC-03-2023-0050/full/html.