Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute InformingScience.org

IJIKM.org

Volume 16, 2021

ESTABLISHING A SECURITY CONTROL FRAMEWORK FOR BLOCKCHAIN TECHNOLOGY

Maitha Al Ketbi	Dept. of Information Systems and Security, UAE University, Al Ain, UAE	201101198@uaeu.ac.ae
Khaled Shuaib*	Dept. of Information Systems and Security, UAE University, Al Ain, UAE	k.shuaib@uaeu.ac.ae
Ezedin Barka	Dept. of Information Systems and Security, UAE University, Al Ain, UAE	ebarka@uaeu.ac.ae
Marton Gergely	Dept. of Information Systems and Security, UAE University, Al Ain, UAE	mgergely@uaeu.ac.ae

* Corresponding author

ABSTRACT

Aim/Purpose	The aim of this paper is to propose a new information security controls framework for blockchain technology, which is currently absent from the National and International Information Security Standards.
Background	Blockchain technology is a secure and relatively new technology of distributed digital ledgers, which is based on inter-linked blocks of transactions, providing great benefits such as decentralization, transparency, immutability, and automation. There is a rapid growth in the adoption of blockchain technology in different solutions and applications and within different industries throughout the world, such as finance, supply chain, digital identity, energy, healthcare, real estate, and the government sector.
Methodology	Risk assessment and treatments were performed on five blockchain use cases to determine their associated risks with respect to security controls.
Contribution	The significance of the proposed security controls is manifested in complementing the frameworks that were already established by the International and National Information Security Standards in order to keep pace with the emerging blockchain technology and prevent/reduce its associated information security risks.

Accepting Editor Ewa Wanda Ziemba | Received: February 7, 2021 | Revised: May 17, June 10, June 24, July 15, July 19, 2021 | Accepted: July 20, 2021.
Cite as: Al Ketbi, M., Shuaib, K., Barka, E., & Gergely, M. (2021). Establishing a security control framework for blockchain technology. *Interdisciplinary Journal of Information, Knowledge, and Management*, *16,* 307-330.
https://doi.org/10.28945/4837

Findings	The analysis results showed that the proposed security controls herein can mitigate relevant information security risks in blockchain-based solutions and applications and, consequently, protect information and assets from unauthorized disclosure, modification, and destruction.
Recommendations for Practitioners	The performed risk assessment on the blockchain use cases herein demonstrates that blockchain can involve security risks that require the establishment of certain measures in order to avoid them. As such, practitioners should not blindly assume that through the use of blockchain all security threats are mitigated.
Recommendations for Researchers	The results from our study show that some security risks not covered by existing Standards can be mitigated and reduced when applying our proposed security controls. In addition, researchers should further justify the need for such additional controls and encourage the standardization bodies to incorporate them in their future editions.
Impact on Society	Similar to any other emerging technology, blockchain has several drawbacks that, in turn, could have negative impacts on society (e.g., individuals, entities and/or countries). This is mainly due to the lack of a solid national and international standards for managing and mitigating risks associated with such technology.
Future Research	The majority of the blockchain use cases in this study are publicly published papers. Therefore, one limitation of this study is the lack of technical details about these respective solutions, resulting in the inability to perform a comprehensive risk identification properly. Hence, this area will be expanded upon in our future work. In addition, covering other standardization bodies in the area of distributed ledger in blockchain technology would also prove fruitful, along with respective future design of relevant security architectures.
Keywords	blockchain technology, standards, security controls, information security, security governance

INTRODUCTION

Blockchain technology is considered as the fastest growing Distributed Ledger Technology (DLT). Its applications have been adopted rapidly in fields such as finance, supply chain, digital identity, energy, healthcare, real estate, and the government sector. This rapid adoption is due to its expected great benefits in terms of achieving decentralization, transparency, immutability, and automation environment. There is a good number of published research papers proposing the adoption of blockchain technology in different industries, e.g., in supply chain (Liu & Li, 2020; Manupati et al., 2020; Wang, Wang, et al., 2020), in healthcare (Fu et al., 2020; Wang, Luo, & Zhou., 2020; Yazdinejad et al., 2020), and in energy (Samuel et al., 2020; Van Leeuwen et al., 2020). However, blockchain technology involves many risks and threats that require serious attention from both governance and management perspectives, which unfortunately is lacking. Thus, one of the main problems related to the adoption of blockchains and distributed ledger technologies is the lack of solid governance needed for such technologies (Drljevic et al., 2020; Otto, 2019).

Currently, there is a shortage of standards related to governing these technologies and their associated applications, and such standards are essential if to better achieve the intended benefits, and thus maintain a strategy of long-term survival and adoption of these technologies. In order to maintain and ensure the scalability, interoperability, flexibility, and governance of the blockchain technology, a set of relevant standards should be developed. There are several organizations throughout the world

responsible for developing standards in general, such as (but not limited to) the following: International Organization for Standardization (ISO), ITU Telecommunication Standardization Sector (ITU-T), IEEE Standards Association, and World Wide Web Consortium (W3C). Standards-developing organizations (SDOs) realize the lack of standardization in relevance to the blockchains technology and its implications. Thus, they understand the importance and the need for creating relevant standards, which requires the contribution of SDOs and the involvement of subject matter experts globally (Lima, 2019).

Therefore, a consensus on developing common sets of relevant standards properly while ensuring to cover different aspects of the technology is needed. Our proposed standards aim to cover various aspects, which include definitions, implementation, management, cyber security, and core attributes (including data). However, one major drawback in the development of standards is that it requires relatively a long time to be released. As of today, most of the planned relevant standards are currently under development. Therefore, this work aims to address the issue of the lack of governing information security risks related to blockchain technology implementation by establishing new related information security controls that have not yet been covered by National and International Information Security Standards, such as the ISO 27001:2013 Standard and the UAE Information Assurance Standards managed by the UAE Signals Intelligence Agency. Consequently, when adopted, this will ensure that information and information assets are protected against possible unauthorized disclosure, modification, and destruction, which could have a negative impact on individuals, entities and/or national levels.

The rest of the paper is organized as follows. In the following section, we review related literature for previous research. The third section introduces new security controls and shows how these controls are established and complement the existing ones. In the fourth section, risk analysis and mitigations are discussed along with an introduction of the use cases. The fifth section provides analysis and discussions of applying security controls in the use cases. In the penultimate section, we provide guidelines for evaluating these security controls, and end with concluding remarks.

LITERATURE REVIEW

The literature review conducted for this work was exploratory. First, databases accessible through the UAE University Library (such as IEEE Xplore, Sage, Elsevier, and Springer) were used to find relevant publications initially, by searching on key words such as "blockchain standards", "blockchain security controls", "blockchain security risks", and "blockchain security governance". Additionally, Google Scholar was used to find publications that were not found in other major databases. Furthermore, the technique of reverse snowballing was utilized to find any missing articles. Based on the literature search, a lack of research in the area of security governance of the blockchain technology in terms of developing blockchain standards and/or establishing relevant security controls was determined. As Drljevic et al. (2020) clearly mentioned, the research landscape around this topic is still in its early stage.

Dagher et al. (2018) proposed a framework called "Ancile", which is an Ethereum-based blockchain framework focused on meeting the need of legislative standards specifically related to protecting patient privacy. For example, it enforces compliance with the Health Insurance Portability and Accountability Act (HIPPA) requirements via managing and controlling access to the Electronic Health Record (EHR) of patients through the encryption and authentication mechanisms of blockchain technologies, thus preserving the privacy of their sensitive information. However, not all information is concealed completely; hence, the level of concealment depends on the implementation. This is usually achieved through the use of smart contracts as well as via tracking the usage of the medical records, secure transfer of medical records, and prevention of unauthorized access of Protected Health Information (PHI). Therefore, preservation of patient privacy and security in compliance with regulations and interoperability guidelines needs to be carefully considered.

Lima (2019) highlights a methodology to develop a framework related to DLT standards through three steps in an iterative process. The first step of this top-down approach is to define an initial reference model in order to create a system of subsystems, identifying the key components (subsystem) of the technology, which include stakeholders, concerns, and architectural viewpoints. The second step is to identify industrial use cases and map with the created model. Lastly, the created model is revised, refined, iterated, and improved.

Moreover, Lima (2019) classifies DLT/blockchain standards into four categories based on the following criteria: the viewpoints, level of depth, boundaries, demarcation points, and the industrial collaboration for each part in the system (including the subsystems) of the technology. The first category, called "Generic Framework Standards", is considered as a starting point of developing standards for all new technologies and as a foundation of the subsequent standards categories. It focuses on Reference Guide, Reference Frameworks, Architectures, Terminologies, Interfaces, Ontology, Classification, and so forth. This type of standards can involve an iterative approach of refining and validating the preliminary assumptions of an initial model through use cases. The working groups and committees developing this type of standards are IEEE DLT/blockchain standards, ISO/TC 307 on blockchain and distributed ledger technologies, and ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT).

The second category, called "Enabling Technology Standards", is mainly focused on technology related mechanisms including but not limited to the following: Client Interfaces, Identity Management, Data Formats, Consensus Algorithm, Token Specifications. Standards of this type are created by institutions such as the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C), the Enterprise Ethereum Alliance (EEA), and the International Telecommunication Union (ITU). The third category, called "Platform-Specific Standards", is relevant to the previous type of Enabling Technology Standards. However, it is platform-based and focuses on a higher level of systemic view. Well-known examples of implementation include Ethereum, Hyper ledger, and Corda. This category of standards also covers cloud-based solutions known as Blockchain-as-a-Service (BaaS). Popular examples include IBM, Microsoft, Amazon, and VMWare.

The final category, called "Vertical-Industry-Specific Standards", is mainly an establishment of specific industrial use cases based on the Generic Framework Standards. It focuses on blockchain implementations in areas such as energy, health care, manufacturing, supply-chain, logistics, and transportations. The success of its creation highly depends on the required involvement, knowledge, and expertise of each industry. Furthermore, Lima (2019) proposes a high level of Blockchain Architecture Framework using ISO/IEC/IEEE 42010 "Systems and software engineering – Architecture description" as a reference model through applying three steps: creating a system-of-systems model in line with this selected reference model, identifying the key components of stakeholders, concerns, architectural viewpoints and systems of interest and finally mapping and refining the created model to the selected industrial use cases. The implementation type of this model is considered as part of the Generic Framework Standards.

Flood and McCullagh (2020) discuss three key areas of concern that should be covered while developing the standards; namely, blockchain governance, smart contracts, and interoperability between and across blockchains.

Blockchain governance includes the following aspects: standards, data, cryptographic key security, and smart contracts. Failures related to blockchain governance may have a negative impact on the advancement of the distributed ledger technology. Examples include failures of the used consensus algorithms such as forking of Bitcoin and Bitcoin Cash, as well as Ether and Ether classic. In term of data governance, it is crucial to ensure data confidentiality and privacy within the desired blockchain architecture. In addition, complying with relevant standards such as the European Union's General Data Protection Rules (GDPR), through ensuring that no Personal Identifiable Information (PII) is

stored on the blockchain itself, is a must. PII should only be stored off-chain in a separate data repository accessible securely through the utilized blockchain environment. In the case of using permissioned blockchains, a common standard for data management and governance should be agreed upon by all members. Another aspect that has been discussed is the security of used encryption keys. This focuses on the protection of the used private keys through implementing of certificated and crack-proof hardware wallets or offline hardware security modules as per relevant standards, such as the US Government FIPS 140-3 (National Institute of Standards and Technology, 2019).

Smart contracts written in the format of software codes are considered a binding law by the blockchain communities; however, it might not be the case from a legal perspective. Another issue to be considered in the deployment of smart contracts is inter-blockchain communication and interoperability.

Interoperability across blockchains is defined in terms of cross-chain interoperability and enterprise system integration while taking into consideration data access and storage, including off-chain. This includes smart contracts interoperability issues, cross-chain, and sidechains, which might have an impact on the outcome and performance of blockchain implementation. Another aspect is the establishment of secure and trusted interactions between cross-chains, including value transfer, using different possible solutions such as Common Inter-Chain Messaging Protocol (CICMP), and Anonymous Multi-Hop Locks (AMHL) (Belchior et al., 2020). As for sidechain interoperability, the main concern of cross-chain interoperability is to enable movement of digital tokens across different blockchains securely.

CohnReznick (2018) states that organizations should identify and understand risks involved when deploying a blockchain/DLT technology. It highlights six high-level risks that might have a negative effect on the implementation and adoption of blockchain technology as part of existing operations and systems of an organization. The identified risks are scalability, technology implementation and acquisition, data security and confidentiality, regulatory hurdles, jurisdiction, and storage limitation. Therefore, in order to mitigate risks associated with the deployment of a blockchain-based solution and ensure data security, confidentiality, privacy, and accountability, an effective risk management strategy should be established, implemented, and monitored properly. This is in addition to enhancing related information technology controls for information security policies, physical security, key management and cryptography controls, computer operations, and logical access controls. Furthermore, CohnReznick highlights six key blockchain areas that an organization has to focus on, along with their involved risks and controls, in order to achieve a secure blockchain environment. These key areas are platforms, nodes, software developments, users, security incidents, and asset management. In addition, other aspects, such as data conversion and legacy systems integration, should be considered. Organizations should perform the required analysis on existing platforms, such as web servers, outsourced database applications, and Identity and Access Management (IAM) solutions. This is to ensure readability through blockchain/DLT interfaces, proper transformation and data loading, and accurate and complete integration with existing systems. In terms of key management for logical access, organizations should implement Public Key Infrastructure (PKI) based solutions effectively in order to protect and maintain the security of users' access keys, both public and private, to the ledger files or interfaces. In addition, organizations that use public-permissioned (also known as "hybrid-permissioned") blockchains need to take into consideration proper management and effective protection of the integrity of used consensus algorithms. Lastly, access considerations for the physical security of hardware-based tokens used for storing private keys, such as physical badges, PIV/CIV cards, and biometric authentication mechanisms, are to be investigated.

However, both Flood and McCullagh (2020) and CohnReznick (2018) do not provide a comprehensive and detailed overview of information security controls related to blockchain technologies in terms of the number of security controls covered. The studies also lack detailed information on how to protect information security and manage involved risks in such technologies.

Gramoli and Staples (2018) proposed a high-level description of the three main elements – consensus, security, and ownership – to be covered by a blockchain-based functional architecture. The description of the consensus element focused on the importance of global agreement on the block publication process and its content. In addition, the description of the security element highlighted the important of preventing malicious individuals from tampering and taking over asset ownership of a user. Finally, the description of the ownership element focused on the tracking of asset ownership through the respective addresses or accounts. In terms of different transaction models across various blockchain applications, they highlighted the legal aspects of smart contracts and token programming languages. The study also highlighted the lack of common terminology with respect to blockchain technologies which is currently under consideration and development by the concerned technical committees of the International Organization for Standardization (ISO). The terminology being considered includes the following terms: Blockchain, Clients and Servers, Consensus and Pseudonymity.

With respect to standards, Uriarte and De Nicola (2018) reviewed existing standards in relation to decentralized cloud solutions in order to maintain and improve compatibility between various relevant projects. They briefly described decentralized clouds requirements, including service definition, smart contracts for Quality of service (QoS), execution flow, management of components, data elements, data privacy, federated clouds, and distributed ledgers. The ongoing initiatives by the international Standards Developing Organizations (SDOs) were highlighted.

Howard and Vachino (2020) evaluated four major blockchain platforms in term of their compliance with the National Institute of Standards and Technology (NIST) cryptographic standards as per the Federal Information Security Management Act of 2002 (FISMA) requirements. The following three criteria applicable to blockchain projects were considered: (1) management and support by a single entity; (2) allowing independent private chains instead of having a single global network; and finally (3) support by libraries which allow easy access to data and protocols related to blockchain technologies.

König et al. (2020) selected a set of published blockchain standards to analyze by comparison according to some document and content criteria. The standards developed by the following organizations were included in their comparative analysis: National Institute of Standards and Technology (NIST), ANSI Accredited Standards Committee X9, International Organization for Standardization (ISO), German Institute for Standardization (DIN), The European Union Agency for Cybersecurity (ENISA), German Federal Office for Information Security (BSI), International Telecommunication Union (ITU) and European Committee for Electrotechnical Standardization (CENELEC). The results of analysis showed that ENISA provided best practices to overcome existing cybersecurity and legal problems in the financial and banking sector. Further, most of the developed standards for blockchains are focused on the overview of the technology itself, including concepts, functionality, and usage, but neither on the guidance for compliance nor on the various economic sectors and specific industries. It is also shown that there is a lack of coverage on how integration of blockchains into existing information security management systems can lead to associated risks, e.g., the concern of privacy in public blockchains. Although introducing relevant standards for newly adopted technologies is generally in slow paces and takes time, there is an urgency for the blockchain technology. Ensuring security and privacy by building on current frameworks and defining relevant laws is highly recommended. This is especially so in regard to the distributed systems standards where incorporating related new sections could serve as a useful reference for the distributed ledger technologies.

Dagher et al. (2018) proposed a blockchain-based framework of patient privacy protection in line with regulatory standards, a regulation called HIPPA. Lima (2019) also proposed a high-level Blockchain Architecture Framework in line with ISO/IEC/IEEE 42010 "Systems and software engineering Architecture description", which falls under the category of Generic Framework Standards. However, the validation and evaluation process of the proposed framework was not included in

Lima's work. Furthermore, both of these studies do not evaluate their effectiveness in terms of information security. In addition, they did not look into how to prevent or mitigate relevant information security risks.

Our work aims to cover limitations of the aforementioned studies by establishing new information security controls specifically related to the blockchain technology that has not been covered by the International and National Information Security Standards; namely, ISO 27001 and UAE IA Standards.

ESTABLISHING BLOCKCHAIN SECURITY CONTROLS

The new information security controls for the blockchain technology are based on the understanding of the technology itself as well as its involved risks, threats, weaknesses, and vulnerabilities in term of information security. The structure of these security controls follows the control structure of ISO 27002, as both ISO27001 and UAE IA Standards – selected to fill the control gaps regarding this technology – are of the same structure in term of control details and descriptions. Therefore, the adopted control structure includes: control statement, implementation guidance of control requirements in detail, and provisions of further information to cover any legal, regulatory, and other considerations if applicable and/or available. Figure 1 shows the components of security controls related to the blockchain technology, including the newly established ones.

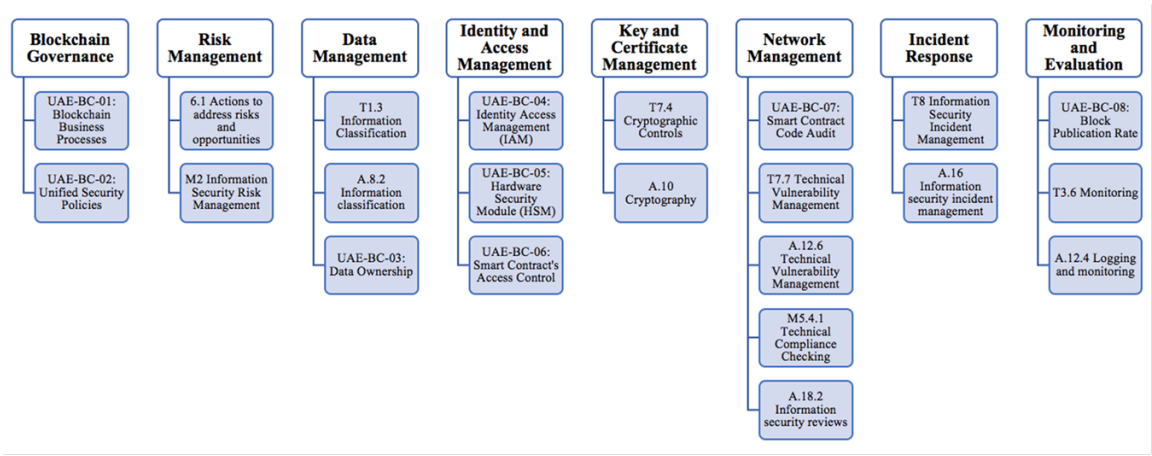

Figure 1. Blockchain security controls and their sub controls (newly proposed are those starting with UAE-BC, others are from the ISO 27001 and UAE IA standards)

PROPOSED BLOCKCHAIN SECURITY CONTROLS

In this section, we introduce the proposed blockchain security controls in detail, which is needed to fill the relevant gap in the two existing standards considered, ISO 27001 and UAE IA. These standards were chosen since they are considered the most comprehensive standards, specifically in term of information security management and governance. The implementation of the proposed controls depends on the desired blockchain type. For example, the proposed security controls, UAE-BC-04 and UAE-BC-02, are specific to permissioned blockchain solutions.

UAE-BC-01: Blockchain Business Processes

Objective: To provide clear and comprehensive vision in relation to the business processes and procedures of blockchain-based services and its use cases in order to maintain a proper business workflow and overall security.

Control: The entity shall define and establish a business process and/or procedure in relation to the blockchain solution and its use cases.

Implementation guidance: The defined process and/or procedure should be aligned with the respective operation model and should include, but not limited to, the following considerations:

- Determining the type of the blockchain-based service, address space and cryptographic functions in use.
- The signing and/or verifying mechanisms of transactions, for example the consensus model in use.
- The mechanism of publishing and adding new blocks on the network including, but not limited to, the average block publishing time and relevant incentives (if applicable).
- Determining the block component, with the maximum size of the block, transaction and data taken into consideration.
- Identifying all participating entities and their roles within the blockchain-based service in case of a permissioned blockchain.
- Establishing secure development processes and/or procedures in relation to the smart contracts, including but not limited to: defining the relevant business requirements and scope of work, using the relevant pre-approved tools and software, and reviewing and testing the code on regular basis and prior to any deployment.

UAE-BC-02: Unified Security Policies

Objective: To ensure and maintain the consistency between all participated entities on the respective blockchain platform through implementing and following unified security policies related to designing, developing, and using the respective platform.

Control: All participating entities on the permissioned blockchain shall define, document, implement, agree, and follow unified security policies in relation to blockchain-based services.

Implementation guidance:

- All entities should agree on the relevant security policies, standards, and best practices to follow and comply with in relation to blockchains.
- The unified security policies shall include, but not limited to, Access Control Policy, Cryptography Policy, Network and Communication Security Policy.
- Establish and maintain the relevant documentations such as, processes, procedures, templates, records, plans, logs and/or guidelines.
- The unified security policies shall be communicated to all users of the participating entities on the blockchain platform.
- The unified security policies shall be reviewed at planned intervals, or in case a significant change occurs, on the relevant blockchain-based service and accordingly they shall be updated and approved by all participating entities.

Other information: Generally, information on security policies-based security control has been mentioned by the International and National Information Security Standards, such as the relevant security control number A.5 in ISO/IEC 27001 and M1.2 in UAE Information Assurance Standards.

UAE-BC-03: Data Ownership

Objective: To define the data type to be stored on the respective blockchain platform taking into consideration applicable national and international laws and regulations. In addition, to define the data ownership and the respective roles and responsibilities for handling the relevant data securely.

Control: All entities shall establish and agree on a process to define the data type to be stored on the blockchain along with the data owner's responsibilities.

Implementation guidance:

- Define the respective roles and responsibilities in relation to the data over the blockchain-based service.
- Establish and maintain the relevant documentations on data handling process, including but not limited to, the following considerations:
  i) The data should be secured during creation, receipt, storage, processing, transmission, disposal and other applicable functions.
  ii) Define the data type taking into consideration personal data types as defined by established international standards/regulations such as the General Data Protection Regulation (GDPR) and ISO/IEC 27001.
  iii) Encrypt the data stored on the blockchain using a strong encryption algorithm approved by international and national authorities.
  iv) Verify if the data is correct as required by the defined data type, encoding and/or encryption mechanisms.
  v) Access criteria on how the data record and/or individual fields of the data record can be retrieved and decrypted.
  vi) Control the flow of information within the blockchain and between interconnected systems and provide the respective authorizations based on specified service access requirements.
  vii) The relevant documentations for processes and procedures should include, templates, records, plans, audit logs and/or guidelines.

UAE-BC-04: Identity Access Management (IAM)

Objective: To identify, authenticate and authorize individuals properly and securely in order to ensure that the proper user has the appropriate access to the respective blockchain platform and its components based on defined processes and procedures specific to the blockchain-based service and solution.

Control: The entity shall define, design, plan, and implement an Identity Access Management (IAM) solution for the permissioned blockchain-based service in line with the users' on-boarding and off-boarding processes.

Implementation guidance:

- Define the roles and responsibilities of the identity and service providers to accordingly grant the respective permissions and/or privileges.
- Maintain and update the list of the identity and service providers regularly.
- Define and establish users' on-boarding and off-boarding processes including the relevant authentication, verification, and authorization mechanisms.
- Assign, reassign, validate and/or remove privileges of users as per the business needs.
- Define and establish the blockchain-based service access process and/or procedures in line with the relevant Access Control Policy; including access means, such as remote access, wireless access and/or through mobile devices.
- Establish and maintain the relevant documentations for processes and procedures such as template, records, plans, audit logs and/or guidelines.
- The blockchain-based service access should cover at least the following privileges in line with the least privilege principle:
  i) Read access to the blockchain.
  ii) Publish new transactions on the blockchain.
  iii) The relevant account/identity is created, approved, enabled, modified, disabled and removed as per Access Control Policy in relation to the blockchain.
  iv) Access control can further be restricted to users' identity or credential to provide content privacy of transactions.

v) Periodically review the relevant account/identity along with its granted/assigned permissions/privileges and any access audits logs/reports.
vi) Continuous monitoring, oversighting and auditing users' access to the blockchain-based service.
vii) In case of any access violations and/or malicious transaction, generate an incident report in line with the approved Information Security Incident Management Policy.

Other information: Generally, access control-based security control has been mentioned by the International and National Information Security Standards, such as the relevant security control number A.9 in ISO/IEC 27001 and T5 in UAE Information Assurance Standards.

UAE-BC-05: Hardware Security Module (HSM)

Objective: To store, manage and maintain users' private keys securely within the Hardware Security Module (HSM) integrated into the respective blockchain platform in order to ensure its integrity, authenticity and availability.

Control: All entities shall establish and agree on the architecture and procedure for the Hardware Security Module (HSM) implementation for securing the blockchain identity keys.

Implementation guidance:

- Conduct risk assessment on the HSM implementation over the proposed blockchain architecture.
- Define and establish an HSM partition process for storing keys along with the respective separated admin rights and roles for each participating entity, such as crypto officers, crypto users and super admins.
- Establish and maintain the relevant documentations for processes and procedures such as templates, records, plans, audit logs and/or guidelines.
- Access to the keys should be enabled only through a secure manner.

Other information: Generally, user credentials-based security control has been mentioned on the International and National Information Security Standards, such as the relevant security control number A9.2.4 in ISO/IEC 27001 and T5.2.3 in UAE Information Assurance Standards.

UAE-BC-06: Smart Contract's Access Control

Objective: To ensure that the smart contracts codes are accessed in a proper and secure manner during their lifecycles as per predefined privileges to respective users. In addition, to ensure that access to smart contracts codes is logged and monitored continuously in order to prevent any malicious activities.

Control: Access to smart contracts lifecycles management should be defined, controlled, logged and monitored on a continuous basis, including the relevant processes and/or applications that any smart contract will be collaborating with.

Implementation guidance:

- Define users' roles and responsibilities in regard to accessing smart contracts along with predefined and approved access control lists.
- Ensure segregation of duties.
- Establish a process/procedure for defining, controlling and monitoring access to smart contracts through their lifecycles including other interactions with relevant processes and/or applications.
- Establish and maintain the relevant documentations for processes and procedures such as templates, records, plans, logs and/or guidelines.
- Use cryptographic solutions such as the Trusted Platform Modules (TPMs) for sensitive code execution.

- Clarify payments and time lists for the execution-smart contracts of given blockchain services to prevent denial of service attacks on the publishing nodes (e.g., full system resource consumption).
- In case of any access violations and/or malicious transactions, release the incident report in line with the approved Information Security Incident Management Policy.

Other information: Generally, access control-based security control has been mentioned by the International and National Information Security Standards, such as the relevant security control number A.9 in ISO/IEC 27001 and T5 in UAE Information Assurance Standards.

UAE-BC-07: Smart Contract Code Audit

Objective: To ensure that smart contracts codes are tested and audited prior any deployment to avoid security vulnerabilities, bugs and flaws and thus prevent any malicious activities that could compromise the security of the respective blockchain platform.

Control: The entity shall establish a process for testing, analyzing and auditing smart contracts codes by an independent outsourced specialized party.

Implementation guidance:

- Establish and maintain documentations for relevant processes and procedures such as templates, records, plans, logs and/or guidelines.
- The need to comprehend business logic of smart contracts to validate compliance with the service need.
- The smart contracts should be tested and audited against legal considerations, security vulnerabilities, bugs and flaws by an independent party.
- The smart contracts should be analyzed using, for example, Expert code Analysis, Control Flow Analysis, Dynamic Code Analysis, Manual Code Analysis, Vulnerability-based Analysis, Taint Analysis, Symbolic Execution and Improper Error Handling.
- The smart contracts outcome reports relevant to testing, auditing and analysis along with the respective approvals from the processes' owners should be published by the blockchain-based service.
- Ensure that the smart contracts executions are not relying on predefined timestamps for determining whether or not to take an action such as making a payment in order to avoid malicious activities resulting from propagation delays, and synchronization errors.

Other information: Generally, information system audit-based security control has been mentioned by the International and National Information Security Standards, such as the relevant security control number A.12.7 in ISO/IEC 27001 and M5.5 in UAE Information Assurance Standards.

UAE-BC-08: Block Publication Rate

Objective: To ensure and maintain the overall security of the respective blockchain platform and prevent any malicious activities intended to compromise the block production process. This should be conducted through proper testing, monitoring and evaluation techniques.

Control: The entity shall establish a process and/or procedure for testing, monitoring and evaluating the publication rate of a block and accordingly adjust influencing factors of the respective rate if required.

Implementation guidance: The defined process and/or procedure should include, but not limited to, the following considerations:

- Agreement on the block validation process of the blockchain-based service. This determines the selection criteria of the validators.
- Mechanism of how new blocks are published to all nodes.

- Details on mathematical calculation adjustments to match changes in computational capacity of the blockchain network to meet a specified average time for successful mining of a single block in case of permissionless blockchains.
- Regular testing and monitoring the effectiveness of the block publication rate against malicious activities as per the established plans.
- Adjust the block publication rate according to the outcomes of the relevant testing, monitoring and evaluation reports along with respective approvals from the processes owners.
- Establish and maintain the relevant documentations for respective processes and procedures such as templates, records, plans, logs and/or guidelines.

Other information: The General Data Protection Regulation (GDPR) is a data protection and privacy law in the European Union. Since the data stored on the blockchain is immutable, therefore ensuring that the stored data type is not of personal information is required in order to comply with the GDPR in addition to ISO/IEC 27001 which is an international standard focused on information security and the management of its associated risks through the Information Security Management System (ISMS) framework.

Risk Assessment and Mitigation

In order to determine the appropriate security controls, Risk Assessment and Risk Treatment have been performed on five blockchain use cases. This was done to determine their involved risks with their respective security controls as per ISO 31000:2018 – Risk Management (International Organization for Standardization, 2018), which provides a generic risk assessment approach that can be implemented/applied to all types of risks. Their relevant applications focused on electronic medical records, student digital documents and energy and financial services. The impact and probability criteria have been defined along with relevant definitions and descriptions as shown in Tables 1 and 2. Accordingly, a risk matrix was established, as shown in Figure 2, along with the relevant risk rating definitions and descriptions, as shown in Table 3. The risk acceptance criterion was excluded as it is specific to every organization's management decision which is out of scope of this work.

Risk Assessments and Treatments have been performed on the chosen blockchain use cases as per the following:

Risk Assessments

Risk Assessments consists of Risk Identification, Risk Analysis and Risk Evaluation.

- *Risk Identification*
  The involved risks, threats and vulnerabilities of the blockchain use cases (along with their services, systems, etc.) were identified with respect to information security through different techniques and methods including, interviewing owners and respective people related to blockchain use cases and reviewing the relevant documents. Therefore, a comprehensive list of the identified risks has been prepared, as part of this stage.

- *Risk Analysis*
  The identified risks were analyzed by first identifying their sources and their potential incident scenarios, along with determining the probability, as well as the impact for each incident scenario based on the established probability criteria and impact criteria sequentially. The risk value for each incident scenarios is calculated by multiplying the determined probability value by the determined impact value.

- *Risk Evaluation*
  The determined and calculated risk value on the Risk Analysis is considered as an input for Risk Evaluation. The risk value of the established risk matrix is based on the corresponding determined probability value and the determined impact value of each incident scenario.

Table 1. Impact levels description

Impact Level	Definition
Very High	The threat event could be expected to have multiple severe or catastrophic adverse impact on the organization's people, process, and/or technology, or the nation.
High	The threat event could be expected to have a severe or catastrophic adverse impact on the organization's people, process, and/or technology, or the nation.
Medium	The threat event could be expected to have a serious adverse impact on the organization's people, process, and/or technology.
Low	The threat event could be expected to have a limited adverse impact on the organization's people, process, and/or technology.

Table 2. Probability levels description

Probability Level	Definition
Very High	A threat event is almost certain to occur or occurs more than 100 times a year.
High	A threat event is highly likely to occur or occurs between 1-100 times a year.
Medium	A threat event is moderately likely to occur or occurs between 1-10 times a year.
Low	A threat event is unlikely to occur or occurs less than once a year.

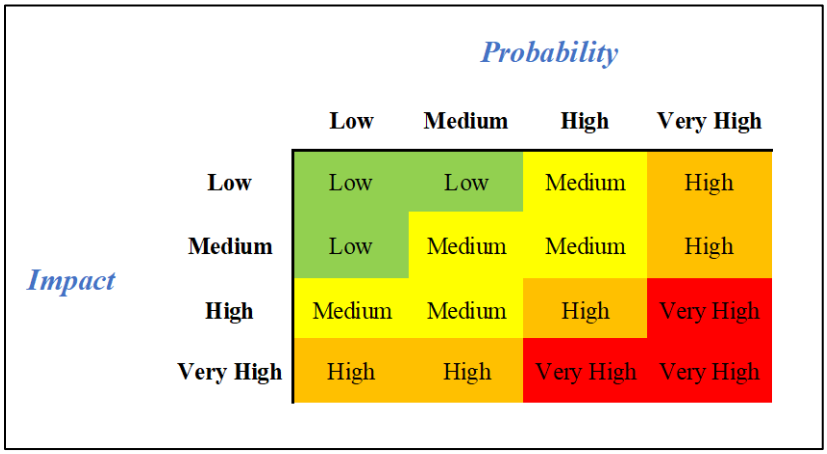

Figure 2. Risk matrix

Table 3. Risk rating description

Risk Rating	Definition
Very High	If a risk is rated as "Very High", there is an immediate requirement for mitigation actions. The affected information asset should be assessed for possible impact and a risk mitigation action must be planned, agreed upon, and implemented before continuing its operation, within the agreed upon period of time.
High	If a risk is rated as "High", there is an urgent requirement for mitigation actions. The affected information asset may continue to operate with compensating controls, but a risk mitigation action must be planned, agreed upon, and implemented, within the agreed upon period of time.
Medium	If a risk is rated as "Medium", a mitigation action is required, and a plan must be developed to incorporate these actions and implemented within an agreed upon period of time.
Low	If a risk is rated as "Low", then the organization may decide to implement a mitigation action or to accept the risk.

Risk Treatment
Risk Treatments are performed to treat the identified risks. Generally, there are four options for treating risks which are:

- *Risk Reduction*
  Mitigating the risks through applying the appropriate security controls.
- *Risk Retention/Acceptance*
  Accepting the risks that falls within the defined risk acceptance level.
- *Risk Avoidance*
  Avoiding the tasks and/or activities that cause a risk.
- *Risk Transfer*
  Transferring the risk to another party.

As per the aim of this research, the primary option in this stage is Risk Reduction. Accordingly, the appropriate security controls have been selected from UAE IA Standard's controls, ISO 27001 Standard's controls and the proposed security controls. The Risk Avoidance option has not been used since there is no particular process or activity to avoid. Regarding the remaining options, the Risk Retention/Acceptance and Risk Transfer, they are dependent on the risk owner and/or organization management decision therefore they are out of the cope of this work.

Blockchain Use Cases

In this section, we briefly discuss five use cases used for our risk analysis, which contains technical details about the implemented solutions. Information on four of these cases are publicly available while one was obtained under a non-disclosure agreement with the owner kept confidential.

Use Case#1 – MedRec – MIT

Since patients could be moving between different health care service providers, their data becomes scattered. Each provider keeps its patients' electronic health records under its supervision, which can lead to patients not being able to view their health information and reports, correct any data entry errors, and distribute their information across other health care providers. Therefore, MedRec is a proposed solution that aims to solve these issues through eliminating centralization and providing transparent access to electronic health records by using a blockchain technology. Moreover, it is a distributed system that provides access and validation features to patients' electronic health records from different providers. It is a private Ethereum based blockchain platform. It does not store patients' records on the MedRec blockchain platform; rather, it uses smart contracts to encode the data of the relevant records locations and provide links to the actual records stored off chain. These records can be retrieved by using database like queries and thus can be accessed securely by the respective patients and the different healthcare providers who are participants of the MedRec blockchain network. In addition, relationships between patients and the respective health care providers are added using the smart contracts including predefined permissions. More detailed information about MedRec can be found by examining the technical document (MedRec, 2018).

Use Case#2 – Energy Web

The decentralization property of the blockchain technology has encouraged and improved utility investments in renewable energy generation, transmission, and distribution. The Energy Web Decentralized Operating System (EW-DOS) aims to use the decentralized digital technologies to accelerate the global transition to a low carbon energy future life style and decrease the carbon footprint of organizations and individuals. EW-DOS is a public based blockchain network for energy trading and tracking between customers, service providers, retailers and grid operators. Thus, anyone/entity can

access the network, deploy a smart contract, and build, develop, and utilize any application on the respective network through paying a token (Energy Web Token "EWT") for the relevant services and/or transactions being performed. It implements a Proof of Authority (PoA) based consensus model. A "transaction relay server" is used for ensuring that all transactions are mined and are error free. A self-sovereign decentralized digital identity (DIDs) with a multi-signature wallet is used to provide the user control over any personal information usage and management. EW-DOS categorizes nodes into two types: one is a validator node, and the other is a utility node. In the case where an organization is hosting both node types, then the organization is required to configure a specific container "Docker images" on its respective hosts. Application Programming Interfaces (APIs) are used for interacting and transferring data between the organization's blockchain platform and other external components and/or platforms. More detailed information about this solution can be found in the technical document (EnergyWeb, 2020).

Use Case#3 – Power Ledger

Power Ledger is a renewable energy trading platform that uses blockchain technologies to facilitate financial settlements and reconciliation of energy transactions between participating parties in a timely fashion within specified time intervals during which the traded energy is produced and consumed without the need for a central authority. It is a hybrid public and consortium based blockchain platform and it supports a number of energy trading applications. Smart contracts are used to govern any performed transactions. Native tokens, called POWER token, are mainly used for facilitating and providing access permissions to participants of the respective platforms. The utility company is responsible for managing and on-boarding participants on its blockchain platform using an application host, while APIs are used for gathering and exchanging required information between external components and the blockchain layers of the public and consortium blockchain platforms. This mechanism is called "EcoChain" and uses Proof of Stake (PoS) for a consensus model. State channels are used to handle high frequency energy transaction settlements in an off-chain manner. High level technical details and more general information about this blockchain implementation can be found by examining their paper (Power Ledger, 2019).

Use Case#4 – Confidential

This case describes a digital wallet that holds university students' and alumni electronic academic records on a private blockchain platform. It was developed as part of a wider smart digital transformation initiative of the university. It enables all students and alumni to manage and share their academic records in a secure, efficient, and flexible manner with internal and external entities who are part of the configured blockchain network. For example, it enables the respective users to request, manage, and share their documents with the other entities when applying for jobs. In addition, participating entities can verify the provided documents through the respective blockchain platform. It is fully integrated with the existing IT systems owned and managed by respective organization.

Use Case#5 – Provenance

Global financial markets invest billions of dollars yearly in financial services, such as audits, trustees and reconciliation, and administration services. However, these markets are suffering from limited liquidity, significant friction, and lack of transparency. Therefore, Provenance uses a blockchain technology in order to reduce the relevant costs and risk, improve liquidity, and open new financial markets. This is achieved through providing effective financial services via registering and exchanging financial assets across markets, such as the loan origination and securitization. Provenance implements a public but permissioned based blockchain platform using Proof of Stake (PoS) as a consensus model. Smart contracts are used to govern any performed transactions between entities. A native digital token, called Hash, is used as part of the implementation. Members are categorized into four types: administrators, regular members, banks, and stakeholders. An administrator is responsible for allocating permissions for other members, monitoring performed activities, approving and setting

stakes, writing, and reviewing smart contracts. More general information about this implementation can be found in their paper (Provenance Blockchain, Inc, 2020).

ANALYSIS AND DISCUSSION

The performed risk assessment on the relevant blockchain use cases shows that, like any other emerging technology, beside its benefits, the blockchain technology can have associated security risks that require specific actions to mitigate for effective implementations and deployments. Figure 3 shows the associated risks with the relevant use cases categorized as per the risk rating levels. The majority of the identified associated risks were rated as Medium and High. This indicates that there are moderate to high risks that should be governed and dealt with properly to reduce possible implications. To achieve that, it is necessary to apply appropriate security controls including the proposed ones in this work.

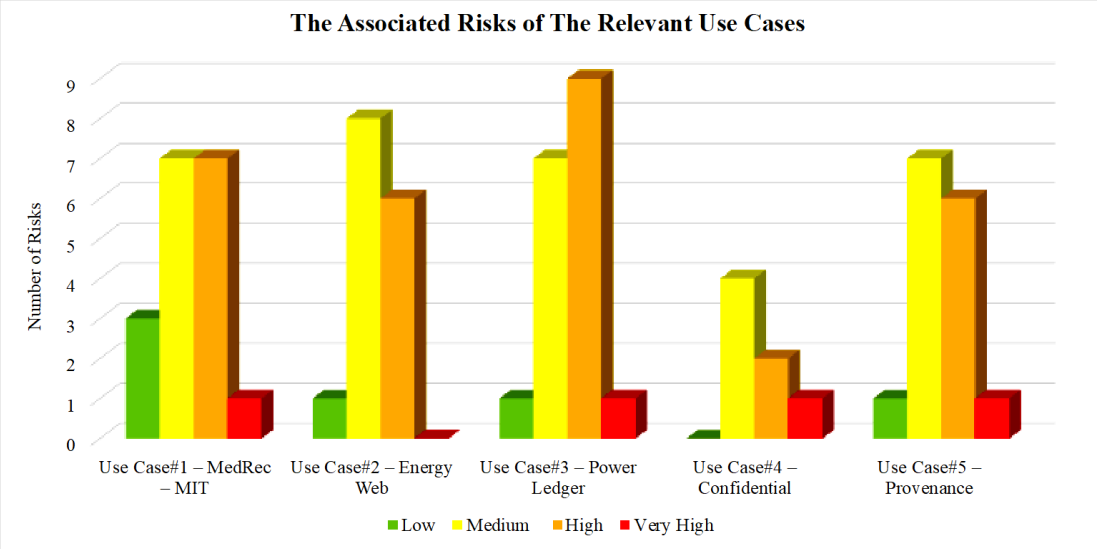

Figure 3. Associated risks of blockchain use cases (categorized by risk rating)

Given that all discussed use cases are based on implementing blockchain as technology, it is logical to assume that common risks are evident to be shared between them. Risks that are identified as shared between at least three use cases are listed below. These risks should be considered while designing, developing, and implementing blockchain based solutions.

- Lack of enforcement for strong security access controls on the users and providers nodes to prevent unauthorized access to the respective private keys.
- No mechanisms are specified to protect the integrity and availability of the nodes private keys.
- No mechanisms are specified for the revocation of nodes.
- Lack of security for endpoints/nodes, utilized relevant applications and software from possible security threats and vulnerabilities.
- Untested and unaudited smart contracts for security threats and vulnerabilities prior to deployments.
- Lack of access control mechanisms to prevent any unauthorized access to smart contracts.
- Unspecified requirements for secure communication over the used platform and its components.
- No incident reporting procedures are specified.

- Unclear vision with respect to data security and confidentiality including, but not limited to, block payloads, transmitted data, and data at rest.
- Unclear vision on the data type to be stored on the respective platform.
- Absence of a business continuity strategy for the respective platform.
- Lack of details on the security of the used cryptographic algorithms against security flaws and vulnerabilities.
- Lack of protection against possible malicious activities of administrators.
- Lack of details on whether the required security assessments against relevant security threats and vulnerabilities have been performed on the respective platforms, utilized applications, and services before any deployments.
- Unclear vision on the intra-platform data flow and on data flows with other linked external platforms and applications.

Table 4 shows the most relevant security controls considered consistently from ISO27001, UAE IA and the proposed ones. Generally, Table 5 shows the consolidated list of associated risks, from the discussed blockchain use cases, and the security controls that can be considered for the mitigation of such risks prior implementing any blockchain solutions.

As per the performed risk assessment and treatment on the relevant blockchain use cases, it was shown that there are risks that could be mitigated and reduced through the proposed security controls. The proposed security controls are needed due to the lack of blockchain specific security controls in the aforementioned International and National Information Security Standards.

Table 4. Most repeated security controls for risk reduction

Most Repeated Security Controls on the Performed Risk Treatment		
ISO27001 Security Controls	**UAE IA Security Controls**	**The proposed security controls**
A.9 Access control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
A.12.6 Technical Vulnerability Management	T7.7 Technical Vulnerability Management	UAE-BC-07: Smart Contract Code Audit
A.18.2 Information security reviews	M5.4.1 Technical Compliance Checking	UAE-BC-03: Data Ownership
A.10 Cryptography	T7.4 Cryptographic Controls	
	T5.2.3 User Security Credentials Management	

Table 5. Consolidated list of associated risks and their security controls

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	**UAE IA Standard Controls**	**Proposed Controls**
R-01	Lack of enforcement for strong security access controls on the users and providers nodes to prevent unauthorized access to the respective private keys.	- User Credentials - Respective platform and its components	A.9 Access control	T5 Access Control	UAE-BC-05: Hardware Security Module (HSM)
R-02	No mechanisms are specified to protect the integrity and availability of the nodes' private keys	- User Credentials - Respective platform and its components	A9.2.4 Management of secret authentication information of users	T5.2.3 User Security Credentials Management	UAE-BC-05: Hardware Security Module (HSM)

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	Proposed Controls
R-03	No mechanisms are specified for the revocation of nodes	- Abuse the respective platform and its components	A.9.2.1 User registration and de-registration A.9.2.2 User access provisioning A.9.2.6 Removal or adjustment of access rights	M4.4.3 Removal of Access Rights T5.2.3 User Security Credentials Management	UAE-BC-04: Identity Access Management (IAM)
R-04	Lack of security for endpoints/nodes, utilized relevant applications and software from possible security threats and vulnerabilities.	- Node - User Credentials - Respective platform and its components	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	A.12.6 Technical Vulnerability Management A.18.2 Information security reviews	UAE-BC-07: Smart Contract Code Audit
R-05	Lack of multi-authentication mechanisms for accessing relevant databases.	- Database - Data - Respective platform and its components	A9.2 User access management	T5.2 User Access Management	-
R-06	Lack of enforcement for database encryption on the respective nodes in order to prevent data leakage and unauthorized disclosure, modification and/or destruction.	- Database - Data - Respective platform and its components	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-07	Lack of database query protection against relevant well known security vulnerabilities.	- Database - Patient Data - Respective platform and its components	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	A.12.6 Technical Vulnerability Management A.18.2 Information security reviews	-
R-08	Absence of a monitoring strategy for the respective platform.	- Respective platform and its components and nodes	T3.6 Monitoring M6 Performance Evaluation and Improvement	A.12.4 Logging and monitoring A.18.2 Information security reviews	UAE-BC-08: Block Publication Rate
R-09	Untested and unaudited smart contracts for security threats and vulnerabilities prior to deployments.	- Respective smart contract - Respective nodes - Respective platform and its components	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	A.12.6 Technical Vulnerability Management A.18.2 Information security reviews	UAE-BC-07: Smart Contract Code Audit
R-10	Lack of access control mechanisms to prevent any unauthorized access to smart contracts.	- Respective smart contract - Respective nodes - Respective platform and its components	A.9 Access control	T5 Access Control	UAE-BC-06: Smart Contract's Access Control
R-11	Unclear vision on the used consensus mechanisms for signing, verifying and publishing blocks on the respective platform.	- Block production - Business processes	-	-	UAE-BC-01: Blockchain Business Processes

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	Proposed Controls
R-12	Unspecified requirements for secure communication over the used platform and its components.	- Respective platform and its network, applications and nodes components	A.13 Communications security A.11 Physical and environmental security A.9 Access control	T4 Communications T2 Physical and Environmental Security T5 Access Control	-
R-13	No incidents reporting procedures are specified.	- Respective platform and its network, applications and nodes components	A.16 Information security incident management	T8 Information Security Incident Management	-
R-14	Unclear vision with respect to data security and confidentiality, including but not limited to, block payloads, transmitted data and data at rest.	- Data	A.10 Cryptography	T7.4 Cryptographic Controls	UAE-BC-03: Data Ownership
R-15	Unclear vision on the data type to be stored on the respective platform.	- Data	-	-	UAE-BC-03: Data Ownership
R-16	Absence of a business continuity strategy for the respective platform.	- Respective platform	A.17 Information security aspects of business continuity management	T9 Information Systems Continuity Management	-
R-17	Lack of details on the security of the used cryptographic algorithms against security flaws and vulnerabilities.	- Data - The chain of the blocks	A.10 Cryptography	T7.4 Cryptographic Controls	-
R-18	Lack of protection against possible malicious activities of administrators.	- Abuse of privileges - Respective platform and its network, applications and nodes components	A.12.4.3 Administrator and operator logs	T3.6.3 Monitoring System Use T3.6.5 Administrator and Operator Logs T5.2.2 Privileges Management	-
R-19	Lack of details on whether the required security assessments against the relevant security threats and vulnerabilities have been performed on the respective platform, utilized applications and services before any deployments.	- Respective platform and its components	A.12.6 Technical vulnerability management A.18.2 Information security reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-20	Failure to specify and embed the necessary security requirements for developers to adhere to while they are developing and building the relevant solutions, tools and back-end application services on the respective platform.	- Respective platform and its applications, tools and services components	A.14.1 Security requirements of information systems A.12 Operation security	M5.4 Compliance with Technical Requirements T3 Operations Management	-

Risk ID	Risk Description	Asset Affected	Recommended Security Controls		
			ISO 27001 Controls	UAE IA Standard Controls	Proposed Controls
R-21	Lack of enforcement for performing the required security assessments (such as threat and vulnerability assessments) of the developed solutions, tools and back-end application services before any deployment on the respective platform.	- Respective platform and its applications, tools and services components	A.12.6 Technical vulnerability management A.18.2 Information security reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-22	Lack of security vision on the specified APIs and on whether they have been tested against relevant security threats, vulnerabilities, bugs, data breaches and DoS attacks.	- Data - Respective platform and its components	A.12.6 Technical vulnerability management A.18.2 Information security reviews	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking	-
R-23	Unclear vision on the intra-platform data flow and on data flows with other linked external platforms and applications	- Data	A.13 Communications security	T4 Communications	-
R-24	Unclear vision with the respect to the security level of relevant servers, including but not limited to, physical security, patching and server maintenance, event logs, system integrity control, anti-virus and anti-malware, authentication and access controls, and backups and restorations.	- Respective server	A.11 Physical and environmental security A.12 Operation security A.14 System acquisition, development and maintenance A.9 Access control	T2 Physical and Environmental Security T3 Operations Management T7 Information Systems Acquisition, Development and Maintenance T5 Access Control	-
R-25	Unclear vision on how the key pairs residing on the respective network are protected against hacking, theft, malicious activities and unauthorized access.	- User Credentials - Respective platform and its components	A.9 Access control A.10 Cryptography	T5 Access Control T7.4 Cryptographic Controls	UAE-BC-05: Hardware Security Module (HSM)
R-26	Lack of security requirements enforcement while developers are configuring the respective Docker images. This include threat and vulnerability management, patch management and others.	- Respective Docker images - Respective platform and its components	A.12.6 Technical vulnerability management A.18.2 Information security reviews A.12 Operation security	T7.7 Technical Vulnerability Management M5.4.1 Technical Compliance Checking T3 Operations Management	-

FUTURE WORK

With respect to evaluating the effectiveness of the proposed security controls, it requires a real implementation of these controls by an organization through establishing and implementing relevant procedures. Therefore, this section briefly provides further information with regards to this aspect, along with a high-level relevant process, as a guideline for organizations. The effectiveness of the implemented Information Security controls (as part of the Information Security Management System (ISMS)) must be assessed in a consistent and repeatable manner, in line with International Standards such as ISO/IEC 27004:2016, in order to obtain high assurance that the implemented controls continue to operate as intended in protecting the organization's information assets. The organization

should ensure that cost effective, comparable, and repeatable measures are used for assessing the security controls, in order to provide the management with the assurance that people, processes, and utilized technologies contributing towards Information Security are effective. The relevant implemented measures can also provide the management with a clear understanding of the existing Information Security risks and recommendations to manage and mitigate such risks. Measures of effectiveness of applied Information Security controls will hence ensure that the Information Security Management System is examined, analyzed, evaluated, and improved on a continuous basis. T Blow is a high-level evaluation process for measuring the effectiveness of the implementation pf security controls in line with International Standards such as ISO/IEC 27004:2016.

- As part of the annual risk assessment carried out by the organization, all risks should be mapped to their corresponding ISO 27001 and UAE IA controls.
- Based on the severity of the risk levels, the effectiveness of the controls should be assessed based on a predefined evaluation criterion (for example, as shown in Table 6).

Table 6. Control effectiveness matrix

Risk Level	Control Effectiveness Score
Very Low	Fully Effective
Low, Medium	Partially Effective
Very High, High	Not Effective

- Based on the effectiveness score assigned to each control, corrective action plans should be prioritized for implementation (for example, as shown in Table 7).

Table 7. Corrective action prioritization

Control Effectiveness Score	Corrective Action Implementation Timeline
Fully Effective	N/A
Partially Effective	Within 3 months
Not Effective	Within 1 month

- The control effectiveness scores along with corrective action plans should be presented to and agreed upon with the organization's information security committee.
- The corrective action plans should be implemented by all stakeholders (for example, the respective departments) within the agreed upon timelines.
- The stakeholders should keep the organization's information security committee informed about progress of any corrective action plans and any potential delays and/or issues.
- Progress on considered corrective actions should be reviewed during the organization's information security committee meetings and enhancements/adjustments to the plans may be made, as applicable.

CONCLUSIONS

The aim of this paper is to introduce a new information security controls framework for blockchain technology, which is currently missing from National and International Information Security Standards. Through the risk assessments performed on the blockchain use cases herein, we have determined risks associated with security controls, in order to mitigate relevant information security risks and consequently protect the information and other assets against unauthorized disclosure, modification, and destruction that could negatively impact individuals, organizations, and/or entire nations. The significance of the proposed security controls is manifested in complementing those controls that have already been established by the International and National Information Security Standards

in order to keep pace with the emerging blockchain technology and prevent/reduce its associated information security risks (the standards utilized in this study are the ISO 27001:2013 Standard and the UAE Information Assurance Standards).

The aforementioned risk assessments were performed on five blockchain use cases, based on the ISO 31000:2018 Risk Management Standard Guidance to determine their involved risks along with their respective security controls as per the UAE IA Standard's controls, ISO 27001 Standard's controls, and the proposed security controls. The analysis results showed that the proposed security controls herein can mitigate relevant information security risks of blockchain based solutions and applications, and consequently protect information and assets from unauthorized disclosure, modification, and destruction. Furthermore, it was demonstrated that some of the security risks were not covered by existing Standards, and these can be mitigated and reduced when applying the security controls proposed herein. This justifies the need for such additional controls and encourage standardization bodies to incorporate these controls in their future editions.

The performed risk assessment on the blockchain use cases herein demonstrates that blockchain can involve security risks that require certain actions to avoid. Hence, practitioners should not blindly assume that through the use of blockchain technology all security threats are mitigated.

That being said, our study still has some limitations. The majority of the blockchain use cases in this study are publicly published papers/reports. Therefore, the lack of technical details about these respective solutions results in the inability to perform a fully comprehensive risk identification. Therefore, this area will be part of our future work. In addition, covering other standardization bodies in the area of distributed ledger related to blockchain technology would also prove fruitful, along with respective future designs of relevant security architectures.

REFERENCES

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2020). A survey on blockchain interoperability: Past, present, and future trends. *ArXiv:2005.14282*.

CohnReznick. (2018). *Risk and control considerations for blockchain technology*. https://www.cohnreznick.com/insights/risk-and-control-considerations-for-blockchain-technology

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283-297. https://doi.org/10.1016/j.scs.2018.02.014

Drljevic, N., Aranda, D. A., & Stantchev, V. (2020). Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Computer Standards and Interfaces, 69*, 1-7. https://doi.org/10.1016/j.csi.2019.103409

EnergyWeb. (2020). *EW-DOS: The energy web decentralized operating system. An open-source technology stack to accelerate the energy transition. Part 2: Technology detail.* https://www.energyweb.org/wp-content/uploads/2020/06/EnergyWeb-EWDOS-PART2-TechnologyDetail-202006-vFinal.pdf

Flood, J. & McCullagh, A. (2020). Blockchain's future: Can the decentralized blockchain community succeed in creating standards? *The Knowledge Engineering Review, 35*(2), 1-11. https://doi.org/10.1017/S0269888920000016

Fu, J., Wang, N., & Cai, Y. (2020). Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. *Sensors, 20*(7), 1898. https://doi.org/10.3390/s20071898

Gramoli, V., & Staples, M. (2018). Blockchain standard: Can we reach consensus? *IEEE Communications Standards, 2*(3), 16-21. https://doi.org/10.1109/MCOMSTD.2018.1800022

Howard, J. P., & Vachino, M. E. (2020). Blockchain compliance with federal cryptographic information-processing standards. *IEEE Security & Privacy, 18*(1), 65-70. https://doi.org/10.1109/MSEC.2019.2944290

International Organization for Standardization. (2018). *Risk management – Guidelines*. ISO 31000:2018(en). https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

König L., Korobeinikova, Y., Tjoa, S., & Kieseberg, P. (2020). Comparing blockchain standards and recommendations. *Future Internet, 12*(12), 222. https://doi.org/10.3390/fi12120222

Lima, C. (2019). Developing open and interoperable DLT/Blockchain standards. *Computer, 51*(11), 106-111. https://doi.org/10.1109/MC.2018.2876184

Liu, Z., & Li, Z. (2020). A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management, 52,* 1-18. https://doi.org/10.1016/j.ijinfomgt.2019.102059

Manupati, V. K., Schoenherr, T., Ramkumar, M., Wagner, S. M., Pabba, S. K., & Singh, R. I. R. (2020). A blockchain-based approach for a multi-echelon sustainable supply chain. *International Journal of Production Research, 58*(7), 2222-2241. https://doi.org/10.1080/00207543.2019.1683248

MedRec. (2018). *MedRec technical documentation.* https://medrec.media.mit.edu/images/medrec_technical_documentation.pdf

National Institute of Standards and Technology. (2019). *Security requirements for cryptographic modules.* https://csrc.nist.gov/publications/detail/fips/140/3/final

Otto, K. (2019). Data standards are fundamental for blockchain implementation. *National Provisioner, 233*(10).

Power Ledger. (2019). *White paper.* https://uploads-ssl.webflow.com/5fc9b61246966c23f17d2601/6087c060d74a5f523f6b84a6_Power%20Ledger%20White%20Paper%202021.pdf

Provenance Blockchain, Inc. (2020). *Provenance: Creating the future of finance.* https://www.provenance.io/documents/Provenance%20Whitepaper%20-%202020.pdf

Samuel, O., Almogren, A., Javaid, A., Zuair, M., Ullah, I., & Javaid, N. (2020). Leveraging blockchain technology for secure energy trading and least-cost evaluation of decentralized contributions to electrification in Sub-Saharan Africa. *Entropy, 22*(2), 1-36. https://doi.org/10.3390/e22020226

Uriarte, R. B., & De Nicola, R. (2018). Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards. *IEEE Communications Standards, 2*(3), 22-28. https://doi.org/10.1109/MCOMSTD.2018.1800020

Van Leeuwen, G., Alskaif, T. A., Gibescu, M., & Van Sark, W. (2020). An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Applied Energy, 263*, 1-13. https://doi.org/10.1016/j.apenergy.2020.114613

Wang, Z., Luo, N., & Zhou, P. (2020). Guardhealth: Blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare. *Journal of Parallel and Distributed Computing, 142*, 1-12. https://doi.org/10.1016/j.jpdc.2020.03.004

Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., & Xiao, Q. (2020). Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in Construction*, 111, 1-13. https://doi.org/10.1016/j.autcon.2019.103063

Yazdinejad, A., Srivastava, G., Parizi, R. M., Dehghantanha, A., Choo, K. R., & Aledhari, M. (2020). Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE Journal of Biomedical and Health Informatics, 24*(8), 2146-2156. https://doi.org/10.1109/JBHI.2020.2969648

AUTHORS

Maitha Al Ketbi graduated from the United Arab Emirates University in 2021 with a Master's degree in Information Security. She completed her Bachelor's degree in Information Security in 2016 at the same university. She has four years of experience in information security governance, including implementing and auditing of International Standard of Information Security Management (ISO/IEC 27001), Risk Management and Business Continuity. She completed training courses such as Project Management Professional (PMP), Certified ISO27001 Auditor, Cisco Certified Network Associate (CCNA) and others related to information security. She aims to continue her work in information security, more specifically governance and operational areas of research and development.

Khaled Shuaib received his PhD in Electrical Engineering from the City University of New York, 1999, his MS and BE in Electrical Engineering from the City College of New York, 1993 and 1991 respectively. Since September 2002, Khaled has been with the College of Information Technology (CIT), at the United Arab Emirates University where he is currently a Professor. His research interests are in the areas of Communication Networks, Blockchains, IoT, Network Security, Smart Grid and Smart Healthcare Systems. Prior to joining the UAE University, Khaled had several years of industrial experience in the US working as a Senior Member of Technical staff at GTE Labs, Waltham, MA (1997-1999), and as a Principal Performance Engineer for Lucent Technologies, Westford, MA (1999-2002).

Dr. Barka is currently an Associate Professor at the United Arab Emirate University. He received his Ph.D. in Information Technology from George Mason University, Fairfax, VA in 2002, where he was a member of the Laboratory for Information Security Technology (LIST). His current research interests include Access Control, where he published a number of papers addressing delegation of rights using RBAC. Other research areas include Digital Rights Management (DRM), Large-scale security architectures and models, Trust management, Security in UAVs, and Network "Wired & Wireless" and distributed systems security. Dr. Barka has published over 50 Journals and conference papers. Dr. Barka is an IEEE member, member of the IEEE Communications Society and member of the IEEE Communications & Information Security Technical Committee (CISTC). He serves on the technical program committees of many international IEEE conferences such as ACSAC, GLOBECOM, ICC, WIMOB, and WCNC. In addition, he has been a reviewer for several international journals and conferences.

Marton Gergely is an Assistant Professor in the Department of Information Systems and Security in the College of IT at the United Arab Emirates University. He was born in New Delhi and grew up in Budapest and Houston. He holds a PhD in Business Administration, with an emphasis on Information Technology, from The University of Texas at San Antonio. His current research interests include Digital Piracy, Social and Cognitive Psychology in Technology Use, Cyber Law and Ethics, Social Desirability Bias, as well as Informed Consent.