Eng Int Syst (2020) 3: 185–191


**Engineering**
***Intelligent Systems***

# A Compromise-Tolerant Key Management Framework for Private Blockchain

**Marius Becherer*, Thien Bui-Nguyen†, Michael Zipperle‡, and Florian Gottwalt§**

*Logistics Insight Lab, UNSW@ADFA, Canberra, Australia*

One major threat for enterprise private blockchains is the compromise of the trust-enabling Public Key Infrastructure (PKI). While the invention of private blockchains has addressed the trust problem in inter-organisational information sharing, the confidentiality, integrity, and availability of information within one organisation is still reliant on traditional, centralised key management like PKI. This design has introduced a number of risks including: a) trust reliance on a few people creating an insider threat vulnerability; b) potential loss of assets, reputation, and privacy; c) single-point-of-failure; and d) defeating the distributed trust introduced by the invention of public blockchains. To mitigate these risks, this work proposes a compromise-tolerant key management approach that combines decentralised blockchain-based trusted PKI with the enforcement of multi-signature and smart contract features. Using a multi-signature feature allows the combination of decentralised blockchains and centralised PKIs, whereas smart contract enables key management transparency among all network participants to establish the distributed trust and mitigate insider and outsider threats.

Keywords: blockchain-based key management, process transparency, enterprise key management

## 1. INTRODUCTION

Enterprises have to secure their assets not only against intruders but also their own employees. One recent prominent case of an insider threat resulted in Twitter blocking Donald Trump's account brought about by a Twitter employee on their last day working for the company [1]. Security incidents related to insider threats still reveal one of the major challenges in cybersecurity. One of the biggest threats to enterprise data management, especially private blockchains, is a reliance on the traditional PKI which does not address the fact that breaches of trust are not only caused by outsiders but insiders too including software providers, administrators, or internal or external users. The vulnerabilities are manifold and may result in a loss of trust, assets, reputation, privacy, broken functionalities, and disrupted services caused by this single-point-of-failure.

*m.becherer@adfa.edu.au
†t.bui-nguyen@adfa.edu.au
‡m.zipperle@adfa.edu.au
§f.gottwalt@adfa.edu.au

The traditional PKI becomes vulnerable as it has a centralised design expressed in one root certificate authority and high trust is placed on a few individuals. Considering potential threats of insider vulnerabilities against a single-point-of-failure, the probability of compromised systems rises. For instance, theft of the private key from the certificate authority opens up the opportunity for them to issue malicious certificates, which would compromise the enterprise's data management. Consequently, risks in the form of losing assets, reputation, and privacy, emerge and may threaten the existence of enterprises. Besides the risk of potential security breaches by the centralised nature of PKI, it is also challenging to trust someone's actions. Existing PKIs are short in transparency about processes and users may be unaware of how data is processed. Without transparent policies, users often have to rely on intransparent decision-making from administrators. Insider actions, such as a malicious administrator, remain undetected and lower the overall level of trust. Hence, it is essential to monitor actions and determine policies to increase trust.

To mitigate these risks, this work introduces a compromise-tolerant key management approach that combines hierarchical blockchain-based PKI with a distributed peer-to-peer Certificate Authority (CA) network. The combination of both key management approaches utilises multi-signature and smart contracts. Finding sufficient approval of critical operations such as certificate issuance, multi-signatures are applied building on common ground based on a certificate authority's response. Supported by a predefined operation set in smart contract, process transparency is enabled among all network participants to forge common trust in distributed environments. The proposed conceptual model addresses insider and outsider risk in the weakest link of enterprise blockchain key management and protects enterprises from the compromise of assets and breaches of trust.

The structure of this work is as follows. An overview of background information and related work will be offered in section II. In section III we will propose the conceptual model of the compromise-tolerant key management concept. Later, we present preliminary work in section IV and discuss the improvement of this conceptual model in section V. Finally, future work will be suggested in section VI and this research will be concluded in section VII.

## 2. LITERATURE REVIEW

Blockchain currently receives much attention due to its promise of a trust-free technology driven by data processing transparency through smart contracts and the difficulty to manipulate data on the blockchain. However, enforced security methods in public blockchains limit the throughput of transactions that leads to the development of private blockchains. The upsurge in transaction throughput needs well-performed consensus protocols and requires the identification of entities such as nodes, individuals, and transaction entities within the blockchain network. Using private blockchains weaken security techniques by the reduction of consensus nodes and missing crypto-economics. The trade-off between using private, public blockchains, or other variations of blockchain frameworks is referred to as the blockchain trilemma [2].

Even though all variations of blockchain should replace trust, all frameworks rely on some aspects of trust. Multiple components in private blockchains are likely to use as attack vendors for insiders such as the key management component. Considering the impact of insider attacks, security breaches in the blockchain network create risks such as loss of assets, reputation, and privacy [3]–[5]. Therefore, existing literature on key management frameworks emphasise the relevance of increasing private blockchain security.

The traditional PKI comes with drawbacks such as high trust required in a centralised Certificate Authority (CA). Compromise of public key infrastructure is a real-world threat that has already led to a loss of assets and loss of reputation [6]. In the past, centralised log-based PKI and decentralised Web-of-Trust concepts gained much interest in this field of research. Centralised log-based PKI is widely applied on the web. The concept of Certificate Transparency (CT) tracks the history of issued certificates [7]. Even though key forging can be detected, the concept of Certificate Transparency cannot prevent valid compromised certificates. Since the different nodes of a Certificate Transparency cluster run physically decentralised, they have a replicated state that makes them logically centralised.

Other research focuses on distributed key management launched by the Web-of-Trust whereas trusted nodes in the network can sign certificates of uncertified nodes [8]. However, since the distributed key management impedes efficient and reliable information sharing in real-time, security mechanisms like certificate revocation cannot sufficiently be applied. Furthermore, the network participants have to be well educated about whom to trust whereas different methods can be applied.

More recent work includes hardware and software-based approaches to reduce the likelihood and impact of certificate compromise through hardening existing security approaches. One software-based approach enforces the principle of "separation-of-duty" through the creation of multiple intermediate CAs by a root certificate authority going offline to protect the private key for signing certificates [9]. To strengthen the key protection of certificate authorities, the private key is linked to a Hardware Security Module (HSM) that binds the digital representation to a physical entity [10]. Even though much research has been done in this domain, traditional PKIs still inherit risks due to the nature of the centralised design [5]. Furthermore, the intransparent key management design allows malicious certificates to go undetected. Therefore, breakthrough research and new approaches are needed to overcome existing issues in traditional PKI.

Blockchain technology introduces policy-based execution transparency powered by smart contracts, data security through immutable chaining technology, and high availability through its distributed nodes. Some blockchain-based PKIs have been proposed to overcome this limitation in intransparent key management and centralised design.

The BlockPKI uses multi-signature to validate domains of a distributed CA network of the requestor for TLS certificates. Furthermore, smart contracts are employed to ensure transparency throughout the process and crypto-economics are applied for certificate issuance. However, issuing a certificate takes several minutes since the blockchain is running in a public blockchain. The proposed framework relies on a third-party blockchain network and, consequently, the flexibility to change procedures for critical operations is limited. Additionally, the BlockPKI so far does not consider an efficient, reliable revocation mechanism of the certificates [11].

More work on blockchain-based PKI focuses on rapid certificate revocation and the elimination of one single-point-of-failure through majority voting. Consequently, if misbehaviour of one CA occurs, the whole system is not totally affected since trust is distributed between the CAs. However, intruders can easily deploy smart contract since this framework is lacking in its prevention mechanism and the trust completely relies on the nodes in the network [12], [13].

The BlockPGP framework is considering a P2P trust network. While the CAs are fully decentralised in a private network, the Proof-of-Authority consensus mechanism is applied to save computational resources. The BlockPGP does

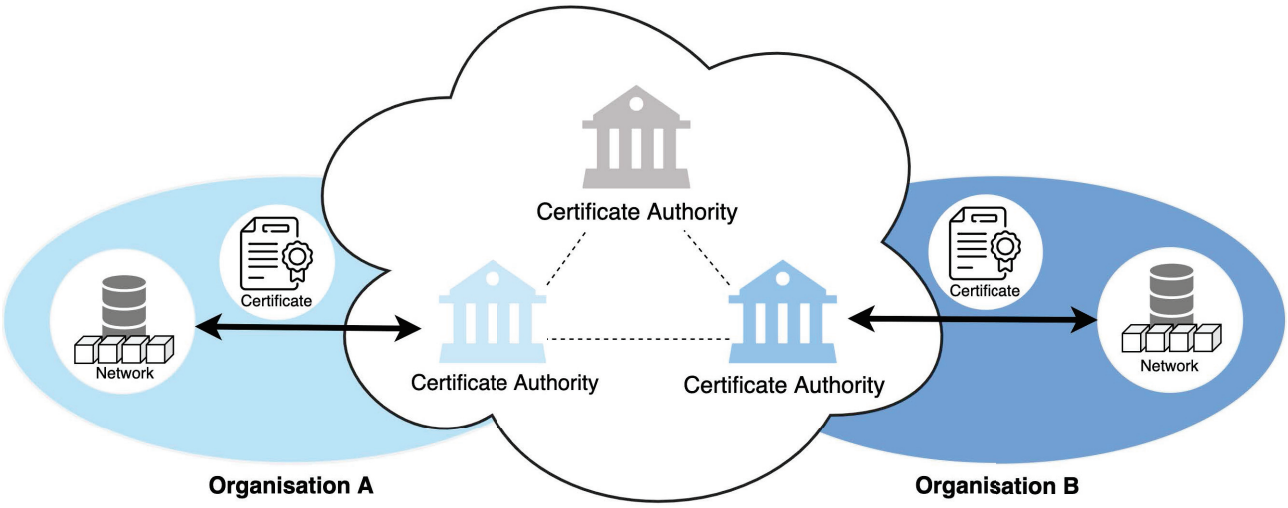


**Figure 1** Conceptual model of compromise-tolerant key management network

not support trust levels and, furthermore, Proof-of-Authority can be tampered with lowering the level of trust [14].

An identity system based on PKI that utilises smart contract, called SCPKI, is also built on the Web-of-Trust network. The proposed PKI considers compromises and limits their impact through multiple nodes. Even though the system is highly reliable, a fully P2P network is not applicable since long communication paths limit the scalability of the network. Managing a distributed network is essential when certificates have to be revoked. Barriers for entry can be challenging as well. Consequently, this proposed method is less applicable to enterprises.

The latest research in blockchain-based PKIs lacks practical implementation and structured evaluation. Even though the proposed concepts often promote their contribution, the limitations are rarely discussed and need to be evaluated against a reference framework to assess benefits and issues with conventional and blockchain-based PKIs.

The literature review on existing key management approaches identified shortcomings in single-point-of-failure vulnerabilities through centralisation of enterprise key management.

Furthermore, current risk mitigation approaches in state-of-the-art enterprise key management systems focus on reducing the likelihood and ignore impact reduction. Few works attempt to find a trade-off between decentralisation key management and efficient and a reliable revocation mechanism to supply essential security mechanisms for long-term deployment.

However, existing literature focuses mainly on TLS certificates to verify authenticity of domain names instead of enterprise key management. Enterprises need to consider circumstances such as dynamism of the computing environment and contextual background of employees to mitigate risks of insider attacks.

Traditional PKIs issue certificates often regarding an intransparent decision-making process from a user's perspective whereas multiple possible attack vendors of insider threats are applicable. Therefore, transparent predefined policies reduce the likelihood of insider threats as long as fitting policies to prevent possible attack vendors are taken into consideration.

To the best of our knowledge, no research has provided a sustainable blockchain-based solution to combine benefits of the distributed and centralised key management in the enterprise domain. In detail, policy-based execution transparency for critical processes, implemented in smart contracts, and multi-signature validation of certificates for a compromised-tolerant certificate authority framework is going to be applied. Additionally, an efficient revocation mechanism in a distributed infrastructure is needed to support an essential security feature for long-term deployment.

## 3. CONCEPTUAL MODEL

A Compromise-Tolerant Key Management framework is proposed in this work to strengthen the weakest link in enterprise private blockchain infrastructures. The novel key management framework is designed to provide: (1) a compromise-tolerant behaviour during a security breach; (2) the provision of a policy-based execution transparency for critical operations; and (3) an efficient revocation mechanism to invalidate tampered certificates.

To achieve the mentioned objectives, the proposed key management applies concepts from both the PKI and the Web-of-Trust to combine the benefits of decentralised and centralised key management approaches. Using the Web-of-Trust for the CA to separate trust between multiple institutions is illustrated in Figure 1. Within the Web-of-Trust, more communication is required in order to find consensus in decision-making, which reduces performance. However, this setup avoids single-point-of-failure security threats since the key management framework does not rely on a single authority. Furthermore, the CA can decide for itself whom to trust and implement their own policies. From the perspective of organisation participants, the key management framework appears as a single CA where they are interacting. This illusive certificate authority disposes of advantages of PKI like efficient communication and easier decision-making. Especially the revocation mechanism of certificates profits from the simplified communication of interacting with only one CA. Consequently, the combined approach

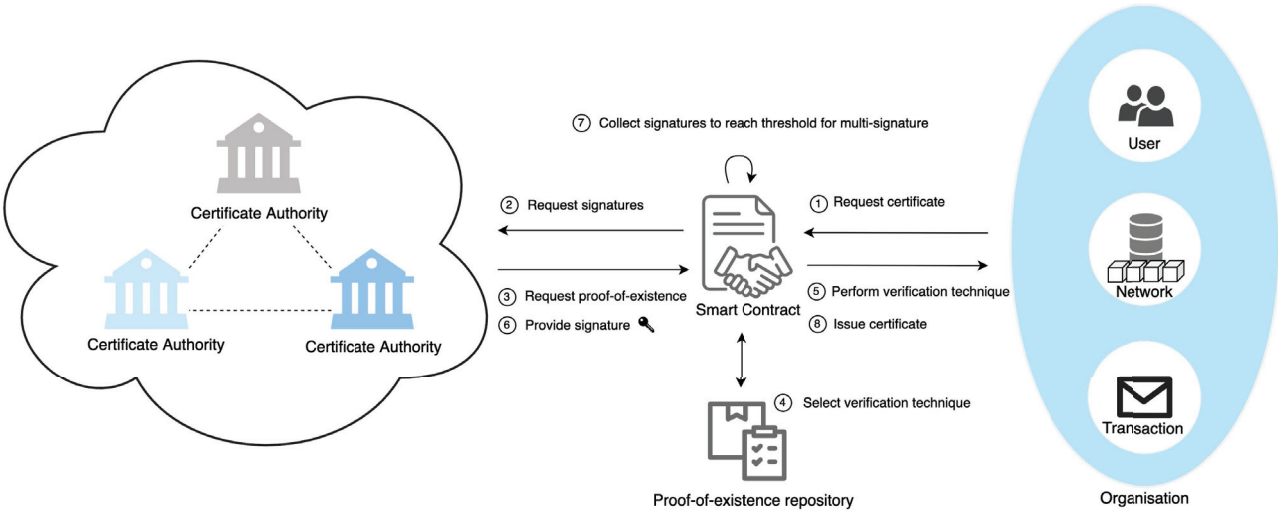


**Figure 2** Interaction between "Web-of-CA" network in conceptual model through smart contract

of centralised and distributed key management provides compromise-tolerant key management that is able to operate properly in exceptional scenarios such as (un)intentionally issuing and reissuing certificates to untrusted requestors.

Integration of business processes into the compromise-tolerant key management uses the concept of smart contracts to support transparency. The characteristic of transparent policies enforces trust in the correctness of business process since the operation of the data processing is public among the network. Especially, critical business processes such as issuance, reissuance, and revocation of certificates need strong observation and equivalent policies for each of the network participants. The combination of streamlined business processes into the distributed key management network of CA requires a compromise-tolerant signing schema.

The application of multi-signatures supports distributed trust among the CA. The process between critical operations in a distributed untrusted environment is presented in Figure 2. Within an organisation, entities such as member, blockchain components, and transactions have to be identified with certificates. Before they can be identified and participate in the network, each entity has to request a certificate. To request a certificate, entities revoke accessible operations on the smart contract. The procedure to sign a certificate is as follows:

1) The entity requests a certificate by invoking "issue certificate" from the smart contract.
2) The smart contract requests signatures of the certificate authorities for multi-signature.
3) Each certificate authority requests proof-of-existence by invoking the smart contract.
4) The smart contract randomly selects a proof-of-existence method, which the requestor of the certificate has to perform.
5) The smart contract performs verification techniques with the requestor. Note that the requestor has to perform multiple verification techniques in order to get the required number of signatures.
6) If the verification process is successful, the certificate authority provides its signature.
7) The smart contract collects all signatures of the certificate authorities.
8) A certificate is created as soon as the required number of signatures of certificate authorities is obtained.

## 4. IMPLEMENTATION OF PKI IN AN ENTERPRISE ENVIRONMENT

In preliminary research, we investigated the deployment process of blockchain in an enterprise environment that raises issues within the system security, especially the reliance on existing key management. For this reason, we present our previous blockchain deployment process and security configuration to provide a common foundation for subsequent discussion in Section V.

Overall, the purpose of the blockchain network in our preliminary work focuses on the use case to provide transparency with asset data management. Using the nature of blockchain, inter-organisational commitments are facilitated to execute rather than only intra-organisational commitments. In detail, extensive hierarchical organisations are characterised by long processes with multiple parties. To ensure process commitment of each party, blockchain provides process transparency through smart contract to achieve commitment and data transparency through a replicated ledger among the network. The enforcement of immutable data, once written into the ledger, builds trust into the asset data management. Overall, actions performed by various blockchain members are traceable and process derivation triggered by a set of blockchain members can be discovered. Since this blockchain implementation considers one hierarchical large-scale organisation, we break down different departments of the organisation to transform our intra-organisation to an inter-organisational scenario.

The prototype scenario involves two different organisations that form a blockchain network implemented by the

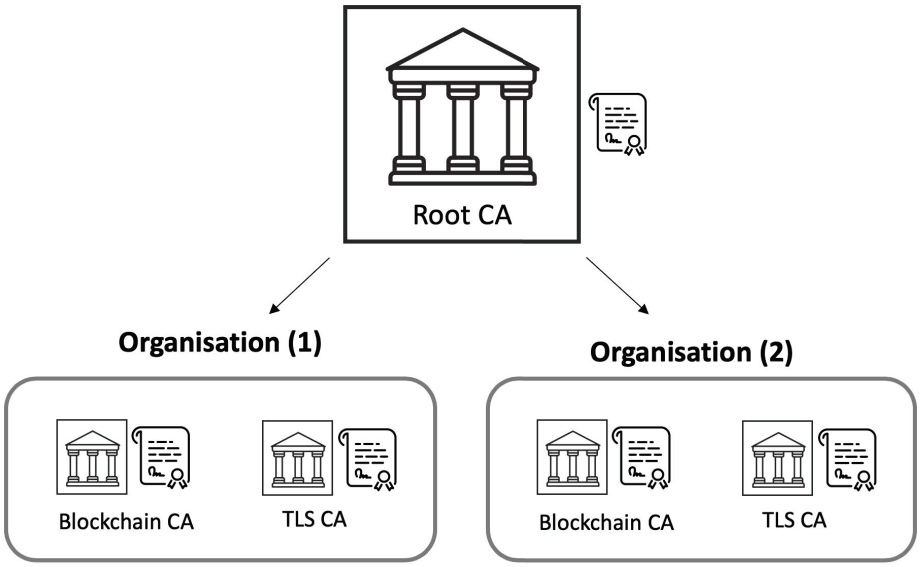


**Figure 3** Implementation of multiple intermediate certificate authorities

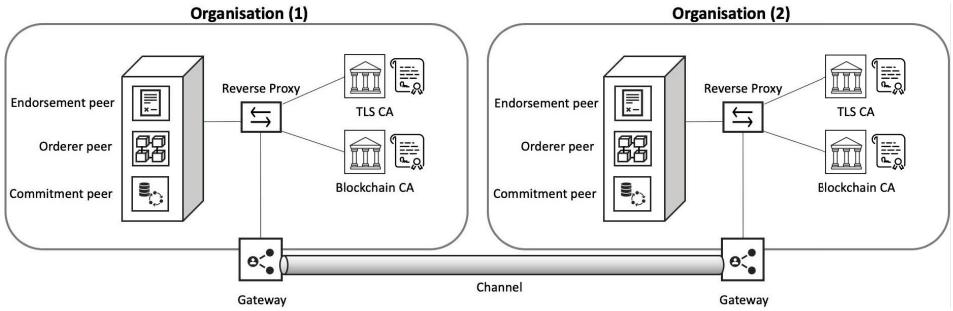


**Figure 4** Implementation of enterprise blockchain deployment

Hyperledger Fabric framework. One trusted organisation consists of: (a) an endorsement peer to validate transaction through the smart contract; (b) an ordering peer to create a block; and (c) a commitment peer to validate distributed blocks onto the blockchain as well as TLS certificate authority and blockchain-specific certificate authority. To facilitate the setup, we do not consider additional components that are necessary to implement but do not add value in explaining key-related issues. Each virtual machine within one organisation holds at least two replications of its network component to be resilient to a single virtual machine failure with minimal consequences.

The design of our public key infrastructure combines hardware- and software-based approaches. The hardware-based approach utilises a Hardware Security Module (HSM) that is used to generate and physically bind all credentials reflected as private and public keys. To create the keys Elliptic Curve Digital Signature Algorithm (ECDSA) with 256 bits is applied to meet current state-of-the-art requirements.

Our blockchain deployment process includes the setup of, firstly, one root certificate authority where the root credentials are stored and, secondly, the Intermediate Certificate Authority (ICA) which represents certificate authority to the member of the belonging organisation. Both root and ICAs have their own HSM whereby the HSM of the root CAs are taken offline after issuing certificates for the intermediate certificate authorities to avoid external access. Overall, each organisation disposes of two root authorities to issue certificates for TLS communication as well as blockchain-related component identification as illustrated in Figure 3.

Based on this, we implemented an automated deployment process that used a configuration of the blockchain network. We experienced less misconfiguration and higher reliability of our deployment. Deploying a blockchain network continues after setting up the intermediate certificate authorities by enrolling administrators. The presence of one administrator within one organisation enables issuing certificates of gateways and peers. At this stage, belonging components within one organisation are identifiable through certificates. To create blockchain among multiple departments, a common network is realised in our configuration for the orchestration environment and in a framework-related channel concept presented in Figure 4. More specifically, the orchestration environment consists of two types of network: private network within one organisation and private network that compounds organisations' gateways. For establishing a channel, the agreement of participating administrators is required. Nevertheless, our careful implementation raises concerns about the weaknesses of existing key management.

Overall, our preliminary work secures keys with HSMs to bind the key to physical entities. Furthermore, certificates can efficiently be revoked through the centralised public key

infrastructure and reduce the potential impact of credential's theft through multiple intermediate certificate authorities.

However, the presented system fundamentally lacks key management that traces back to centralisation in the perspective of public key management and high trust in the administrator. The private keys especially from CAs have to be securely protected against all entities as they are essential to the proper working security infrastructure. A serious threat comes from an organisation's members that have privileges through higher access rights and physical access to machines of the blockchain network. Therefore, this private enterprise blockchain is facing threats from insiders whereas compromised certificates are possible that can cause data theft or compromises. Various challenges also arise within development and deployment stages, which concern establishing and changing policies that mitigate insider threats as well as keep a certain level of simplicity. Consequently, compromises have to be considered and actions discussed to limit damage to the enterprise security infrastructure.

## 5. EVALUATION AND DISCUSSION

Findings from our preliminary work identified shortcomings in the logical and political centralisation of security infrastructure reflected in the CA and administrator as well as compromise-intolerant data theft threatened by insiders. Therefore, moving from logical and political centralisation to greater distribution requires less trust in a single entity. Additionally, process transparency enforces trust in a third party entity within critical operations such as certificate issuance.

The conceptual model of our compromise-tolerant key management framework mitigates threats coming from logical centralisation of PKI by using multiple certificate authorities. Hereby, each certificate authority is independent and decides, based on defined policies, how to operate. If a certificate authority has undertaken tampering, the system is able to deal with compromises until a threshold of required signatures is reached. A similar scenario can be prevented by insider threats through limiting the power of the administrator. More specifically, the most powerful person reflected in administrators in a security infrastructure has limited opportunities to compromise the system. Possible compromising attempts by administrators, like deploying malicious smart contracts or signing malicious certificate requests, requires the consensus of other administrators. However, moving from centralisation to a distributed key management increases communication complexity since more information has to be shared between each party to reach consensus. Therefore, scalability in distributed systems is one challenge that depends on multiple factors such as the number of involved parties and consensus protocol. The increasing communication complexity complicates an efficient and reliable revocation mechanism.

To increase trust in third parties, addressing how data is processed and which policies have to be fulfilled improves transparency. This conceptual model relies on transparent policies that can be verified. Therefore, all operations are subject to reasonable decision-making rather than intransparent and arbitrary decision-making from humans.

Nonetheless, process transparency exposes details and policies of the certificate issuance process and, consequently, malicious users could use this information to execute attacks against the security infrastructure. From the perspective of continuous integration, firstly new updates on the policy expressed in smart contracts need consensus by all administrators and, secondly, regardless of thorough testing, new security vulnerabilities could be introduced.

## 6. FUTURE WORK

Overall, the proposed compromise-tolerant key management framework improves existing centralised PKIs through distributed approaches and high transparency. Our proposed model is facing shortcomings as well and a few details require more in-depth consideration.

Policies should be seriously considered and implemented for CAs along with entities verified whether individuals or network components. How can other certificate authorities trust each other and their actions? Additionally, policies for critical operations need reliable and verifiable methods against tampering. Besides, determining the threshold of required signatures from CAs in a dynamic environment needs the proper balance between simplifying communication effort and strengthening security.

Another aspect is deploying a certificate authority network. The certificate authorities have to discover each other and evaluate whether they trust each other. Especially in networks with few participants and based on trust assessing methods, it constitutes a challenge to establish trust among certificate authorities and to achieve consensus.

Last but not least, increasing scalability in a distributed network is key to supporting an efficient revocation mechanism. More investigation should be undertaken to find a scalable consensus mechanism to accelerate certificate issuance and revocation.

## 7. CONCLUSION

Centralised PKI in a private enterprise blockchain suffers from one trusted certificate authority and trust in the administrators. Additionally, lack of processing transparency lowers trust in responsible individuals. The combination of one single-point-of-failure, centralisation of control, and insufficient processing transparency poses risks of insider threats.

These issues are being addressed in this conceptual model of a compromise-tolerant key management framework. To operate properly, the proposed system consists of multiple certificate authorities to mitigate the potential of a compromised certificate authority. Endorsement of critical operations depends on the agreement threshold of certificate authorities using multi-signatures. Furthermore, transparent policies and the processing sequence to execute critical operations assists emerging trust in each certificate authority. The employment

of predefined transparent processes makes it difficult for insiders to leave specified processes.

To demonstrate the benefits of the proposed compromise-tolerant key management framework, we presented our preliminary work and show how the proposed key management framework overcomes existing bottlenecks. In the future, more work needs to be done in expressive policies and efficient revocation mechanisms.

## ACKNOWLEDGEMENT

This project is funded by the Australian Department of Defence, the Capability, Acquisition, Sustainment Group and the CSA group under the leadership of the Assistant Director, Stuart Green.

## REFERENCES

1. J. Walters, and O. Solon, "Experts warn about security after Donald Trump's Twitter account briefly deleted", *The Guardian*, 4 November 2017.
2. J. Abadi, and M. Brunnermeier, "Blockchain Economics," National Bureau of Economic Research, Cambridge, MA, Tech. Rep., Dec. 2018.
3. B. Putz, and G. Pernul, "Trust factors and insider threats in permissioned distributed ledgers: An analytical study and evaluation of popular DLT frameworks," *Lecture Notes in Computer Science*, vol. 11860, pp. 25–50, 2019.
4. C. Hebert, and F. Di Cerbo, "Secure blockchain in the enterprise: A methodology," *Pervasive and Mobile Computing*, vol. 59, p. 101038, 2019.
5. I. Homoliak, S. Venugopalan, Q. Hum, and P. Szalachowski, "A Security Reference Architecture for Blockchains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 390– 397.
6. J. R. Prins, "DigiNotar Certificate Authority breach "Operation Black Tulip"," *Fox-IT, November*, p. 18, 2011.
7. B. Laurie, "Certificate transparency," *Communications of the ACM*, vol. 57, no. 10, pp. 40–46, 2014.
8. S. Garfinkel, "*PGP: Pretty Good Privacy*." O'Reilly Media, Inc., 1995.
9. Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman, "Analysis of the https certificate ecosystem," in *Proceedings of the 2013 Conference on Internet Measurement Conference*, ser. IMC '13, Barcelona, Spain: Association for Computing Machinery, 2013, pp. 291–304.
10. S. Koley and P. Ghosal, "Addressing hardware security challenges in internet of things: Recent trends and possible solutions," in *2015 IEEE 12th Intl Conf onUbiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, IEEE, 2015, pp. 517–520.
11. L. Dykcik, L. Chuat, P. Szalachowski, and A. Perrig, "BlockPKI: An automated, resilient, and transparent public-key infrastructure," *IEEE International Conference on Data Mining Workshops, ICDMW*, vol. 2018Novem, pp. 105–114, 2019.
12. M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "CertLedger: A new PKI model with Certificate Transparency based on blockchain," *Computers and Security*, vol. 85, pp. 333–352, 2019.
13. A. Yakubov, W. M. Shbair, A. Wallbom, D. Sanda, and R. State, "A blockchain-based PKI management framework," *IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*, pp. 1–6, 2018.
14. A. Yakubov, W. Shbair, and R. State, "BlockPGP: A Blockchain-Based Framework for PGP Key Servers," in *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, IEEE, Nov. 2018, pp. 316–322.