Paper ID : 598

Unchaining the Future of Software License management in the Digital Age Through Blockchain

K A D de Alwis[1#], D D Chamindya[2], K R Hettiarachchi[3],WAAM Wanniarachchi[4] and PPNV Kumara[5]

[1,2,3,4,5]*Department of Information Technology, Faculty of Computing, General Sir John Kotelawala Defence University, Sri Lanka*

[#] *<38-bit-0032@kdu.ac.lk @kdu.ac.lk>*

Abstract— *In the current digital age, software license management plays an essential role in assuring compliance, security, privacy, and optimal use of software resources. With the dawn of blockchain technology, there is a growing interest in exploiting its potential to transform software license management. This research study focuses on how blockchain technology, digital signing, and smart contracts can be used to redesign software license management. The Research investigates the unique contributions of blockchain technology in improving security, trust, and automation in software license administration, as well as software license challenges. It delves into the concept of digital signing, which offers a cryptographic technique for verifying the validity and integrity of license agreements, assuring non-repudiation, and prohibiting unauthorized modifications. Furthermore, this research looks into the potential of smart contracts in automating license verification, activation, and expiration processes based on established conditions, expediting administrative duties, and reducing human intervention. This research sheds light on their combined impact on software license management. It emphasizes the advantages of using blockchain for immutable record keeping, transparent audit trails, and improved license compliance. The study also covers the various obstacles and considerations in deploying these technologies, such as scalability and privacy. This research paper investigates the digital age's reformation of software license management, highlighting the transformational possibilities of blockchain, digital signing, and smart contracts.*

Keywords— Software license management , Blockchain , Digital signing, Smart contracts , Privacy

I. INTRODUCTION

Effective software license management is crucial in the digital age to ensure compliance, and security, and optimize software resources. Traditional approaches face challenges such as lack of transparency and enforcement. This has led to the exploration of blockchain technology as a solution. This research aims to investigate the benefits and challenges of implementing blockchain, digital signing, and smart contracts in software license management. Blockchain is also recognized for its data security, anonymity, and integrity, finding applications in industries like healthcare. (Gupta, 2023) Bitcoin, Blockchain, Ethereum, and Hyperledger Fabric are popular platforms that utilize blockchain technology for secure transactions and smart contracts (Habib et al., 2022). It focuses on digital signing for verifying license agreements and smart contracts for automating processes. The goal is to reinvent software license management practices for improved security, efficiency, and transparency.

II. LITERATURE REVIEW

Effective software license management is crucial in today's digital. Traditional approaches face challenges such as lack of transparency, inefficient administration, and difficulties in enforcing license agreements. The advent of blockchain technology has generated interest in leveraging its unique characteristics to revolutionize software license management. By harnessing blockchain's capabilities, there is an increasing exploration of its potential to enhance transparency, streamline administration, and improve enforcement mechanisms. This offers new possibilities for transforming software license management practices and addressing existing challenges.

In the realm of license management, there are diverse license managers designed with specific goals in mind. These goals emphasize the need for flexibility to accommodate customer and software vendor preferences when licensing products. Additionally, license managers must address challenges posed by factors such as X-terminals, multiprocessor computers, and the availability of floating or node-locked licenses. Apart from commercially available license managers like SunNet License and FLEXlm, there are also In-House Developed License Managers created by software developers for their own products..(Mirabella, no date) A decentralized online service known as a Dapp, built on the Ethereum platform, leverages blockchain technology to ensure consistency, decentralization, and a consensus mechanism for effective software license management. The service includes a smart contract and user-friendly services that simplify the process of working with the license database, providing a transparent and straightforward experience.(Liubinskyi, Demediuk and Topylko, 2022) Another research introduces

the Bespoke Model, a customized blockchain transaction specification for software license validation. It utilizes additional fields tailored to diverse user and license models. By leveraging blockchain technology, mechanisms such as license upgrades, ownership transfer, and software integrity checks can be implemented, enhancing validation processes and security(Herbert and Litchfield, 2015). The utilization of encryption in blockchain technology enhances its security by making data corruption highly challenging. As a result, extensive research is required to investigate the efficiency, security, and distribution of data within this cryptographic framework. The blockchain's inherent ability to safeguard information through encryption makes it an exceptionally secure medium for transferring and storing large volumes of data.(Gasimov and Aliyeva, 2021).

A. Problem overview of Software license management

1) Software privacy

The idea of "software privacy" refers to the cloning or use of computer software that breaches its licensing requirements. (Mooers1977, n.d.).In developed countries, the level of software piracy level is consistently high at 60%. The total amount of unauthorized licensing was 62.7 billion US dollars. Cloud subscription models were supposed to decrease license violations..(Liubinskyi et al., 2022) Software piracy is defined by the Business Software Alliance (BSA) as the unauthorized copying or circulation of intellectual software, which includes downloading, sharing selling, or installing several copies of licensed software. (Software Management: Security Imperative, Business Opportunity, n.d.) Five types of software privacy:

• End-user piracy, which is the illicit usage of software for personal gain

• Client-Server design, which implies that numerous network users would utilize an application with centralized licensing.

• Internet piracy, which involves obtaining software over the Internet;

• Creating copies of programs from hard drives, which requires the setup of unauthorized software items. Selling personal computers used to be a frequent activity.

• Software fraud, which includes direct copies of software and license duplication.

2) Compliance and License Misuse

Tracking and controlling software inventories, as well as avoiding abuse, overuse, and noncompliance, are all challenges in licensing compliance.

3) Manual and Time-Consuming Processes

Manual software licensing management systems are inefficient and administratively burdensome since they are time-consuming, error-prone, and difficult to scale.

4) License Complexity and Entitlements

Complexity of licenses and entitlements Organizations face challenges, resulting in the under or over-purchasing of software licenses.

5) License Audit and Vendor Compliance

License audits evaluate software vendor compliance, necessitating time-consuming documentation and correct proof of entitlements.

6) Lack of Transparency and Asset Visibility

Organizations need better transparency and real-time insight into software assets and license consumption for informed decision-making and compliance.

7) License Renewals and Expirations

Software interruptions and legal hazards are avoided with proper licensing tracking and management

III. RELATED WORK

A. Software license

Software license validation is a method of verifying that the software license is legal, to prevent the free use of proprietary software. In the case of trial software, software license validation allows the software to remove trial restrictions or unlock. additional features only to available users. (M. Altaie et al., 2020)

B. Examples of popular license verification methods are

1) License key verification

Using a unique alphanumeric code, license key verification confirms the correctness and legality of software products. Packaged software includes installation media, technical manual, and license key for activation and installation (diskette, CD-DVD).

Microsoft Windows and Adobe Photoshop, for example, require a valid license key to activate and authenticate its operating system, Later, the installation disk was replaced by an internet-accessible download link (e.g., Microsoft Office).

2) Online license validation

By comparing the key to a database of sold licenses, online licensing key validation assures unique keys and prohibits unauthorized usage. Software activation is prevented if validation fails.

3) Hardware license validation

Hardware license validation employs a unique record of licensing key and host machine manufacturer, guaranteeing that software is only activated when it has been validated with the publisher.

Modern validation methods have evolved (Digital Signing), with online methods being more secure but still vulnerable to fraud.

IV. BLOCKCHAIN

A blockchain refers to a decentralized ledger system that allows open access to all participants. Notably, once data is recorded within a blockchain, it becomes extremely challenging to modify. A block in a blockchain structure is made up of three parts: data, the block hash, and the preceding block hash. The data kept within a block is determined by the blockchain type, such as Bitcoin, and includes transaction details such as sender, recipient, and coin amount.. Each block possesses a unique hash, which can be compared to a fingerprint. This hash serves as an identifier for the block and its contents. Importantly, any modification made to the block will result in a change in its hash, indicating that the block is no longer the same. In the realm of data access and updating, a notable procedure takes place whereby any modifications are meticulously recorded and validated. Following this, the altered data undergoes encryption to ensure its immutability against subsequent modifications. These modified data entries are subsequently incorporated into the principal records, constituting an iterative process where each change begets a new block. A remarkable feature of this system is the interconnectedness between the original version of the information and its most recent counterpart. Consequently, while the changes made remain transparent to all observers, only the most recent block retains the capability for further modifications(Priyadarshini, 2019). Furthermore, the inclusion of the previous block's hash in each block creates a chain of interconnected blocks, establishing the high level of security associated with blockchain technology.

Blockchains, managed by peer-to-peer networks, provide secure storage for transaction batches through hashing. The healthcare industry recognizes the benefits of blockchain, including data security, anonymity, and integrity. Its decentralized nature eliminates the need for centralized authorities and reduces the risk of fraud and network attacks. The use of smart contracts and immutable ledgers ensures timestamped and secure storage of user information. Blockchain technology also eliminates manual processes, reducing system costs. The cryptographic linked chains enhance transaction speed and security. Overall, blockchain proves to be a feasible solution for securing patient medical records and improving the efficiency of healthcare systems.(Gupta, 2023)

V. PROPOSED WORK

A. Blockchain enable software license management

Blockchain is a technology that already exists and applies in other sectors like Supply chain management and logistics, insurance, and financial services (Fosso Wamba & Queiroz, 2018). Implementing a Blockchain system for software licensing management can increase software license traceability throughout its lifespan. A software license may be tracked from purchase to allocation to decommission - when the program is reused. The ledger (in this example, the license entitlement baseline) is continually updated depending on Blockchain transactions, resulting in a near-real-time picture of available assets and the used assets. Top software producers lack technological mechanisms to prevent software installation without a license (if not effectively handled by the company's SAM or IT functions). By prohibiting software installation when no licenses are available, blockchain systems can reduce over-utilization. Implementing a decentralized, immutable Blockchain system for licensing key authentication can help to avoid non-valid keys such as pirate or vendor-specific internal keys, hence enhancing trust in the used software license market

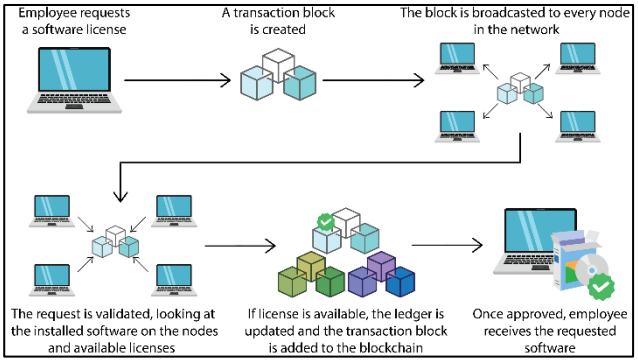

Figure 1: The diagram shows how a software request process and license validation works.

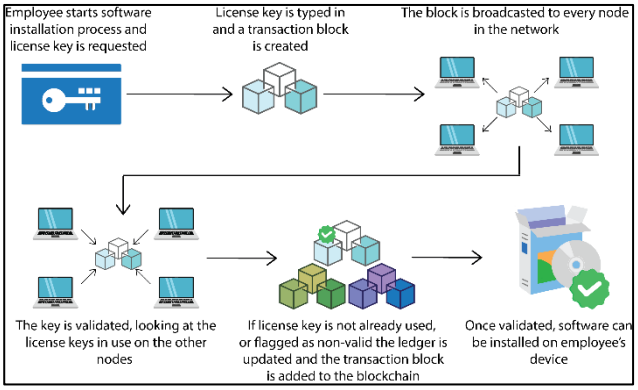

Figure 2: The diagram shows how a software license validation works.

B. Smart Contract

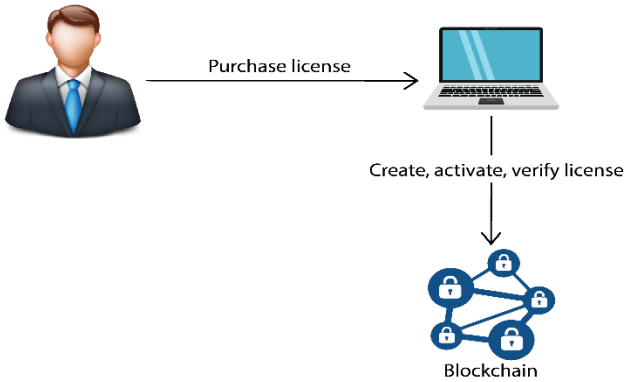

Figure 3: The diagram shows how smart contract works with software license management using blockchain.

An innovative approach for dealing with software licensing in network contexts that enables software suppliers to

transfer license selling, administration, and accounting to smart contracts operating on a permissionless blockchain.(Magnanini et al., 2019)

1) Smart contract in software license management

On a blockchain, smart contracts may be written to enforce license requirements and streamline license-related operations. When a user buys a software license, for instance, a smart contract may automatically validate the payment and activate the license. It may also track license usage and automatically impose limits, such as restricting the number of installations or the length of usage. When the license expires, the smart contract can disable the program automatically. This automation removes the need for manual intervention while also lowering administrative expenses, assuring compliance and effective software licensing management.

C) Digital Signing

The process of verifying the validity and integrity of a document by the sender is known as a digital signature. It encrypts the message with the sender's private key, while the recipient receives the equivalent public key. The sender generates a hash, encrypts it, and delivers it, while the recipient use sender's public key to decrypt the document. The goal of a digital signature is to ensure authenticity rather than security. Digital signatures are necessary to secure the integrity and validity of information exchanged through the Internet by various parties both within and outside of national boundaries (Gamalielsson et al., 2015)

1. Digital signing in software license management

The use of cryptographic techniques to verify the validity and integrity of licensing agreements is involved in digital signature in software license management using blockchain. In other words, a digital signature assures that the licensing agreement is legal and unaltered. It generates a one-of-a-kind digital signature that certifies the identity of the parties involved, such as the software vendor and licensee. The licensing agreements may be securely maintained and accessible by implementing digital signatures into the blockchain, reducing conflicts and increasing confidence. Furthermore, the digital signature allows for a visible and auditable record of licensing transactions, which ensures compliance and streamlines the license management process.

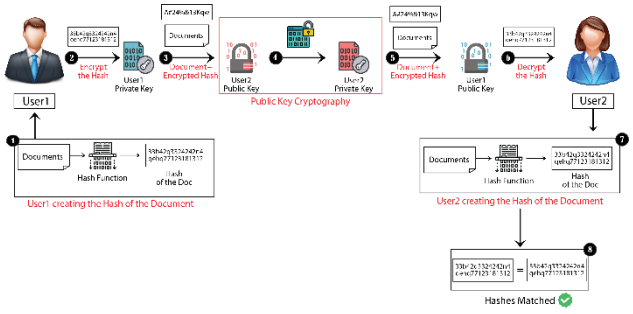

Figure 4: The Digital signing process

The procedure of digital signature validates the validity and integrity of a document by the sender. It encrypts the message and sends it to the recipient using the sender's private key. The document is hashed, encrypted using the sender's private key, then sent. The document is decrypted by the recipient using the sender's public key. guaranteeing that it was sent by the anticipated sender. The goal of a digital signature is to ensure the source of the message transaction rather than security.

User 1 in the figure 4 encrypts the hash and sends it to User 2, who can decode it using User 1's public key. User 2 then computes the hash and compares it to User 1's, guaranteeing that the document and hash are legitimate and have not been tampered with by network attackers. Cryptographic keys, rather than personal information, can be used to identify users, maintaining their privacy.

VI. RESULTS AND DISCUSSION

A. Research Design

As the research methodology Mixed approach research was used and both quantitative and qualitative statistics were used, using standard questionnaires, interviews, documents, surveys, and content analysis.

The first segment of the questionnaire was devoted to demographic statistics and also general information about the software license and blockchain technology of the respondents and the second section was comprised of questions inquiring about the potential benefits of using blockchain. Questioner related questions was pretested with the help of IT related professors who also provided insights into the blockchain technology. We created this questionnaire not only for the software licence vendors but also for customers, IT industry professionals, students and lecturers, etc to get their feedbacks on software license management utilizing blockchain

.

B. Sampling, Data Collection, and Analysis

The questionnaire was created using Google Forms and then shared among software license vendors, various university students, researchers, and lecturers who had been randomly chosen for the questioner. The online distribution strategy used gained up to 216 responses through the social media platforms Instagram, Facebook, and WhatsApp. The questionnaire consisted of 8 simple questions that anybody may answer.

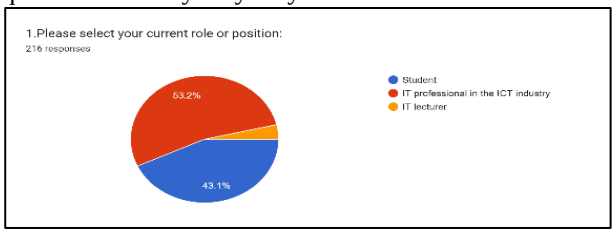

Figure 5. Demographic information

We received many responses from IT experts in the ICT field, which includes software vendors, IT-related organizations, and so on (53.2%), as well as students and lecturers. Since blockchain technology is new, many people are unsure what it is, but based on the responds we

obtained, it was evident that respondents in the IT field are well-versed in blockchain technology. The technology is familiar to 84.3% of respondents. Only 2.8% of the 216 respondents have heard of blockchain technology. 87% of respondents believe that blockchain will be used for licensing management in the software business.

Privacy is the most serious threat in the software industry. Protecting software licenses from intellectual property users is a monumental challenge. The privacy of software license data is more important to software owners.

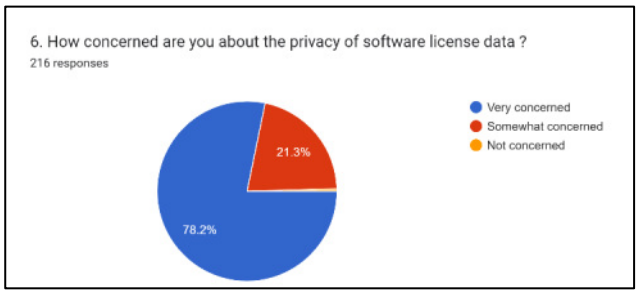

Figure 6. statistics privacy of software license data

96.3% of the respondents believe that blockchain technology can be used to address software privacy and security features

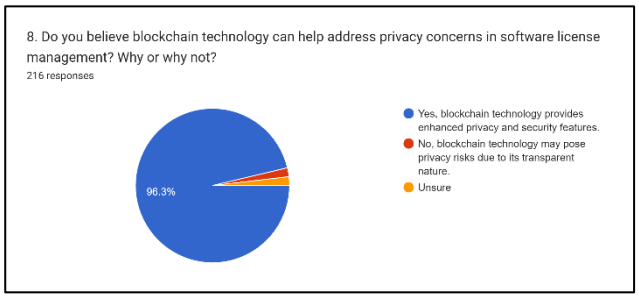

Figure 7. statistics on privacy concerns in software license management

88% of the respondents believe that by using blockchain technology, privacy can be mitigated. 49.5% have selected improved security and tamper-proof licensing records

Table 1. statistics on potential benefits of using blockchain for software license management

Description	Percentage value
Reduction in software piracy	190 (88%)
Increased transparency in license tracking	73 (33.8%)
Improved security and tamper-proof licensing records	107 (49.5%)
Enhanced compliance and license enforcement	72 (33.3%)

The respondents (93.1%) suggests that in order to protect the privacy of software license data on a blockchain that is sensitive should be encrypted for this as a solution we can suggest digital signing. And also 81.9% suggests that strict access control should be imposed for license data.

Table 2. statistics on measures to protect the privacy of software license data on a blockchain

Description	Percentage
Encryption of sensitive data	201 (93.1%)
User consent and control over data sharing	62 (28.7%)
Anonymization of personal information	160 (74.1%)
Strict access controls for license data	177 (81.9%)

According to the responses we received, individuals are more concerned about the privacy of their software licenses. One of the characteristics of software licensing is the ability to copy. This aspect of digital assets makes them vulnerable and defenceless against the circulation of pirate copies without intellectual property licenses. As a result, the privacy of software licensing should be prioritized. Blockchains, smart contracts, and digital signatures may all be utilized to secure digital assets.

VII. CONCLUSION

In conclusion, this research explores the transformative potential of blockchain, digital signing, and smart contracts in software license management. Blockchain technology improves security, trust, and automation in license administration. Digital signing ensures validity and integrity, while smart contracts automate license management. Using blockchain enables immutable records, transparent audits, and better license compliance. Despite challenges like scalability and privacy, these technologies have the power to reshape software license management, enhance security, and optimize resource utilization. Continuous exploration and innovation in this field can unlock their full potential and shape the future of digital licensing practices.

REFERENCES

Fosso Wamba, S., & Queiroz, M. (2018). *International Journal of Information Management Call for Papers (Special Section @IJIM) Theme: Blockchain in the Operations and Supply Chain Management Short Title SI: blockchain i Artificial Intelligence and Big Data in Business and Management View project Data mining: Master degree project View project*.

Gamalielsson, J., Jakobsson, F., Lundell, B., Feist, J., Gustavsson, T., & Landqvist, F. (2015). On the availability and effectiveness of open source software for digital signing of PDF documents.

IFIP Advances in Information and Communication Technology, *451*, 71–80.

Liubinskyi, B. B., Demediuk, M. S., & Topylko, P. I. (2022). Architecture of the License Software Manager using Blockchain technology. *Mathematical Modeling and Computing*, *9*(2), 326–332.

M. Altaie, A., Gh. Alsarraj, R., & H. Al-Bayati, A. (2020). VERIFICATION AND VALIDATION OF A SOFTWARE: A REVIEW OF THE LITERATURE. *Iraqi Journal for Computers and Informatics*, *46*(1), 40–47.

Magnanini, F., Ferretti, L., & Colajanni, M. (2019, September 1). Efficient License Management Based on Smart Contracts between Software Vendors and Service Providers. *2019 IEEE 18th International Symposium on Network Computing and Applications, NCA 2019*.

mooers1977. (n.d.).

Software Management: Security Imperative, Business Opportunity. (n.d.).

Alspaugh, T.A., Scacchi, W. and Asuncion, H.U. (2010) 'Software licenses in context: The challenge of heterogeneously-licensed systems', Journal of the Association for Information Systems, 11(11), pp. 730–755. Available at: https://doi.org/10.17705/1jais.00241.

Gupta, B. (2023) 'Understanding Blockchain Technology : How It Works and What It Can Do Comprendiendo la tecnología blockchain : Cómo funciona y lo que puede hacer', pp. 1–7.

Habib, G. et al. (2022) 'Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing', Future Internet. MDPI.

Gasimov, V.A. and Aliyeva, S.K. (2021) 'Using blockchain technology to ensure security in the cloud and IoT environment', *HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, pp. 0–4.

Herbert, J. and Litchfield, A. (2015) *A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology*.

Liubinskyi, B.B., Demediuk, M.S. and Topylko, P.I. (2022) 'Architecture of the License Software Manager using Blockchain technology', *Mathematical Modeling and Computing*, 9(2), pp. 326–332.

Mirabella, R. (no date) *License Management: How Developers Control Software Licensing*.

Priyadarshini, I. (2019) *Introduction to Blockchain Technology*, *Cyber Security in Parallel and Distributed Computing*.

ABBREVIATIONS AND SPECIFIC SYMBOLS

Business Software Alliance (BSA)

ACKNOWLEDGMENT

A special thanks go to our supervisor, Mr.Ashen Wanniarachchi, for his invaluable assistance throughout this research. Thank you for all your support and feedback during this research. Further, the appreciation goes to all other senior and junior lecturers for their valuable comments and continuous support. Finally, also I would like to appreciate our colleagues for the support they offered us in the completion of this research.

AUTHOR BIOGRAPHY/IES

KAD de Alwis is a Third year information technology undergraduate of faculty of computing, at General Sir John Kotelawala Defence University.

D D Chamindya is a Third year information technology undergraduate of faculty of computing, at General Sir John Kotelawala Defence University.

KR Hettiarachchi is a Third year information technology undergraduate of faculty of computing, at General Sir John Kotelawala Defence University.

Mr.WAAM Wanniarachchi is a lecturer at the Department of Information Technology, Faculty of Computing, General Sir John Kotelawala Defence University. His research field includes Data Engineering and Machine Learning.

Mr. PPNV Kumara is a Senior Lecturer at the Department of Computer Science, Faculty of Computing KDU.His research fields include Information Systems Strategies, Data Science, and Cloud Computing and Virtualization.