IEEE ICBC'24 1570972518

Unlocking Borderless Identity: B-Passport and the Blockchain Revolution

***Abstract*— Blockchain is an emerging technology that has revolutionized various sectors with its decentralized, transparent, and secure nature. It finds applications in cryptocurrencies, finance, and now, we are proposing to integrate it into the current Passport System. Unlike the centralized government-operated system, the B-Passport system will be decentralized, transparent, and governed by a consensus mechanism. It will eliminate the need for physical passports, relying on smart contracts to handle processes securely and efficiently, addressing issues like lost passports, fraud, revocation, and expiration.**

Keywords*— *Blockchain, Passport system, b-passport, Decentralization, Document verification, Trustless system

1. Introduction

Blockchain is a technology which in very little time has earned worldwide recognition. Blockchain technology gained worldwide recognition in 2008 with Satoshi Nakamoto's whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System." It introduced decentralized digital currencies and introduced the concept of blockchain. Applications include integrating passport systems with blockchain technology, as proposed in this paper. The technology has gained widespread interest from teenagers to adults.

Passport systems regulate international travel and ensure security, but face challenges like counterfeiting, fraud, identity theft, and travel delays. To address these, a multi-faceted approach involving advanced security features, international cooperation, technological innovations, and streamlined processes is needed. Electronic passports, also known as biometric passports, incorporate digitized photographic images, fingerprints, and iris data, becoming more prevalent as governments strive for efficiency.

Integrating blockchain with the passport system will be the main motive of our proposed “B-passport” which will lead to the passport system being more flexible, decentralized and secure. This paper will explore the evolution and problems faced in the passport system along with how these problems can be solved. It will give the introduction to the “B-passport" and its implementation on the current passport system.

2. Blockchain and Passport System Ease of Use

2.1. Review of Passport Systems:

The concept of passports can be traced back to ancient times when governing authorities issued documents to individuals traveling beyond their territories. These early versions were primarily used to establish the identity of travellers and provide safe passage. However, the modern passport system as we know it today began to take shape during the early 20th century[1].

With reference to, the International Civil Aviation Organization (ICAO), established by the League of Nations to regulate international air travel, which marked the beginning of standardized travel documents, as a precursor to modern passports[2], [3]. The League of Nations' Passport aimed to streamline the identification process and enhance security during international travel. The First World War and subsequent conflicts prompted governments to tighten border controls and improve passport security. Technological advancements, such as the introduction of biometric identifiers and machine- readable zones, further enhanced the accuracy and efficiency of passport systems.

2.2. Features of Blockchain Technology:

2.2.1. Decentralization:

Decentralization is the distribution of power and decision-making, not concentrated in a central authority. Blockchain employs a distributed system, reducing reliance on a single point of failure and preventing excessive central control.

2.2.2. Transparency:

Blockchain transactions are transparent, with details and history accessible to anyone. They form an unchangeable and chronological chain of linked blocks, ensuring data openness[4].

2.2.3. Autonomy:

Autonomy is a feature of blockchain that refers to the ability of participants within a blockchain network to have independent control over their own data, assets, and actions without relying on centralized authorities or intermediaries. The blockchain system is often described as "trust-less" or "trust-free" since it operates in a peer-to-peer (P2P) manner without the need for a central authority to establish trust[5], [6]. This feature empowers individuals with greater self-governance and sovereignty over their transactions and interactions within the blockchain network.

2.2.4. Security:

Blockchain systems achieve inherent security using asymmetrical cryptography, employing public keys accessible to all and private keys known only to the respective owners[7]. This critical aspect of blockchain technology encompasses a range of measures and mechanisms to safeguard the confidentiality, integrity, and availability of blockchain networks and the data they store.

2.2.5. Immutability:

In the context of blockchain, immutability is the inability to change or alter data that has once been recorded on the blockchain. Once the data has been added to the ledger or the transaction or a block of data is confirmed and added to the blockchain, it becomes nearly impossible to tamper, modify or delete it without the consensus from the validators. In a Blockchain, data blocks are time stamped and encrypted

using hashing algorithms, ensuring that the data remains permanent and secure from tampering unless most nodes or computers in the system approve any changes[8].

2.2.6. Consensus mechanism:

The consensus mechanism in blockchain is responsible for validating transactions and reaching an agreement on their impact on the ledger. It involves participants in the network coming to a consensus regarding the validity of transactions and the overall state of the blockchain. This mechanism ensures that all participants maintain a shared and consistent view of the blockchain, even when facing network disruptions or potential malicious activities[9].
Different consensus mechanisms have been developed, each with its own approach to achieving agreement among network participants. Some of them are listed as follows:

- Proof of Work (PoW):

Proof of Work (PoW) serves as the consensus mechanism in cryptocurrencies like Bitcoin. Miners compete to solve intricate mathematical puzzles that demand substantial computational resources[10]. The first miner to successfully solve the algorithm adds a new block to the blockchain and receives a reward. PoW ensures that the network's computing power remains primarily honest, as it becomes exceedingly difficult for an attacker to control more than half of the computational power.

- Proof of Stake (PoS):

Proof-of-Stake (PoS) is a different consensus mechanism that selects the next block validator based on their stake or ownership of the cryptocurrency. Validators are chosen in a deterministic manner, considering factors like the number or age of coins held. PoS consumes less energy than PoW but maintains security by penalizing malicious or rule-violating validators.

3. BLOCKCHAIN TECHNOLOGY VULNERABILITIES AND ITS SECURITY FEATURES

3.1. Blockchain Vulnerabilities :

While blockchain technology offers many benefits, it is not completely immune to vulnerabilities. Here are some common vulnerabilities associated with blockchain:

3.1.1. 51% attack:

In a blockchain network, a 51% attack happens when a single entity or a group of entities gain control over more than 50% of the network's computational power in a Proof of Work (PoW) consensus mechanism[11]. This control allows the attacker to manipulate transactions, reverse transactions, and potentially double-spend coins. However, for well-established and secure blockchain networks, achieving a 51% attack becomes increasingly difficult as the network grows.

3.1.2. Private Key Vulnerabilities:

Blockchain relies on public-private key cryptography, and the security of the blockchain depends on the secrecy and integrity of private keys[6], [12]. If private keys are compromised or stolen, malicious actors can gain unauthorized access to digital assets and manipulate transactions.

3.1.3. DDoS Attacks:

Distributed Denial of Service (DdoS) attacks can disrupt the operation of blockchain networks by overwhelming the network with a high volume of fake requests or traffic. DdoS attacks can lead to network congestion, transaction delays, and temporary denial of service.

3.2 Block chain algorithm for security:

3.2.1. Hash Function:

In blockchain technology, hash functions play a crucial role in maintaining data integrity and security. These functions are mathematical algorithms that take input of any size and produce a fixed-size output, usually represented as alphanumeric characters[13]. Their primary purpose is to ensure the integrity of data for online or offline transactions. Hash functions are commonly used to verify the authenticity of files downloaded from online sources. One widely used hash function in blockchains is "SHA256." and “Keccak256” which have been rapidly gaining popularity and widespread adoption in various applications.

3.2.2. Digital Signature:

A digital signature is a technique which is used to verify the integrity and authenticity of digital documents. It serves as an electronic equivalent of a handwritten signature or a seal on a physical document. Digital signatures use public key cryptography to provide security and ensure that the signed document cannot be tampered with without detection[14]–[16]. They provide several benefits like integrity, authentication, non- repudiation, efficiency and security. They are widely used in various domains including legal contracts, financial transactions, electronic records, government documents and email communications to establish trust and security in digital interactions.

4. INTEGRATING BLOCKCHAIN WITH PASSPORT SYSTEM

A passport is an authorized travel document issued by a government that verifies an individual's identity and nationality[17]. It acts as proof of citizenship, allowing the holder to travel abroad and enter foreign countries with official authorization.

4.1. Issues with the traditional Passport System

While the current passport system has improved significantly over the years, there are still some challenges and problems that exist. The problems that are faced by the current passport system are as follows:

4.1.1. Document Forgery and Fraud:

Despite the advancements in security features, passports can still be forged or tampered with which poses a significant risk to national security and can facilitate illegal activities such as identity theft and human trafficking[18].

4.1.2. Privacy and Data Protection:

With the increasing use of biometric data in passports, there are concerns about privacy and data protection. Collecting and storing sensitive biometric information raises questions about how securely this data is stored, who has access to it, and how it is used[19].

4.1.3. Inefficient and Lengthy Application Processes:

Many countries face time-consuming and cumbersome passport application processes due to complex documentation, limited appointments, and lengthy procedures.

4.1.4. Limited Accessibility and Coverage:

In some regions, obtaining a passport can be challenging due to limited accessibility to passport offices or processing centers, making it harder for individuals in those areas to obtain a passport.

4.1.5. Physical Document Vulnerabilities:

Even with the integration of electronic features, physical passport documents remain vulnerable to loss, theft, or damage[20]. Losing a passport can be a significant inconvenience for travelers, often requiring time-consuming procedures to replace the document.

4.1.6. Travel Delays and Inconvenience:

Passport systems, particularly during peak travel periods, often face challenges in processing a large volume of travelers efficiently. Insufficient staffing, inadequate infrastructure, and complex bureaucratic processes can result in long queues, delays, and inconvenience for passengers.

4.1.7. Geographic Restrictions:

Centralized passport systems are frequently constrained by physical borders and by certain legal restrictions. For people who travel frequently or must deal with several passport officials in various countries, this might make the procedure more difficult[21].
Efforts are continually being made to address these challenges and improve the passport system's security, efficiency, and accessibility. Governments, international organizations, and technology advancements play a crucial role in implementing solutions to overcome these problems and enhance the overall passport experience for travelers[22], [23].

4.2 Advantages of this Integration:

- Blockchain's inherent security features, such as encryption and decentralized data storage, can make passport information more secure, reducing the risk of data breaches and identity theft.
- Passport data stored on a blockchain would be tamper-proof and verifiable, ensuring the accuracy and integrity of the information.
- Travelers could have more control over their personal information, deciding when and how it is accessed and shared, increasing privacy and data ownership[3], [24].
- Moving passport information to a blockchain could eliminate the need for physical passports, reducing the risk of loss or theft.
- A blockchain-based passport system could facilitate cross-border travel by providing a standardized and easily verifiable identity solution.
- Integrating the Machine-Readable Zone (MRZ) with blockchain can enhance passport data security and reliability, as the blockchain ensures the tamper-proof storage of this critical information, making it less susceptible to unauthorized alterations or data fraud.
- Integrating visa information with blockchain technology can create a secure and transparent system for visa issuance and verification[25], [26]. Blockchain's tamper-proof and auditable nature ensures the authenticity of visa data, reducing the risk of fraud and streamlining the visa application and approval process.

Note: The International Civil Aviation Organization is a specialized agency of the United Nations that sets standards and regulations for international air travel. It plays a crucial role in developing and maintaining global standards for machine-readable travel documents, including passports.
The passport issuing authority is the government entity responsible for issuing and managing passports within a country[27]. It ensures compliance with legal requirements, establishes application procedures, and maintains a centralized passport database for its citizens.

4.3. Contrast Between Passport and B-passport:

	Passport System	***B-passport System***
Definition	A passport system is the administrative framework and processes implemented by a government or authorized authority to issue, manage, and control passports, which are official travel documents used for international travel and	A blockchain-based passport system is an administrative framework that utilizes blockchain technology to issue, verify, and manage passports. It employs the decentralized and transparent nature of blockchain to enhance security, trust, and

	identification purposes.	efficiency in passport issuance, verification, and record-keeping processes.
Modes of working	A traditional passport system is typically centralized, with a central authority responsible for issuing and managing passports.	A blockchain-based passport system operates on a decentralized network where multiple participants collectively validate and maintain the passport records.
Trust and Verification	In a traditional passport system, trust is placed in the central authority to accurately verify and issue passports.	In a blockchain-based system, trust is distributed across the network, as the information recorded on the blockchain is transparent, tamper-evident, and validated by consensus mechanisms.
Data Security	Traditional passport systems rely on physical documents that can be lost, stolen, or tampered with.	In a blockchain-based system, passport data is stored securely on the blockchain, utilizing encryption and cryptographic techniques. The immutability and decentralization of the blockchain enhances the security and integrity of passport information.
Efficiency And Processing Time	Traditional passport systems often involve manual processes, leading to delays and long processing times.	Blockchain-based systems can streamline processes through automation, smart contracts, and digital verification, resulting in faster and more efficient passport issuance and verification.
Accessibility And Inclusivity	Traditional passport systems may have limited accessibility, especially in remote or underprivileged areas	Blockchain-based systems can potentially overcome geographical barriers by providing online access to passport services, enabling individuals to apply and verify their passports from anywhere with an internet connection.
Cost	Traditional passport systems can involve substantial costs, including physical infrastructure, staffing, and administrative expenses.	Blockchain based systems have the potential to reduce costs by eliminating the need for physical paperwork, streamlining processes, and reducing manual intervention.

Table I. Comparing Traditional Passports and Blockchain-Based B-Passports.

4.4. Proposed Model Analysis:

Blockchain is a long chain through which the 'Present Hash' and 'Previous Hash' maintain the immutability of a Blockchain technology.

In our model our chain will be divided in blocks which further would be divided into sub blocks. The division will be as follows:

1.Core Block (Passport Block)
2.Sub Block (Visa Block)
    2.1. Core Block (Visa Block)
    2.2. Sub Block (Entry/Exit Block)

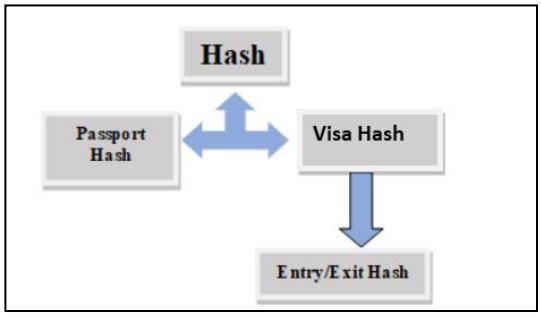

Fig. 5.1. Hashing Division

Our Proposed system will represent a central pillar known as the "Main Chain" or a "Root Chain". This Main Chain is elegantly designed to be a 64-bit block which will contain all the necessary information about the passports and the passport holder. Additionally, this Block will also contain the Private and the Public key pairs where the Private key contained in this block will only be accessible by the passport holders whereas the public key would be accessible by the higher or central authorities.

From this root chain, the system generates two main hashes each serving a unique purpose. The first hash which would be of a 64-bit hash will represent the information pertaining to passport's unique identification, simplifying the process of verifying its legitimacy. Another hash that would be generated will contain a 256-bit hash which will be part of a sub block which contains the visa related information. This in-depth data offers a comprehensive insight into the passport's travel history and visa permissions. This dual-hash architecture enhances both the efficiency and security of our innovative system.

Within the Visa Hash Block, there exists a sub block or a sub hash which would be Entry/Exit hash. Visa, as an official document granting entry, exit, or stay within a specific country, is a crucial component. It is essential to have appropriate Visa before entering a foreign country. Hence our proposed system also contains the information about the Visa which will further simplifies the process of visa issuance alongside the standard passport procedures along with the record for entry and exit[28].

All the blocks in the chain are connected just like the contemporary blockchain system i.e., via the concept of previous and next hash. This is how the chronological order in blocks is maintained[29]. Here, we call the Previous hash as P-hash which serves as the reference for the additional passport information, to maintain a logical and continuous sequence. This chain is further scalable which allows addition of new blocks easily.

In our separate sub-chain, dedicated to Visa-related information, we uphold the concept of chronology, ensuring

that the blocks are interconnected through the V-hash obtained from the previous block within the root chain. Confidential data is protected inside this block more efficiently due to the presence of Sub blocks which in turn controls and effectively manages the Entry and Exit information.
The Entry and Exit Hash (E-hash) that we created in our system, which was the sub hash of visa block, maintains the record of the entry and exit of a person in/out of a country. This block comprises of a 256-bit hash which improves the accountability and openness of travel history as the entrance and departure of passport holders are being recorded and maintained in it. As a result, it becomes effortlessly traceable, and thus, more straightforward to access and verify trip information whenever necessary.
Citizens of certain countries do not need Visa as an authorization to enter another country for a specified amount of time. This privilege is often based on agreements, diplomatic relations, or the perceived low risk of visitors overstaying or violating the terms of their stay. In such cases the Visa hash would no longer be needed for the visit. And hence, the Entry/Exit Hash would act as a sub hash of the root Block instead of acting as the sub hash of the Visa Block, further simplifying the process[30], [31]. Proof of stake consensus mechanism will be used for the verification of the system.
Consequently, our proposed system will render the passport system tamper-resistant, immutable, secure, and decentralized, thus ensuring a rapid, efficient, and secure process. The generation of distinct hashes for Visa and Passport is attributed to the presence of separate blocks, enhancing the overall accountability of our system.
Additionally, the system uses consensus mechanisms and secure smart contracts to maintain data integrity, while access control and authentication protocols provide an additional layer of security. The process is regularly audited and updated, making it highly secure and reliable, thereby ensuring the confidentiality of sensitive data and promoting trust in the system.

5. DISCUSSION

5.1. Different Perspectives with respect to our proposed system:

5.1.1. Passport Holders:

Passport holders have a stake in the proposed blockchain-based system. They benefit from increased data security since their personal information is stored on a decentralized, un-hackable blockchain[32]. Passport holders observe improved data privacy, efficiency, and overall ease of the process. Undoubtedly, the incorporation of smart contracts in the suggested blockchain-oriented passport system has the potential to considerably minimize the duration for validation and simplify the process of acquiring passports. By eliminating intermediaries, they boost swiftness and efficiency in processes.

5.1.2. Visa Applicants:

Visa applicants are necessary to the suggested system. They may use blockchain technology to securely submit their visa applications and supporting documents. The benefit of more transparency for visa applicants is the capability to track the application in real time[33]. The technology makes the visa approval process simpler due to the self-executing smart contracts, perhaps requiring less time and effort.

5.1.3. Immigration Authorities:

Immigration authorities play a significant role in the ecology in this process. The recommended solution provides them with a complete and clear picture of the travel history and the applications[34]. If immigration officials use the blockchain to quickly verify the validity of passport and visa information, they may be able to prevent fraud and illegal entrance more efficiently.

5.1.4. Border Control Authorities:

Border control Authority are in charge of maintaining the integrity and security of borders. The recommended approach gives them access to a reliable and verifiable source of travel related information[31], [35]. By linking to the blockchain, border control authorities may swiftly verify the legitimacy of passports and visas, reducing the risk of fraud and illegal entry. The technology provides real-time data of arrivals and exits, enabling quicker and more accurate border checks.

6. FUTURE SCOPES OF B-PASSPORT:

In future, blockchain-based passport systems might revolutionize identity management, improve security, and simplify administrative procedures.

6.1. Improvements in Security and Privacy:

Blockchain's immutability and encryption make passport data more secure, reducing the risk of identity theft and fraudulent passport issuance[6], [36].
Smart contracts can help to ensure privacy protections while facilitating safe and transparent transactions.

6.2. Straightforward Identity Verification:

Blockchain-based passport systems can streamline the identity verification process, by offering a decentralized and impenetrable method[37]. It can make it possible for confirmed identification data to be shared effectively and securely across suitable parties, eliminating the need for additional verification steps.

6.3. Effective and Unchangeable Records:

A permanent and unchangeable record of passport-related transactions may be provided via blockchain technology, confirming the validity of issuance of passports, their renewals, and other related processes.

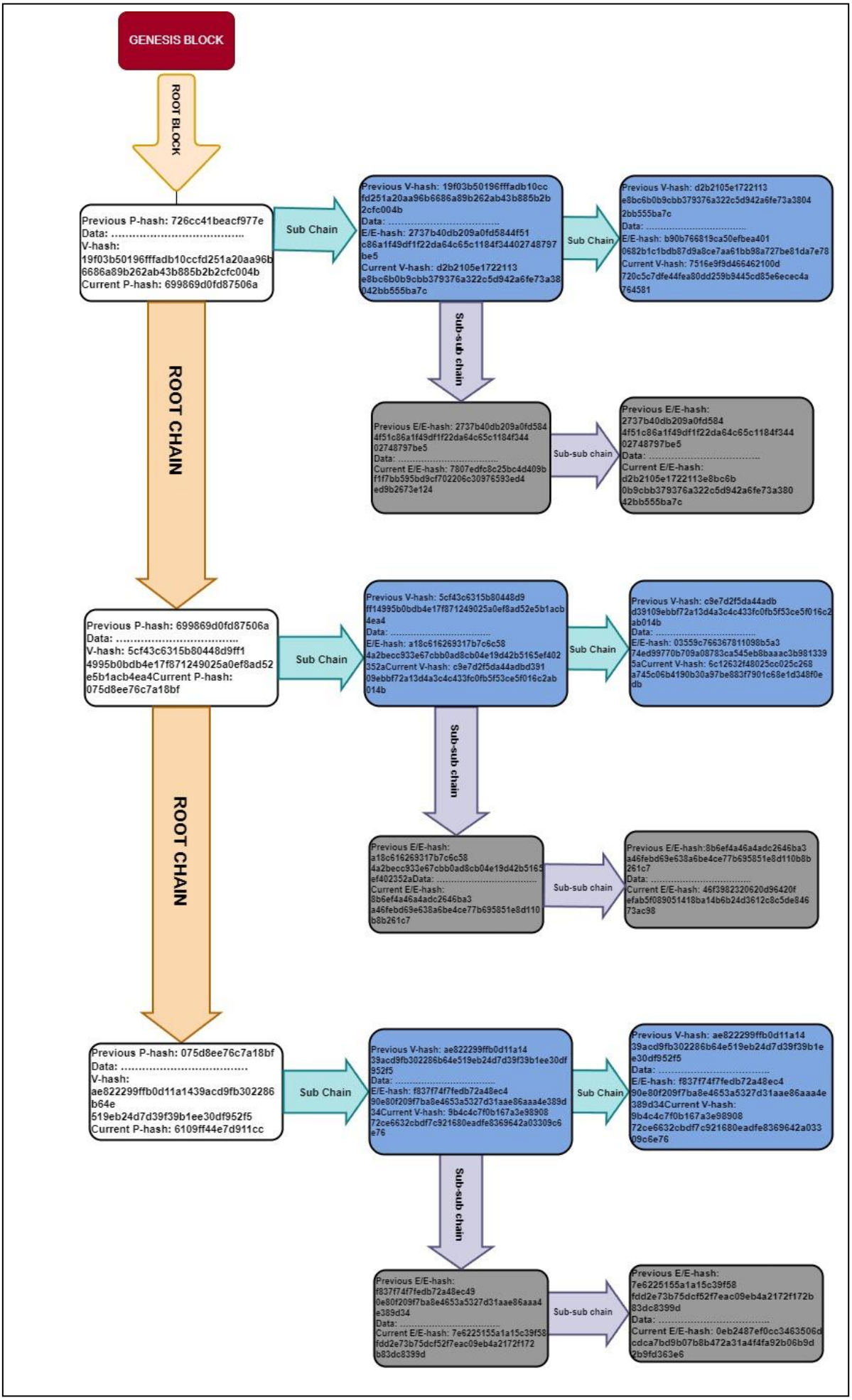

Fig. 5.2. Hashing Model

6.4. Seamless and Interoperable Travel:

Blockchain simplifies identity verification at immigration checkpoints, reducing processing times and improving overall efficiency.

6.5. Individual Empowerment and User Control:

Individuals can have more control over their passport data, deciding when and how it's accessed and shared, enhancing personal privacy.

6.6. Reduced Fraud:

Blockchain's transparency and traceability can significantly reduce passport fraud, as the authenticity of passports and visa records can be easily verified[16], [38].
Passport and visa data stored on a blockchain remains tamper-proof and accurate, ensuring the integrity of the information.

As more countries embrace blockchain-based passport systems, it could lead to a standardized and widely accepted approach to identity verification and travel documentation.

7. CONCLUSION

A decentralized passport system integrated with blockchain technology presents a promising solution to the complexities and risks associated with current day passport systems. By relying on a network of trusted verifiers, smart contracts, and an immutable audit trail, this innovative approach ensures the secure and tamper-proof verification of an individual's identity before granting access to sensitive services or government databases. Each user's digital identity attestations would be signed digitally and stored on the blockchain using a cryptocurrency like Bitcoin, establishing a transparent and reliable record. Through the consensus mechanism, trust is established, offering a decentralized, robust, and efficient alternative for governments struggling to create a secure and dependable centralized passport system.

REFERENCES

[1] M. Saugy, C. Lundby, and N. Robinson, "Monitoring of biological markers indicative of doping: The athlete biological passport," *British Journal of Sports Medicine*, vol. 48, no. 10. 2014. doi: 10.1136/bjsports-2014-093512.

[2] K. Berger, J. P. Schöggl, and R. J. Baumgartner, "Digital battery passports to enable circular and sustainable value chains: Conceptualization and use cases," *J. Clean. Prod.*, vol. 353, 2022, doi: 10.1016/j.jclepro.2022.131492.

[3] I. Atta, E. S. Bakhoum, and M. M. Marzouk, "Digitizing material passport for sustainable construction projects using BIM," *J. Build. Eng.*, vol. 43, 2021, doi: 10.1016/j.jobe.2021.103233.

[4] P. Shen *et al.*, "A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology," in *Proceedings - 2022 IEEE International Conference on Blockchain, Blockchain 2022*, 2022. doi: 10.1109/Blockchain55522.2022.00076.

[5] R. A. Alzahrani, S. J. Herko, and J. M. Easton, "Blockchain Application in Remote Condition Monitoring," in *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*, 2020. doi: 10.1109/BigData50022.2020.9377895.

[6] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2896108.

[7] N. Zahed Benisi, M. Aminian, and B. Javadi, "Blockchain-based decentralized storage networks: A survey," *Journal of Network and Computer Applications*, vol. 162. 2020. doi: 10.1016/j.jnca.2020.102656.

[8] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2. 2021. doi: 10.1016/j.ijin.2021.09.005.

[9] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/9992353.

[10] A. P. Balcerzak, E. Nica, E. Rogalska, M. Poliak, T. Klieštik, and O. M. Sabie, "Blockchain Technology and Smart Contracts in Decentralized Governance Systems," *Administrative Sciences*, vol. 12, no. 3. 2022. doi: 10.3390/admsci12030096.

[11] Z. Jadidi, A. Dorri, R. Jurdak, and C. Fidge, "Securing manufacturing using blockchain," in *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 2020. doi: 10.1109/TrustCom50675.2020.00262.

[12] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9. 2021. doi: 10.1109/ACCESS.2021.3072849.

[13] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7. 2019. doi: 10.1109/ACCESS.2019.2936094.

[14] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for e-health systems," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3022429.

[15] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3062471.

[16] D. Levis, F. Fontana, and E. Ughetto, "A look into the future of blockchain technology," *PLoS One*, vol. 16, no. 11 November, 2021, doi: 10.1371/journal.pone.0258995.

[17] J. Herbert and A. Litchfield, “A novel method for Decentralised Peer-to-Peer software license validation using cryptocurrency blockchain technology,” in *Conferences in Research and Practice in Information Technology Series*, 2015.

[18] T. Alameri, M. N. Hammood, J. K. Mezaal, and B. Eneizan, “E-PAYMENT MODEL FOR THE IRAQI PUBLIC SECTOR: A PASSPORT ISSUANCE E-SYSTEM,” *J. Eng. Sci. Technol.*, vol. 17, no. 1, 2022.

[19] T. Habibu, E. T. Luhanga, and A. E. Sam, “Evaluation of users’ knowledge and concerns of biometric passport systems,” *Data*, vol. 4, no. 2, 2019, doi: 10.3390/data4020058.

[20] Y. Zuo, “Making smart manufacturing smarter–a survey on blockchain technology in Industry 4.0,” *Enterprise Information Systems*, vol. 15, no. 10. 2021. doi: 10.1080/17517575.2020.1856425.

[21] S. N. Yin, H. S. Kang, Z. G. Chen, and S. R. Kim, “Intrusion detection system based on complex event processing in RFID middleware,” in *Proceedings of the 2016 Research in Adaptive and Convergent Systems, RACS 2016*, 2016. doi: 10.1145/2987386.2987397.

[22] U. Odyurt, J. Roeder, A. D. Pimentel, I. G. Alonso, and C. De Laat, “Power passports for fault tolerance: Anomaly detection in industrial CPS using electrical EFB,” in *Proceedings - 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems, ICPS 2021*, 2021. doi: 10.1109/ICPS49255.2021.9468262.

[23] P. F. Scott, “Passports, the right to travel, and national security in the commonwealth,” *International and Comparative Law Quarterly*, vol. 69, no. 2. 2020. doi: 10.1017/S0020589320000093.

[24] K. Bobkowska, K. Nagaty, and M. Przyborski, “Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault,” *IET Image Process.*, vol. 13, no. 13, 2019, doi: 10.1049/iet-ipr.2019.0072.

[25] A. Razzaq, S. A. H. Mohsan, S. A. K. Ghayyur, N. Al-Kahtani, H. K. Alkahtani, and S. M. Mostafa, “Blockchain in Healthcare: A Decentralized Platform for Digital Health Passport of COVID-19 Based on Vaccination and Immunity Certificates,” *Healthc.*, vol. 10, no. 12, 2022, doi: 10.3390/healthcare10122453.

[26] W. O. Larkotey, J. Effah, and R. Boateng, “Development of e-passport application portal: A developing country case study,” in *Proceedings ot the 21st Pacific Asia Conference on Information Systems: “‘Societal Transformation Through IS/IT’”, PACIS 2017*, 2017.

[27] A. Atanasiu and M. I. Mihailescu, “Biometric passports (ePassports),” in *2010 8th International Conference on Communications, COMM 2010*, 2010. doi: 10.1109/ICCOMM.2010.5509095.

[28] Y. Cheng and H. Shaoqin, “Research on blockchain technology in cryptographic exploration,” in *Proceedings - 2020 International Conference on Big Data and Artificial Intelligence and Software Engineering, ICBASE 2020*, 2020. doi: 10.1109/ICBASE51474.2020.00033.

[29] C. Cachin, S. Schubert, and M. Vukolić, “Architecture of the Hyperledger Blockchain Fabric,” in *Leibniz International Proceedings in Informatics, LIPIcs*, 2016.

[30] O. Sonmezturk, T. Ayav, and Y. M. Erten, “Loyalty Program using Blockchain,” in *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, 2020. doi: 10.1109/Blockchain50366.2020.00074.

[31] A. B. Jeng and L. Y. Chen, “How to enhance the security of e-passport,” in *Proceedings of the 2009 International Conference on Machine Learning and Cybernetics*, 2009. doi: 10.1109/ICMLC.2009.5212583.

[32] Y. Mulyana, “Efforts of Counterfeiting Criminal Acts Passport Identity,” *Int. J. Educ. Vocat. Stud.*, vol. 2, no. 8, 2020, doi: 10.29103/ijevs.v2i8.2761.

[33] S. Vaudenay, “E-Passport Threats,” *IEEE Secur. Priv.*, vol. 5, no. 6, 2007, doi: 10.1109/MSP.2007.164.

[34] M. Bivand Erdal and A. H. Midtbøen, “‘Birthplace unknown’: on the symbolic value of the passport for identity-construction among naturalised citizens,” *Identities*, vol. 30, no. 1, 2023, doi: 10.1080/1070289X.2021.1933827.

[35] A. Juels, D. Molnar, and D. Wagner, “Security and privacy issues in E-passports,” in *Proceedings - First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005*, 2005. doi: 10.1109/SECURECOMM.2005.59.

[36] H. Guo and X. Yu, “A survey on blockchain technology and its security,” *Blockchain Res. Appl.*, vol. 3, no. 2, 2022, doi: 10.1016/j.bcra.2022.100067.

[37] C. A. Shoniregun *et al.*, *Securing biometrics applications*. 2008. doi: 10.1007/978-0-387-69933-2.

[38] R. T. Moreno, J. Garcia-Rodriguez, J. B. Bernabe, and A. Skarmeta, “A Trusted Approach for Decentralised and Privacy-Preserving Identity Management,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3099837.