Blockchain-Based National Digital Identity Framework – Case of Palestine

Firas Abu Hasan*, Huthaifa I. Ashqar*, Anas AlSobeh†, Omar Darwish‡
*Arab American University of Palestine, Palestine
Email: huthaifa.ashqar@aaup.edu
†Information Technology, Southern Illinois University Carbondale, Carbondale, IL, USA
Email: anas.alsobeh@siu.edu
‡GameAbove College of Engineering & Technology, Eastern Michigan University, Michigan, USA
Email: odarwish@emu.edu

***Abstract*—Digital technologies' emergence has promised a transformative era in identity management. This thesis presents a holistic exploration of a blockchain-based national digital identity framework designed to meet the unique needs and challenges of the Palestinian context. The proposed model leverages blockchain's security and decentralization to create a secure, user-centric, and multi-purpose platform for identity management. Through an in-depth analysis of identity proofing, authentication, authorization, and assurance levels, the model offers a holistic approach to identity management. Users are equipped with digital wallets to store, manage, and control access to their identity information, fostering user empowerment and data privacy. The proposed model's scalability, modular architecture, and adherence to open standards ensure seamless integration with diverse entities, overcoming occupation-related limitations and managing financial costs. at the same time, strict compliance with data privacy and cybersecurity standards reinforces user trust. Offline access options, such as quick response (QR) codes, bridge infrastructure gaps, and enhance customer experience. The model facilitates the digital economy, ease of access to government services, financial inclusion, and environmental conservation, and extends services to Palestinians in the diaspora. In a world increasingly reliant on digital identities, this thesis proposes a model that not only meets the demands of the digital age but also addresses the unique challenges of the Palestinian context. Doing so provides a robust foundation for secure and inclusive digital identity management in Palestine and offers valuable insights for similar contexts worldwide.**

***Index Terms*—Blockchain, Digital Identity, Self-Sovereign Identity, Authentication, Identity Proofing, Decentralized Systems, Cryptographic Protocols, Data Privacy, Identity Management, Governance Frameworks,**

I. Introduction

By 2022, approximately 60 percent of the global gross domestic product (GDP) had been Digitalized [1]. In Palestine, there is a notable interest from the public and private sectors in expanding digital services to meet the growing demand. However, the rapid digitalization and increased electronic services adoption necessitate a deeper understanding of how individuals are identified and verified in the Digital Era. Consequently, governments and regulatory authorities must focus on establishing robust digital identity systems that facilitate people's access to digital services and create a more comprehensive representation in this digital landscape.

Digital identity serves as a critical enabler for accessing services in the digital realm, paralleling physical identification in tangible environments [2] [31], while facilitating digital growth and engagement in contemporary digital life [3] [32]. As the cornerstone for digital service development [4], digital identity empowers individuals to fully engage with the digital ecosystem and capitalize on opportunities presented by the digital era, enhancing their participation in the evolving digital landscape [33].

As the demand for digital services continues to rise, it becomes imperative for Palestine to address the issue of digital identity and work towards establishing a comprehensive and secure national digital identity system. This system will not only enhance the accessibility of digital services for its citizens but also contribute to the overall growth and advancement of the country in the digital age [22].

This research aims to explore the options for establishing a secure and inclusive digital identity system in Palestine. Given the exploratory nature of the study and the need to gain in-depth insights and contextual information, a qualitative research approach is employed. According to Yin [5], the qualitative approach can be used in four situations, one of which is when the study is focused on addressing "what" and "how" questions, like in our case. The study employs purposive sampling to select participants with relevant expertise and knowledge on digital identity systems and their potential implementation in Palestine. The target participants include: (1)Government Officials: Representatives from relevant ministries and agencies including: The Palestine Cabinet, Ministry of Telecommunications, Ministry of Interior Affairs, and The Palestine Monetary Authority, who are involved in digital infrastructure and identity management will be invited to provide insights on the policy and regulatory aspects of the Digital Identity system. (3) Technical Experts: Professionals with expertise in digital identity technologies and cybersecurity will be included to understand the technical requirements, challenges, and potential solutions.

II. Literature Review

Digital Identity has received significant attention for its potential to revolutionize digital services and digital trans-

979-8-3503-5469-0/24/$31.00 ©2024 IEEE

formation. The author has explored various aspects of digital identity, including: Makoto Takemiya [4] proposed A potent electronic identification solution that empowers users to retain complete control over their personal information, enabling them to selectively share information with specific services. Through the implementation of a decentralized infrastructure model, Blockchain technology has the potential to realize a self-sovereign identity paradigm, wherein individuals assume authority over their own data. Quinten Stokkink [6] presented A digital identity solution rooted in Blockchain technology is presented. This solution, unlike traditional systems reliant on a single trusted third party, attains the status of a legally recognized identity akin to a passport. It operates on a versatile provable claim framework, necessitating the collection of attestations from third-party sources to establish truth. Notably, this claim model is designed to be agnostic, accommodating various Blockchain structures and proof methods. The study demonstrates four distinct implementations that uphold both the Blockchain structure and proof method agnosticism, delivering rapid performance for claim creation and verification, often within fractions of a second. This comprehensive approach combines the strengths of Self-Sovereign Identity, legal validity, and efficient performance.

Nutthakorn Chalaemwongwan in his paper [7] demonstrated The Thailand National Digital ID Framework built on Blockchain (NIDBC) was showcased as an effective solution to enhance government digital identity services. It simplified the user experience through a seamless single sign-on process while upholding privacy. Under this framework, individuals retain control over their personal information, granting permission for its disclosure to specific services only when deemed necessary. Mühle, Grüner, Gayvoronskaya, Meinel [8] gave an overview of The SSI concept represents a new approach in digital identity management, underpinned by the transformative potential of Blockchain technology. This novel approach encompasses four integral components, fundamentally altering traditional Identity Management registration procedures. In this context, the author delves into authentication solutions, emphasizing the pivotal role of verifiable claims when interacting with relying parties. Furthermore, the discussion encompasses verifiable claims solution, considering both on-chain and off-chain options, each accompanied by its unique set of advantages and drawbacks. Reza Sultani [9] in his paper harnessed the potential of Hyperledger Indy, a distributed ledger technology (DLT) with both public and permissioned attributes, as the foundation for constructing a digital onboarding framework firmly rooted in the principles of SSI. This innovative framework represents a significant stride in mitigating the shortcomings prevalent in contemporary KYC procedures and conventional identity management paradigms. Moreover, it demonstrates a commitment to adhering to the principles of SSI, Privacy by Design, and compliance with the General Data Privacy Regulations (GDPR).

Buccafurri, Lax , and Russo [11] discussed the issue of pseudo-anonymity within the Blockchain landscape was effectively tackled through a novel proposition, which integrates the concept of public digital identity with Blockchain technology by means of Identity-Based Encryption. The authors not only conceptualized this solution but also demonstrated its practical implementation in a real-world case study. Geoff Goodell [12] discussed an electronic identity, which can be used in cyberspace that considers human rights, and providing individuals with capabilities to handle their individual al information in a variety of ways in a variety of situations, by creating numerous unrelated identities. Md Sadek Ferdous [13] in his article conducted a thorough examination of the necessary properties for a SSI system and assessed its influence on the Laws of Identity. It also shed light on the crucial lifecycles within an Identity Management System and demonstrated how the concept of SSI can be integrated into these lifecycles. Additionally, the author provided detailed scenarios and flows depicting the utilization of self-sovereign identity with Blockchain technology across various facets of an Identity Management System. This article marks a significant and pioneering academic exploration into the realm of self-sovereign identity.

Jingxuan Li [15] devised an assessment framework to gauge international involvement in the realm of decentralized identity. As a case study, the author scrutinized the United States to assess the existing state of development and engagement on the global stage concerning decentralized identity, examining it from a multifaceted perspective. Furthermore, the author offered insights and suggestions for other nations seeking to bolster their participation in the decentralized identity domain. Moreover, a review was conducted for other industry publications from regulators and international organization who are specialized in the scope of work in this paper as follows: Organization for Economic Co-operation and Development (OECD) released a report in 2011 [16] that gives a detailed analysis for national strategies and supporting policies for identity management systems in 38 countries worldwide. The Sovrin Foundation published a paper [17] In 2016, a comprehensive study was conducted to delve into the technical underpinnings of the Sovrin identity network. This study was aimed at providing insights and understanding to Internet architects, analysts, and developers. It particularly focused on demonstrating how the Sovrin architecture effectively realizes a distinctive blend of a public Distributed Ledger Technology (DLT) for self-sovereign identity. This DLT operates through presmission nodes that are overseen by a global non-profit foundation. The World Bank Group published in 2016 [31] that gives guidelines for the Digital Identity Onboarding, and publication [18] in 2021 that discusses the European Commission digital identity framework in terms of ID4D "digital identity 4 dimensions" coverage, acceptance, usage and user friendly. NIST digital identity guidelines [19] published in 2017 give guidelines for digital identity implementation in many aspects including the digital identity lifecycle management, risk management, assurance level, and federation considerations.

Access now organization article [20] (Digital-Identity-Paper-2018-05) published in 2018 discusses concerns related to digital identity systems in terms of governance, data privacy,

and cybersecurity [10]. Arab Monetary Fund (AMF) published a paper [21] in 2020, that gives detailed outlines for regulatory authorities in the Arab region on implementing digital identity systems and electronic know your customer (KYC). European Committee of Experts on the evaluation of AML measures and the financing of terrorism [33], Government of New South Wales (NSW) published in 2021, an identity strategy that covers many strategic directions including; identity management, related crimes, identity enablers, and identity initiatives. The European Union Agency for Cybersecurity (ENISA) report [22] in 2022, The report conducted a comprehensive and critical evaluation of the existing literature, providing an in-depth analysis of the current technological landscape concerning Self-Sovereign Identity (SSI) and other conventional identity solutions. It explored the emerging standards, communities, and pilot projects that are actively contributing to the advancement of SSI solutions. the report adopted a broad perspective on decentralized electronic identity, encompassing various architectural components and governance mechanisms. It also conducted an extensive examination of the security implications associated with SSI, with a particular focus on cross-border interoperability, mutual recognition, and technology neutrality. These aspects were assessed in alignment with the regulatory requirements stipulated by eIDAS regulations. After analyzing the above literature, the following gaps were identified: (1) The majority of the studies are pure academic studies that analyze concepts, propose development and enhancement, address challenges and so on, but very few applied research studies were found that employ technology in a practical use case. (2) Very few studies were found that addressed the national-level identity management system. (3) No studies were found that address providing a framework for digital identity in Palestine.

III. Model for a Blockchain-based National Digital Identity System

Figure 1 shows the main model components: Central Blockchain Network: At the core of the system lies a central blockchain network. This blockchain serves as the backbone of the digital identity ecosystem, storing encrypted identity records, and transaction data. It ensures the immutability, transparency, and tamper-resistance of identity-related information. Digital Wallet: To provide users with control over their identities. This user-centric interface allows individuals to securely store, manage, and control access to their digital identity information. Identity Proofing Service: To establish the authenticity of individuals, a robust Identity Proofing Service need to be in place. This service conducts a range of identity verification processes, including basic proofing, enhanced proofing which is sometimes referred to as Know Your Customer (KYC), and securely stores the verified information in the Digital Wallet. Authentication Service: The Authentication Service is responsible for verifying users' identities when they access services or applications within the ecosystem. It offers multiple authentication methods, including biometric authentication (fingerprint, facial recognition), mobile device authentication (push notifications, QR codes), and one-time passwords (OTP) for added security. Authorization Engine: Managing access control is critical to safeguarding sensitive identity data. Our Authorization Engine employs Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) mechanisms. Additionally, it includes a Consent Management module that allows users to grant or revoke access permissions to specific entities.

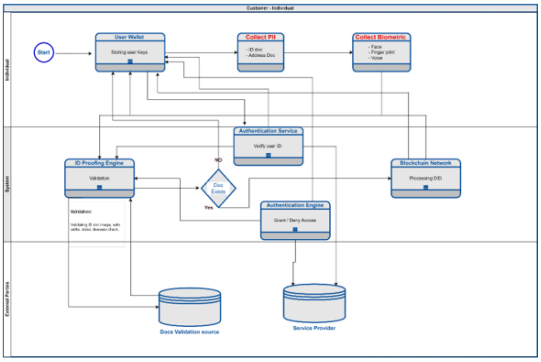

Fig. 1. The proposed model layout

A. Identity Proofing

Identity proofing also known as identity verification and authentication, is the process of confirming the identity of an individual or entity [28]. It involves collecting and verifying various types of information, such as Personal Identifiable Information (PII) as biometric data [26] [34] [35], government-issued documents, and other evidence, to establish the subject's identity. This section demonstrates the identity-proofing requirements and options that will be provided by the proposed model. Figure 2 shows the ID proofing flow.

National ID systems are created to support a diverse array of sectors and a variety of services or applications, each with its unique requirements. Hence, different applications require varying levels of assurance. maintaining the right balance between security and privacy is essential to maintain suitable room as per the need, for instance, Id proofing for financial services may require higher level of authenticity compared to other services like IP proofing for online subscription for forum or library and so on. However, Higher IP levels require more rigorous verification processes, potentially leading to more complexity in the system design. While achieving higher IP levels can sometimes involve complex processes, impacting the user experience. Hence, striving for user-friendly solutions is important.

Identity proofing involves a spectrum of assurance levels, each indicating the extent to which an individual's identity has been verified. These levels often referred to as Identity Proofing Levels (IP levels), play a crucial role in establishing trust and enabling secure interactions within decentralized ecosystems. The following are the different levels of identity proofing and their significance in the proposed model. Identity Proofing Levels: (1) Identity Proofing Level 1 (IP1) represents

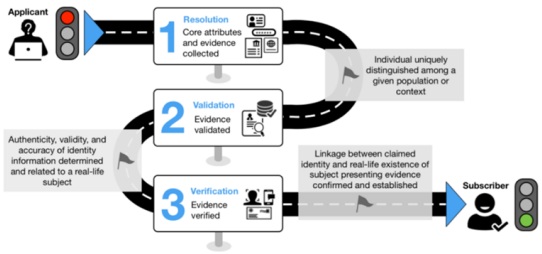

Fig. 2. ID Proofing process

the basic level of identity proofing, focusing on minimal verification [29]. It involves collecting and verifying information that is easily accessible and doesn't require extensive verification. This level is suitable for scenarios where a low level of trust is acceptable, such as accessing publicly available information. (2) Identity Proofing Level 2 (IP2) indicates a moderate level of identity proofing [29]. It involves more thorough verification, including checks against official documents and databases. This level is suitable for situations where a higher level of trust is required, such as online services that involve financial transactions. (3) Identity Proofing Level 3 (IP3) signifies a high level of identity proofing and assurance [29]. It involves comprehensive verification through multiple sources, including government-issued identification, biometric data, and third-party verification. IP3 is suited for critical applications with high-security requirements, such as accessing sensitive medical records or managing legal documents. With these diverse options, the model can accommodate various services while maintaining an appropriate level of security and privacy tailored to the specific service or application. This approach reduces complexity, ensuring a seamless user experience while upholding data protection standards.

B. Authentication

Figure 3 Authentication is the process of confirming the identity of an individual or entity seeking access to a system, service, or resource [30]. It is a critical aspect of information security and involves validating that the claimed identity is legitimate [8]. Authentication relies on various factors or components to establish identity securely. These factors fall into three main categories: (1) Something You Know: like passwords, PINs, and personal questions [8]. (2) Something You Have: like keys, tokens, and mobile devices[54]. (3) Something You Are: like Biometrics includes facial recognition, voice recognition, fingerprints, and iris scans [8]. This demonstrates the innovative authentication methods that will be implemented within the proposed model. These methods aim to enhance security, privacy, and efficiency while ensuring the integrity of identity data. The following proposed authentication methods offer a robust framework for identity verification and access control. Within the proposed model, "something you know" includes secret information held exclusively by the legitimate user. This involves a "passphrase" used to create cryptographic keys tied to DIDs. Which is normally used for transaction signing and authentication. Incorporating "something you have," the proposed model leverages private cryptographic keys stored on the user's digital wallet. This factor enhances trust by verifying the user's ownership of the keys. The authentication process will combine DID ownership with cryptographic proofs from Verifiable Credentials. While cryptographic authentication forms the core, the proposed model will also embrace "something you are" through biometric data integration. Biometrics like fingerprints or facial recognition serve as trust-enhancing elements while preserving privacy, this contributes to user verification, augmenting trust in a secure and privacy-conscious manner.

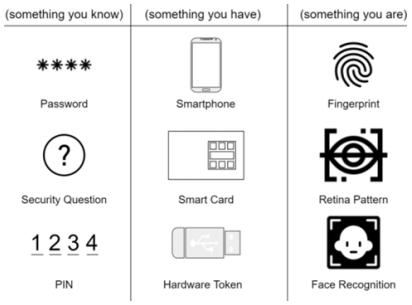

Fig. 3. ID Proofing process

C. Authorization

Authorization refers to granting or denying access to specific resources, services, or data based on the verified identity of the requesting party [30]. Authorization forms the cornerstone of secure access control for identity systems, dictating what actions individuals or entities are permitted to undertake based on verified identities. The proposed model will leverage cryptographic capabilities including verifiable credentials (VCs) and decentralized identifiers (DIDs) to enhance access control while prioritizing user-centric control and data privacy. The proposed model may allow for traditional authorization options associated with the authentication factors mentioned above such as using passwords, OTP, and biometric attributes for some use cases. However, it introduces new novel concepts, which are "Authorization of the Presenter" and "Authorization of the Purpose" [25].

Authorization of the Presenter is a novel concept that involves verifying the presenter's identity and authority to share specific attributes. Verifiable credentials include information about the presenter's authenticity, empowering the system to assess the presenter's trustworthiness. Authorization of the Purpose validates the intention behind access requests. Verifiable credentials are augmented with the purpose of access, ensuring resources are accessed for legitimate reasons only.

Incorporating these new concepts will enhance authorization methods such as Attribute-Based Access Control (ABAC). Initially, verifiable credentials validate user attributes, while "Presenter" and "Purpose" refine who can present and for what reason. Additionally, verifiable credentials become dynamic access tokens, injected with "Presenter" and "Purpose." This involves the concept of "who is presenting" and "why,"

facilitating nuanced access control. Moreover, authorization policies, driven by distributed ledgers, incorporate "Presenter" and "Purpose." These policies not only verify the identity but also assess the presenter's legitimacy and the purpose behind access requests. The advantages can be summarized as follows:

1) Enhanced Access Control: Integrating "Authorization of the Presenter" and "Authorization of the Purpose" creates a comprehensive access control model, enhancing security and user trust.
2) Contextualized Access: Purpose-driven access ensures that resources are accessed only for genuine, authorized reasons, mitigating potential misuse.
3) Enhanced Accountability: By validating both presenter and purpose, decentralized systems heighten accountability, minimizing unauthorized access.

1) Level of Assurance: Figure 4 shows the Level of Assurance (LOA) is a measure of the confidence or trustworthiness in the identity verification and authentication processes used in a digital identity system [29]. It helps determine how reliable and secure an individual's digital identity is within the system. Assurance levels are typically categorized into different tiers, with higher levels indicating a stronger and more rigorous verification process. These levels are commonly used in digital identity systems and can vary from one system to another, but they generally assess the risk and security associated with an individual's identity.

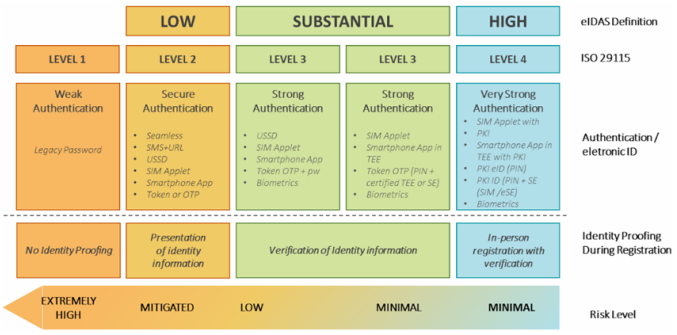

Fig. 4. Level of Assurance

In our model employs a tiered approach to the level of assurance (LOA) associated with digital identities. The model will support the following LOA tiers:

- Weak assurance identities are suitable for basic online services that do not involve sensitive data such as subscriptions to forums. Users at this level undergo weak authentication mechanisms and may use a username/password. No ID proofing is required for this tier.
- Low assurance identities are employed for services requiring a higher degree of trust such as online shopping. Secure multi-factor authentication like OTP or tokens can be used for this tier. Presenting an ID is required as part of the ID proofing process for this tier.
- Substantial assurance identities are reserved for critical services, such as government interactions or financial transactions. Users undergo strong authentication that includes multiple factors such as biometric authentication and OTP. Extensive identity proofing is required for this tier, including verification of ID information and liveness checks.
- The proposed model will not accommodate this tier due to challenges including hardware requirements and proofing requirements.

D. Advantages of the Proposed Model

1) **LoA Alignment to Business Needs:** LOA aligns with the trust requirements of specific applications, ensuring the application of suitable security measures without undue restrictions.
2) **User-Centric Flexibility:** The proposed model empowers users to present authentication credentials aligned with the required LOA, adapting to the context of use.
3) **Contextual LoA:** varies based on context, for example, a financial transaction might necessitate LOA 3, whereas accessing general content could require LOA 1.
4) **Balancing Complexity and Security:** Stronger LOAs necessitate robust authentication methods, striking a balance between security and usability. Authorization within the LOA hierarchy ensures resource access only by authenticated and authorized entities.

E. Security Protocols and Controls in Digital Identity Systems

Digital identity systems rely on robust security protocols and controls to safeguard user data and ensure reliable authentication. Cryptographic protocols form the foundation of these security measures. The Distributed Public Key Infrastructure (DPKI) enables asymmetric encryption for secure communication and authentication, while digital signatures ensure the authenticity and integrity of transactions. Hash functions, particularly SHA-256, play a crucial role in maintaining data integrity throughout the system.

Data protection and privacy are paramount in digital identity systems. Blockchain technology provides immutable data integrity, ensuring that records cannot be altered without consensus. Sensitive data is protected through encryption, and pseudonymity is employed to reduce exposure of personally identifiable information. Zero-Knowledge Proofs (ZKPs) enable selective disclosure of identity information, allowing users to prove specific attributes without revealing unnecessary details. Furthermore, consent-based data sharing empowers users to control access to their personal information.

Figure 5 shows authentication measures that are enhanced through Multi-Factor Authentication (MFA), which requires multiple forms of verification. This can include mobile authentication, where users receive one-time codes on their devices, biometric authentication using fingerprints or facial recognition, and security tokens. By combining these factors, the system significantly reduces the risk of unauthorized access.

Governance in digital identity systems encompasses the entire lifecycle of a digital identity, from enrollment and creation to management, presentation, and verification. Key stakeholders in this process include issuers, holders, and verifiers, each

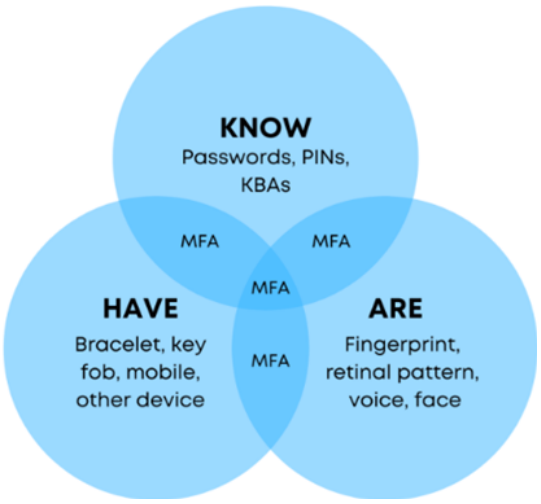

Fig. 5. Multi-Factor Authentication and attributes

with distinct roles and responsibilities. Issuers verify identities, generate cryptographic keys, and issue credentials. Holders manage and present their digital identities, while verifiers validate presented identities and make access decisions, as shown in Figure 6.

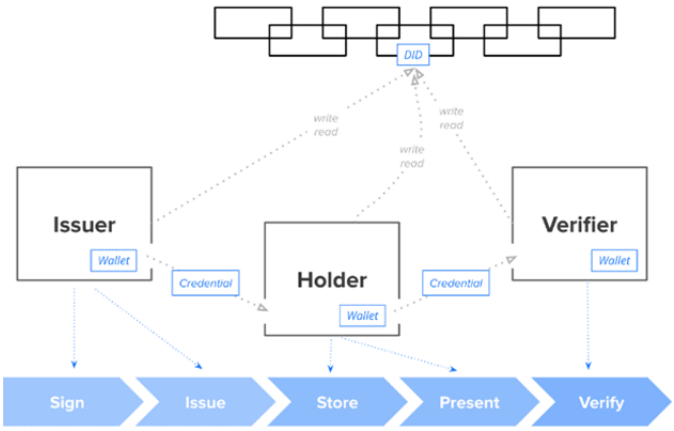

Fig. 6. Governance framework

The consensus mechanism is a critical component of the blockchain-based digital identity system. After careful consideration of various options, Proof of Stake (PoS) has been chosen for its balance of security, scalability, and efficiency. This mechanism allows for a more energy-efficient and potentially more decentralized approach compared to alternatives like Proof of Work.

Adherence to international standards is crucial for ensuring interoperability and reliability of digital identity systems. Several organizations contribute to these standards, including ISO, NIST, and ETSI. ISO standards such as ISO/IEC 29100 and ISO/IEC 24760 provide frameworks for identity verification and management. NIST Special Publication 800-63 offers comprehensive guidelines on identity proofing and authentication. ETSI standards focus on trust services and identity proofing requirements. Additionally, the W3C's Web Authentication API and the Decentralized Identity Foundation's work on Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) are shaping the future of decentralized identity management.

Financial considerations are a crucial aspect of implementing a national-level digital identity system. Studies suggest that for low-income countries, the initial establishment could cost approximately 0.6% of GDP, with ongoing annual costs of 0.06–0.1%. Key cost categories include human resources, identity credentials, IT infrastructure, physical establishments, enrollment equipment, and information, education, and communication initiatives. The actual costs can vary significantly based on system design choices and country-specific factors. For a country like Palestine, a detailed analysis considering these factors within the local context would be necessary to provide an accurate cost estimation.

IV. Evaluation and Discussion

To evaluate the proposed blockchain-based national digital identity system for Palestine. The assessment is based on insights gathered from interviews with government representatives and cybersecurity experts, revealing the current digital identity landscape, ongoing initiatives, and specific needs and challenges in the Palestinian context.

Interviews highlighted several ongoing initiatives in Palestine's digital identity ecosystem. These include the Ministry of Telecommunication's efforts to establish governance frameworks and introduce a supervisory body for the sector, the implementation of single sign-on solutions for 'Hukumati' to enhance user access to government services, the 'X-road' initiative designed to promote interoperability among government entities, and the Palestinian Monetary Authority's (PMA) plans for a financial sector-specific identity system. These insights are crucial for implementing the proposed system in a way that avoids duplication and optimally utilizes existing infrastructure in Palestine.

Through these interviews, key needs and challenges were identified. The needs encompass facilitating the digital economy, ensuring ease of access to government services, promoting financial inclusion, providing a smooth customer experience, extending services to Palestinians in diaspora, and addressing environmental concerns. Challenges include integration with diverse entities, occupation-related limitations, financial costs, lack of expertise and awareness, data privacy and security concerns, and infrastructure requirements.

The proposed model effectively addresses these identified needs and challenges. In terms of facilitating the digital economy, the model offers secure online identity verification, enabling e-commerce transactions, online banking, and digital financial services. It facilitates integration with payment platforms, reducing reliance on cash and encouraging digital financial transactions. For government services, it implements Single Sign-On (SSO) solutions, minimizing paperwork and manual processes, thus streamlining bureaucratic procedures and enhancing service efficiency.

To promote financial inclusion, the model simplifies the process of opening bank accounts and accessing financial products, particularly for underserved populations. It aids in assessing creditworthiness and verifying eligibility for government aid programs. The customer experience is enhanced through user-centric design principles influenced by Self-Sovereign Identity (SSI), offering various authentication options including multi-factor authentication (MFA) and biometric capabilities.

For Palestinians in the diaspora, the model enables access to consular services, educational resources, and cultural institutions remotely, fostering connections with homeland institutions. Environmental concerns are addressed by digitizing processes, reducing paper usage and transportation-related emissions. The use of software digital wallets and Proof of Stake (PoS) consensus mechanism contributes to a more sustainable system.

In addressing the challenges, the model adheres to international standards and applies open standards to ensure interoperability with diverse entities. It leverages Distributed Public Key Infrastructure (DPKI) technology and software wallets, eliminating reliance on hardware that could be subject to border control restrictions. QR technology is integrated for offline authentication to mitigate occupation-related limitations.

Financial limitations are addressed through the use of cost-efficient blockchain infrastructure and open-source software. The model is designed for scalability and suggests public-private partnerships and international funding opportunities. To bridge expertise gaps, the model proposes training programs and capacity-building initiatives in collaboration with international firms specializing in blockchain technology and identity management.

Data privacy and security concerns are tackled through robust encryption techniques, decentralized architecture, user consent mechanisms, and immutable audit trails. The model adheres to regulatory standards such as eIDAS, NIST, and ISO. Infrastructure limitations are addressed by leveraging both blockchain and cloud computing technologies to provide a robust, scalable, and flexible infrastructure.

The proposed system would have varying impacts on different stakeholders. For individuals, it offers enhanced control over personal information, reduced risk of identity theft, and streamlined access to services. Businesses can benefit from efficient user onboarding, enhanced security, and potential cost savings, although they may face integration costs and interoperability challenges. Government entities can expect improved governance and transparency, more efficient public services, and reduced fraud, but may need to invest in infrastructure and establish regulatory frameworks. The overall ecosystem could see improved interoperability and stimulated innovation in identity management solutions, though stakeholders may face resistance to change, necessitating awareness campaigns and education initiatives.

V. Conclusion and Future Work

The proposed blockchain-based national digital identity system for Palestine demonstrates significant potential in addressing key needs and overcoming substantial challenges within the country's unique context. This innovative approach offers promising solutions to facilitate the digital economy, ensure ease of access to government services, promote financial inclusion, enhance customer experience, extend services to the Palestinian diaspora, and address environmental concerns. However, the success of this system hinges on careful consideration of implementation strategies. Particular attention must be given to areas such as integration with existing systems, regulatory compliance, and public acceptance. The complexities of the Palestinian context, including occupation-related limitations and infrastructure challenges, necessitate a nuanced and adaptable approach to implementation. As the digital identity landscape continues to evolve, it is crucial to remain adaptable and responsive to emerging technologies and changing user needs. The proposed system lays a foundation for a more secure, efficient, and user-centric approach to identity management in Palestine, with the potential to drive socio-economic development and enhance overall well-being.

As we look ahead, it becomes imperative to consider quantitative approaches for future research and development in the realm of blockchain-based national digital identity systems. Future work could involve comprehensive quantitative assessments of user experience metrics. This would include conducting surveys and usability testing to quantify aspects such as system accessibility, response times, and overall user satisfaction. The resulting empirical data will be invaluable in refining and enhancing the user-centric design of the system. A thorough cost-benefit analysis using quantitative methods will provide stakeholders with a clear understanding of the economic implications of the system. This should include measuring the return on investment, cost per user onboarded, and the broader economic impact of the system on various sectors of the Palestinian economy. Quantifying the adoption rates of the blockchain-based national digital identity system among different demographic groups and sectors will be instrumental in understanding its reach and effectiveness. Additionally, assessing the impact of outreach initiatives through quantitative measures, such as increased registrations or reduced identity fraud, will provide valuable insights for future strategies. A quantitative comparison between the proposed blockchain-based system and traditional identity management systems will provide empirical evidence of its advantages. Metrics for this analysis could include processing times, security incident rates, and overall system reliability. Developing and implementing quantitative metrics for assessing the security and privacy aspects of the system will be crucial. This could involve measuring the frequency and nature of security incidents, the effectiveness of privacy-preserving features, and the system's resilience against various types of attacks. Conducting rigorous performance tests under various load conditions will be essential to ensure the system

can scale effectively. This involves quantifying factors such as transaction throughput, latency under different network conditions, and system capacity. Quantitative studies on the system's interoperability with other digital identity systems, both within Palestine and internationally, will be crucial for ensuring its long-term viability and usefulness in an increasingly connected world. By employing these rigorous quantitative methodologies, researchers can contribute valuable insights and data-driven recommendations. This approach will ensure the continuous evolution of the blockchain-based national digital identity system, keeping it aligned with emerging technological trends and user needs. As the digital identity landscape continues to evolve, such quantitative research will be instrumental in refining and optimizing the system, ultimately enhancing its effectiveness and impact on Palestinian society.

REFERENCES

[1] A. Regional and F. Working, "Digital Customer On-Boarding, e-KYC and Digital Signatures In The Arab Region," no. 139, 2020.

[2] N. Naik and P. Jenkins, "Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity," Proceedings of 2020 7th IEEE International Conference on Behavioural and Social Computing, BESC 2020, 2020, doi: 10.1109/BESC51023.2020.9348298.

[3] P. Tammpuu and A. Masso, "Transnational Digital Identity as an Instrument for Global Digital Citizenship: The Case of Estonia's E-Residency," Information Systems Frontiers, vol. 21, no. 3, pp. 621–634, 2019, doi: 10.1007/s10796-019-09908-y.

[4] M. Takemiya and B. Vanieiev, "Sora Identity: Secure, Digital Identity on the Blockchain," Proceedings - International Computer Software and Applications Conference, vol. 2, pp. 582–587, 2018, doi: 10.1109/COMPSAC.2018.10299.

[5] R. K. Yin, "Case Design and Methods," American Psychological Association., pp. 3–24, 2003.

[6] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1336–1342, 2018, doi: 10.1109/Cybermatics.

[7] N. Chalaemwongwan and W. Kurutach, "A Practical National Digital ID Framework on Blockchain (NIDBC)," no. June, pp. 497–500, 2019, doi: 10.1109/ecticon.2018.8620003.

[8] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," Comput Sci Rev, vol. 30, pp. 80–86, 2018, doi: 10.1016/j.cosrev.2018.10.002.

[9] R. Soltani, U. T. Nguyen, and A. An, "A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger," Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree, pp. 1129–1136, 2018, doi: 10.1109/Cybermatics_2018.2018.00205.

[10] A.M.R. AlSobeh, K. Gaber, M.M Hammad, et al. Android malware detection using time-aware machine learning approach. Cluster Comput (2024). https://doi.org/10.1007/s10586-024-04484-6

[11] F. Buccafurri, G. Lax, A. Russo, and G. Zunino, "Integrating Digital Identity and Blockchain," vol. 11229 LNCS. Springer International Publishing, 2018. doi: 10.1007/978-3-030-02610-3_32.

[12] G. Goodell and T. Aste, "A Decentralized Digital Identity Architecture," Frontiers in Blockchain, vol. 2, 2019, doi: 10.3389/fbloc.2019.00017.

[13] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," IEEE Access, vol. 7, no. 1, pp. 103059–103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[14] A. Alsobeh and A. Shatnawi, "Integrating data-driven security, model checking, and self-adaptation for IoT systems using BIP components: A conceptual proposal model," in *International Conference on Advances in Computing Research*, Cham: Springer Nature Switzerland, May 2023, pp. 533–549.

[15] J. Li and Y. Jing, "Establishing an International Engagement Model of Digital Identity Based on Blockchain," Mobile Information Systems, vol. 2022, pp. 1–7, 2022, doi: 10.1155/2022/6988211.

[16] OECD, "National Strategies and Policies for Digital Identity Management in OECD Countries," OECD Digital Economy Papers, no. 177, 2011.

[17] D. Reed, J. Law, and D. Hardman, "The Technical Foundations of Sovrin," no. September, p. 26, 2016.

[18] E. Commission, "The European Digital Identity Framework," 2021.

[19] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines.(National Institute of Standards and Technology, Gaithersburg, MD)," NIST Special publicaiton 800-63-3, vol. 58, no. 2, pp. 130–137, 2020.

[20] Aggarwal, Ben-Hassine, and Chima, "National digital identity programmes: what's next?," Access now, no. May, pp. 2–38, 2018.

[21] C. Issued, "Arab Regional Fintech Working Group Digital Identity and e-KYC Guidelines in the Arab Region Arab Monetary Fund," no. January, 2020.

[22] A. AlSobeh, "OSM: Leveraging Model Checking for Observing Dynamic behaviors in Aspect-Oriented Applications," arXiv preprint arXiv:2403.01349, 2024.

[23] A. M. AlSobeh, S. AlShattnawi, A. Jarrah, and M. M. Hammad, "Weavesim: A scalable and reusable cloud simulation framework leveraging aspect-oriented programming," Jordanian Journal of Computers and Information Technology, vol. 6, no. 2, 2020.

[24] M. Naghmouchi, H. Kaffel, and M. Laurent, "An automatized Identity and Access Management system for IoT combining Self-Sovereign Identity and smart contracts," pp. 1–13.

[25] K. H. Kim, S. Lim, D. Y. Hwang, and K. H. Kim, "Analysis on the Privacy of DID Service Properties in the DID Document," in International Conference on Information Networking, IEEE Computer Society, Jan. 2021, pp. 745–748. doi: 10.1109/ICOIN50884.2021.9333997.

[26] L. Bathen et al., "SelfIs: Self-sovereign biometric IDs," in IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, IEEE Computer Society, Jun. 2019, pp. 2847–2856. doi: 10.1109/CVPRW.2019.00344.

[27] G. Goodell and T. Aste, "A Decentralized Digital Identity Architecture," Frontiers in Blockchain, vol. 2, Nov. 2019, doi: 10.3389/fbloc.2019.00017.

[28] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," Comput Secur, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102050.

[29] M. Da Silva and A. Pardo Vegezzi, "Author: Marcos Allende López (@marcosallendeL) SELF-SOVEREIGN IDENTITY The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain," 2020.

[30] 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, pp. 171771–171783, 2020, doi: 10.1109/ACCESS.2020.3022429.

[31] A. M. R. AlSobeh and A. A. Magableh, "BlockASP: A Framework for AOP-Based Model Checking Blockchain System," IEEE Access, vol. 11, pp. 115062–115075, 2023, doi: 10.1109/ACCESS.2023.3325060.

[32] O. Darwish, C. M. Stone, O. Karajeh, and B. Alsinglawi, "Survey of educational cyber ranges," in *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020)*, Springer International Publishing, 2020, pp. 1037–1045.

[33] A. A. E. Momani, M. O. Bani Yassein, O. Darwish, S. S. Manaseer, and W. Mardini, "Intelligent Paging Backoff Algorithm for IEEE 802.11 MAC Protocol," Netw. Protoc. Algorithms, vol. 4, no. 2, pp. 108–123, 2012.

[34] M. Elkhodr, E. Gide, O. Darwish, and S. Al-Eidi, "BioChainReward: A Secure and Incentivised Blockchain Framework for Biomedical Data Sharing," International Journal of Environmental Research and Public Health, vol. 20, no. 19, p. 6825, 2023.

[35] A. Shatnawi and S. Clyde, "Modeling Personal Identifiable Information using First-Order Logic," in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, October 2018, pp. 1–10.

[36] A. M. J. H. A. Shatnawi, "Estimating Accuracy of Personal Identifiable Information in Integrated Data Systems," M.S. thesis, Utah State University, 2017.