I.J. Information Engineering and Electronic Business, **2023, 4, 13-25**
Published Online on August 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2023.04.02

Towards a Novel Identity Check Using Latest W3C standards & Hybrid Blockchain for Paperless Verification

Samiur Rahman Khan*
American International University-Bangladesh/Faculty of Science and Technology (FST), Dhaka, 1229, Bangladesh
E-mail: samiurk70@gmail.com
*Corresponding Author

Md. Al-Amin
American International University-Bangladesh/Faculty of Science and Technology (FST), Dhaka, 1229, Bangladesh
E-mail: alamin@aiub.edu

Received: 28 September, 2022; Revised: 26 October, 2022; Accepted: 11 November, 2022; Published: 08 August, 2023

Abstract: With the advent of W3C standards such as DID, VCs, and DPKI beyond 2020, the industry has reached a new level where a technological infrastructure overhaul is possible. By employing blockchain and other Decentralized Ledger Technologies, it is believed that we can eliminate the requirement for paper-based verification. Researchers are aware of the technological components we possess at present and are trying to bring forth their sets of POCs. Additionally, governments ranging from developing to developed countries are taking industrial initiatives that incorporate these technologies. This research also evaluates the latest events and cases to find the need for paperless verification. Previous development conducted in the domains of Information Systems and Public forensics has presented us with various issues at both infrastructural and user levels. It also introduced us to the presence of lots of gaps present that can be improved with a more improvised form of decentralized paperless solution. Researchers have pointed out that the modern day identity check and forensic solutions will face difficulties with blockchain compatibility, since most of those previous components will require built-in integration with a decentralized environment. As the latest researches suggest the key to this integration is now possible with the proper application of the W3C standards. In this paper, we propose an architecture that interlinks the latest decentralized W3C standards with a permissioned blockchain for implementing paperless verification and identity check.

Index Terms: World Wide Web Consortium(W3C), Decentralized Identifier(DID), Verifiable Credentials(VC), Decentralized Public Key Infrastructure(DPKI), User Management Agency(UMA), Blockchain, Decentralized Infrastructure

1. Introduction

With the advent of recent technologies there has been global incentives to improve overall infrastructural systems. Some of which need to be adjusted for the purpose of improving upon the problems that are already inherent in it. To understand this we can have look at the most common infrastructural aspects subjected to issues like cross-border verification, Identity management, and secured authentication. Administrative preferences regarding such cases have more or less been dealt with through centralized means for technological measures. But in recent years with technologies like blockchain, Peer to Peer networks, Decentralized Systems, etc. It is possible to undertake a whole new measure for the benefit of international public verification for traveling and border crossing. Judging by current events as of the year 2022, two of the most devastating events that are unfolding before the world are the wars & the refugee crisis. The people who have gone through these two events in most cases fail to have such identification documents and verification information. In the worst case, they fall victim to unprecedented events. However, the main question that remains the same now is, "What is the use of the information being digital if people cannot be verified digitally?”. At present, it is a necessity for people to have access to physical means like documentation for the assessment of their verification. In order to update this infrastructural process to a fully governed digital system with utmost security is possible with the addition of the latest technologies. If we look at the current processing that most countries possess. It is evident that public identification is being maintained by means of national identity papers & passports. But in both developing and developed countries the government is trying to digitize this process. They are doing this through the introduction of electronic passports and digital identifications also termed as electronic identity(eID) [1].

Lots of algorithms and systems have been generated for the purpose of digitization of identification, one among them is RSA and Elliptic Curve Digital Signature Algorithm (ECDSA), which are used to verify the authenticity and integrity of digital documents. Also Hash-based signatures, such as Merkle signatures, are used to prove the authenticity of a large data structure or file by providing a short, fixed-size proof. In order to provide proof of possession of specific information to verifiers without revealing the actual information to the verifier, technologies such as Zero-knowledge proofs like zk-SNARKs and zk-STARKs are implemented. One of the most common globally recognized Identity solutions is biometric authentication which utilizes technologies such as facial recognition, fingerprint scanning that can confirm the identity of an individual. Research is ongoing in the Blockchain use cases so that we can use distributed ledger technology to ensure the immutability and authenticity of public identification. ~ existing sols

But even with application of these existing solutions, it doesn't solve the problem of dependency on paper based documents. Moreover it raises issues regarding shortcomings of these existing systems. The foremost shortcoming is the lack of standardization. Different countries and organizations have different identification and verification systems, which can make it difficult for individuals to use their identification across different systems. In many cases it is observed that public identification and verification systems are vulnerable to hacking and other forms of cyber attacks, which can lead to the loss of personal data and identity theft. The typical case in all verification centers is that people need to physically have access to identification documents. Even though their data are in the records of the government's public database. The accessibility limitation occurs as identity verification needs to be committed by means of cross-matching the documents which are either machine-readable or have an electronic chip in them [1]. This process raises concerns regarding situations where people are not in possession of such documents. Which will result in them falling into dire circumstances? For newcomers the Public identification and verification systems can be slow and inefficient, causing delays and long wait times for individuals trying to access services. Also some individuals, such as those who are homeless or live in rural areas, may not have the necessary documentation to obtain a government-issued identification. This can prevent them from accessing essential services and benefits. Also in most cases, these documents can be forged illegally for fake verification and smuggling purposes [2]. Privacy cases are also considered since Public identification and verification systems collect and store large amounts of personal data. ~limitations

In order to overcome such limitations, the present day public verification system leverages solutions like Risk-based authentication, Blockchain-based verification, Regular System Audits and Public-private partnerships. It is evident that the scope of such technologies as blockchain in recent years had a huge boost in terms of sustainability, affordability & scalability [3]. There are now ways to integrate the application of blockchain domains in sectors of Human resources & Public Management. The complex means of making this integration a possibility was due to the latest achievement made in the last few years. Industry-leading blockchains like Hyperledger Fabric, Ethereum, Avalanche, Cardano, Chainalysis KYT, Hyperledger Sawtooth, and many more have become more accessible for development [4]. Due to the availability of resources and dApp compatibility with centralized architectures. Most of these blockchains have different network types needed for respective industrial and business applications. This leads us to the option for the earliest undertaking of renovating the verification process using the most suitable hybrid blockchain [4,5]. All of the problems mentioned earlier point out the root cause which can be identified as Identification data handling. Something that can now be easily assessed with use of latest W3C standards like DID, VC and DPKI. This leads us to the main aim of this research which is to construct a framework based on blockchain and W3C components to provide a standardized global outline for governments to follow. Although achieving a paperless verification system in the form of digital ID has been implemented in few countries. But at the infrastructure level it has yet to receive success. This is also another objective of this research and we hope to achieve it through an in-depth analysis and the demonstration of our noble architecture.

2. Related Works

Work on verifying public identification has a profound history. The process started immediately after the events of World War I, through a passport standard [1]. During World War 1, most European countries proceeded with border document checks for security reasons. This form of document would then be used to identify people with their skills and occupations. This was issued back in the 1920s by the League of Nations [1]. One reason for this process was to control the number of immigrants being admitted to different countries. This process was seemingly revised after 1947 with designs and layouts that would suit and identify 42 separate nations. The initial passports were said to have included biological traits among people, like facial features, hair color, etc. This happened to provide the authorities with much-needed bioinformatics. for feasible authentication [7,8]. However, as technology progressed, we were introduced to modern ways of dealing with public verification. Since the early 2000s, governments have had new means to fetch records, crosscheck identifiers, and authenticate better bioinformatics [1]. This provided the world with the first outline of a framework for Public Identity Verification that is still in modification today.

Although we live in an increasingly digital world, Sanket Panchamia and Deepak Kumar Byrappa's research demonstrates that passports are still physical documents. It is kept on hand at all times, much as other necessary travel documents like visas and immigration stamps [8]. Information on a person's arrival and exit from a country is stored in a database designed for that country. This piece laid the groundwork for the widespread adoption of electronic passport, visa, and immigration form processing. Digitalization has the potential to simplify and standardize processes, including issuing, renewing, and canceling passports and VISAs, as well as checking and confirming them. This research demonstrated the importance of data storage needed for the Public Identity system. Inorder to improve the storage mechanics we suggest a distributed ledger-based system which can help to track and retrieve information about similar processes. Once in place, this framework would facilitate the elimination of the need for superfluous, time-consuming verification of personal information. It will also allow the prevention of the use of fake papers like passports and visas.

Another research conducted by Loi Luu, et al showcased that adopting a distributed ledger technology, such as blockchain, would reduce the complications associated with paper-based verification, while also streamlining processes and increasing efficiency—all of which might result in savings [31]. The findings of a study by Kenta Sekiguchi et al. add weight to those of the preceding authors. Based on their findings, it's clear that the advantages of Distributed Ledger Technology (DLT), such as fault tolerance and cost savings, are garnering a lot of interest [2]. Both of these research on blockchain technology shows the necessity of a framework that can allow paperless verification to be a possibility.

In 2017, the Bank of Japan commissioned a series of seminars on DLT in securities settlement and produced a report summarizing the outcomes. For accurate securities settlement, it examined how DLT interacts with the Act on Book-Entry Transfer of Corporate Bonds and Shares, that controls paperless securities. The paper provided multiple interpretations of existing legislation. That later on mandated a multi-layered settlement structure which in light of DLT's fault tolerance qualities allowed network members to communicate information. The authors also examined the present legal framework in light of DLT's prospects in securities settlement [2]. This research backed a claim on how DLT based systems can coherently work with multi layered data sets which can as well be applied on Public Identity Verification systems.

Bo Tang et al contributed to developing a noble concept of the IoT Passport with blockchain usage in their research. According to the authors, the number of "things" will very quickly surpass that of humans in the very near future [9]. Cross-platform collaboration helps improve the user experience since user requirements and vendor offers are always shifting over time. Trust that is centralized makes it more difficult to be flexible and to scale. IoT Passport offers trust between different platforms using blockchain technology [9]. The offering of trust and the source of security plays one of the most vital roles in any infrastructure which this research justified.

Dongjuan Na et al. focused on data security of IoT devices which are vulnerable to multiple instances of attacks and points of failures. Their research offers blockchain-based access management for the Internet of Things and edge computing, in addition to incorporating platform and user preferences [32]. Marco Verissimo Oliveira proceeded to develop a conceptual architecture for a passport ledger [10]. According to their research, the author asserts that blockchain and other distributed ledger technologies are the most effective means of protecting customer data. Multiple blockchains were analyzed to ensure that the intended effort will not compromise user privacy. Permissioned blockchains that employ an authorization abstraction layer are the most effective at regulating the conduct of uniquely recognized people. This study demonstrated Hyperledger Fabric's platform development feasibility [10]. Regarding India's rising population, Ambica Sethy and Abhishek Ray conducted a thorough review by validating digital certificates and other documents [13]. They utilized blockchain's inherent safety characteristics to secure private information during verification. The suggested approach uses a unique hash key for validation and verification. The proposed framework encrypts the hash key with Argon2. This will show who accessed a document when limiting document misuse [13]. These three papers suggest the use of blockchain for any ideal platform so that it can have vulnerability and privacy protection.

When it comes to the concept of paperless Prof. Dr. Hong Xue deeply reviewed the legal frameworks for the protocols and proceedings [11]. In his work, it was discussed how the Framework Agreement(FA) actually revolves around different international organizations under the laws of already established articles [11]. V. N. Kustov and E. S. Silanteva debated the veracity of paperless exchanges. Their work focuses on using reliable data for decision-support systems. Different technologies, laws, and administrations make cross-border data validation difficult [12]. Cross-border data networks can help. Trust technologies facilitate worldwide electronic data exchange. They reviewed how TTP technology for the cross-border document can transfer and analyze three validation techniques (DVCS, XKMS, and OASIS DSS). The study further discusses the hardware and software components of TTP implementation as a package, illustrating effective cross-border electronic legal document flow [12]. From these researches we can assess that when it comes to global electronic data exchange any standardized platform would need to have cross-border network support. Along with an established license that can support its proper functionality.

3. Key Terminologies

3.1. DLT:

DLT refers to the protocol stack and underlying architecture that enables immutable record-keeping on a distributed network where several parties have real-time access to the data and can make modifications as necessary. It is a method for ensuring that a distributed database operates efficiently. To avoid authority abuse in a decentralized system, a third party is unnecessary. DLT employs a tried-and-true method of encryption to safeguard data during storage. A physical key or a digital signature may be used to unlock any given piece of data. The gathered information is recorded irrevocably and is subject to the network's regulations [4,14].

3.2. Decentralized Infrastructure:

The decision-making authority in a Decentralized Infrastructure rests with each department or unit. Instead of relying on a single, centralized system, each division will have its own means of data processing, analysis, and administration. This suggests they function adequately without a centralized server. Since there appears to be no overarching administration, it's possible that data will need to be standardized to the technologies used by other departments in order for them to connect with one another. A huge organization, like a governmental institution, may benefit from this in the not-too-distant future. However, as data and software consumption continues to rise, it is crucial to develop a regulatory body to prevent unnecessary spending on activities like data inventory, data landscaping, and compliance. To "decentralize" an architecture means to have each section or branch run its own central computer [15].

3.3. DPKI:

The distributed identity system strongly relies on the decentralized public key infrastructure supporting it. Blockchain facilitates DPKI by providing a reliable and immutable record for the distribution of identity holders' asymmetric verification and encryption keys. Using a decentralized public key infrastructure, anybody may generate and store cryptographic keys on the immutable, chronologically arranged Blockchain. These keys can be used by third parties to validate digital signatures and decode material for the correct identity holder [16].

3.4. Verifiable Credentials:

It is a standard that establishes a method for expressing these types of credentials on the Web in a cryptographically secure, privacy-preserving, and machine-verifiable manner. Validated credentials may reflect the same data as physical credentials. Adding technology like digital signatures makes verifiable credentials more secure and trustworthy than physical credentials. Holders of verifiable credentials may create and share verifiable presentations which verify to demonstrate their credentials. Verifiable credentials and verifiable presentations may be provided quickly, making them more convenient than actual credentials for establishing confidence remotely [17].

3.5. Decentralized Identifiers:

The concept of a Decentralized Identifier (DIDs) is determined by the controller of the DID and can be anything like a person, organization, item, data model, abstract entity, etc. Instead of being tied to centralized databases, identity providers, and certificate authorities, DIDs have been designed to be detached. Instead of relying on others to help find information about a DID, the design lets its owner verify authority over it on their own, without the need for anybody else's consent. It is possible to have secure interactions between a DID person and a DID document through the use of DID URIs. Cryptographic content, verification techniques, and services may all be expressed in DID documents, giving DID controllers the tools they need to demonstrate control over DIDs. The DID subject's trustworthy interactions are enabled through services. If the DID subject is an information resource, such as a data model, the DID may provide a way to return the actual DID subject [18].

3.6. Issuer & Verifiers:

Public Validation is a core fundamental for security and trust that enables authentication, identity verification, encryption, and non-repudiation in e-governance. In order for e-government services to be available across international boundaries, a security infrastructure must be implemented that can ensure a consistently high level of service for all parties involved. Issuers are considered government-certified bodies who hold a claim to provide authentic forged documentation to the public. Verifiers, on the other hand, are the department/agency that is in charge of validating the documented credentials [19].

3.7. Paperless:

Paperless is formed from the eradication of all paper documents. However, when we say "Paperless Validation," we refer to the usage of identification without a paper-based medium. It is an electronic process in which document production, execution, and review are all performed digitally, and validation checks are performed via software, allowing real-time data to be concurrently stored and tracked [6].

4. Case Study

4.1. Country-wise Overview of Public Management with Blockchain

Around the world different countries have already set up the initial starting phase for blockchain implementation in major sectors of their infrastructural systems. However, it has been indicated by recent reports that in the upcoming years we may see the global GDP top up by a huge margin through the application of the blockchain domain [30]. All such analytical research does serve as tools that are currently motivating developed to under-developed countries to bring forth blockchain for their own benefits. In order to do so, they are currently engaged in developing the foundational approaches for their projects [22,30].

4.1.1. Lebanon:

For managing banking facilities we have observed that Lebanon wishes to adopt distributed baking through administrative procedures. As of 2021, the Lebanese CBDC project has demonstrated how the Lebanese population can act as a community for empowering the functionality of digital money which acts as an alternative to their local currency lira. So far they have managed to identify and retain public information and maintain a central ledger for the national bank to function the monetary transactions [28].

4.1.2. Estonia:

Estonia was the first nation in the world to promote a national-level e-voting system. Going through their development phases it was pretty clear that the ballot services, public interaction, and public identifiers were all maintained in a government ledger but it was public for people to see. They were able to do this using only public national ID or Nationality documents for people over 18 years old. The management on the blockchain level followed a less complicated approach where the smart contracts were responsible for only dealing with three parameters at the same time. Moreover, the Estonian government has issued a blockchain policy in e-residency where public validation can be conducted through a city-level blockchain architecture [27].

4.1.3. United Kingdom:

In the constant fight against identity fraud and scams the regional authority of the United Kingdom has been issuing execution of blockchain technology. One of the prominent projects termed “Innovate UK” established the use of BaaS (Blockchain-as-a-service) back in August 2016 for managing welfare checks and student loans. The service functions by taking into account the student or public info and verifying their authenticity to determine the validity of check claims. The management of this process is undergoing updates for newer W3C standards. Also, the UK managed to empower pension payments through dApps in mobile phones functioning under the surveillance of the UK’s Department of Work and pensions [26].

4.1.4. China:

Although China has a strict policy regarding mining and cryptocurrency upsurge. The authorities in China have always been involved in experimenting with Blockchain for their infrastructure improvements. In doing so they have introduced smart contract programs like VeChain, NEO, Qtum, and TRON. These are employed in many public management sectors like school systems, administration, NGOs, Health sectors, etc. One thing in particular that the Chinese government is focusing primarily on is the avoidance of capital controls [24,25].

4.1.5. Japan:

The initial adopters and pioneers of blockchain technology were Japan. But there have not been any POCs prototypes from them regarding public management and validations. So far they are the only nation that has a legitimate lawful cryptocurrency protocol for all users. Even the government of Tokyo decided to make Bitcoin a legal medium of exchange for the public [24].

To get an overview of the ongoing projects that involve public management in any sort of way can be assessed by following Table 1[20,22,24,28]

Table 1. Projects Involving Blockchain-based Public Validation

No	Country	Project Name	Industry/Sector	Government Level Involvement
1	Switzerland	uPort decentralized identity	Digital identity for proof of residency	Local (Municipality of Zug)
2	Malta	Academic Credentials	personal document storage and sharing	National
3	Netherlands	Pension Infrastructure	Pension Management	National
4	Georgia	Land Title Registry	Property Management	National
5	South Africa	Project Khoka	Finance & E-commerce	National & International
6	Luxemburg	Blockchain Governance Framework	Human Resource Management	National

4.2. *Paperless Identity Management in Light of Blockchain*

Multiple sorts of organizations may benefit from Blockchain's various advantages, which include greater transparency, security, and other elements of efficiency. This means that it may greatly improve security while altering how identity is now handled. Currently, there is no accessible tried-and-true way for managing IDs [6,11]. At different places along the route, voter identification cards, passports, social security cards, and other kinds of official identification are frequently requested. Identity theft and other security breaches are more likely when individuals are required to carry multiple forms of identification. This indicates that blockchain technology can allow the development of decentralized networks that protect the right of individuals to create and use unique IDs [20]. Alongside it also ensures,

- when valid forms of identification are checked
- validation of the occurrence of two authorized parties attesting to each other's identity
- the safekeeping of identity thus empowering the overall Trust factor of the system

4.2.1. *Traditional Identity System*

Despite their significance, identity documents are frequently lost or misplaced. Typically, identification verification is required when applying for a loan, opening a bank account, acquiring a SIM card, or booking a vacation. The fact that many entities, such as the government, financial institutions, and credit reporting agencies, keep and process the personal information of individuals is a fundamental weakness in the existing identity management system [26]. The introduction of blockchain technology has the potential to eliminate the need for these intermediaries while also granting consumers greater control over their personal data. Before transitioning to the blockchain, we must have a deeper grasp of identity management and the problems that affect the current system [20].

A. *Identification fraud or theft:*

Individuals' identities may be stolen if they disclose sensitive information about themselves on insecure websites or through unreliable services. As more individuals migrate their data storage online, this creates a risk for online applications, as hackers can more easily access and steal data from centralized servers. According to the 2018 Breach Level Index, hackers corrupt an average of 18,525,880 records per day. This further accounts for [23],

- Per hour, 771,909 records.
- Minutely, 12 865 records.
- Approximately 214 records per second.

B. *User Info Maintenance Control:*

User Info Maintenance is usually controlled through Personally Identifiable Information (PII) in order to keep track of user-validated documentation. However, users cannot modify or interact with PII. They are unaware of the number of times their personal information has been shared without their consent, as well as the whereabouts of any databases containing their information. Thus, a novel method of identity management is required. Blockchain-based identity management can provide users control over their personal data by producing a universal ID that can be used for a multitude of purposes. Blockchain may be the solution to the aforementioned issues since it gives individuals assurance that their personal information will not be shared without their consent [18,21].

C. *KYC Onboarding:*

Traditional Identity Systems need to Know Your Customer (KYC) organizations, end users, and external verifiers. Overall, the system is rather costly for all parties involved. To meet the different demands of their clients, which include banks, healthcare providers, and immigration authorities, KYC service providers require additional time and employees. Customers are charged hidden processing fees to cover the additional cost of the KYC verification procedure. In addition, the time required by external organizations to sign up clients is considerable. The projected yearly global cost of KYC ranges from 48 million to 60 million [11].

4.3. *Relevancy of The Findings*

From the above mentioned discussions it is evident that all of these cases are trying to solve the same problem but in respect to different scenarios. In most of these cases the governmental and research bodies are eager to utilize modern technologies for implementing an all-in-one solution. Something that can leverage the decentralized factors from DLT and blockchain. As well as staying paperless with the help of Digital Identification system. This more or less aligns with our research objective. Which is to provide a noble framework that ensures all of the necessary data verification and data security aspects found on the provided case studies. The development of different POC done by the countries and organizations mentioned above provides a deeper insight into the key elements of the problems. Issues like how credentials and identifiers need to be maintained in a decentralized infrastructure. Also how the entire framework can automate the flow of dealing with multiple layers of data manipulation and verification whenever needed. As a result these case studies provide the essential feedback needed to improve upcoming and future architectures.

5. Methodology

The Methodology and Proposed Architecture sections will be divided into different narratives and component utilization. This was done for the purpose of establishing a well-defined framework for this research. Most of the focus in the upcoming segments will be highlighted through diagrams, clarifications, and schema.

5.1. Initialization of DID & VC

In order to achieve our goal of envisioning a globally functional paperless blockchain verification system, we first need to lay the groundwork. In terms of public identification in the real world, we all have certain biometric characteristics from birth, which can be termed as our first set of identification credentials. In the process of growing up, we happen to achieve other such credentials in the form of birth certificates, nationality papers, educational certificates, driving licenses, passports, and so on. All such credentials act to verify the actual person, and this authentication procedure is carried out by an Identity Provider(IdP). The traditional format of this procedure was mainly using a username and password to identify individuals. But with the forthcoming of DID and VC, we no longer need to depend on traditional Idp approaches along with their associated vulnerabilities.

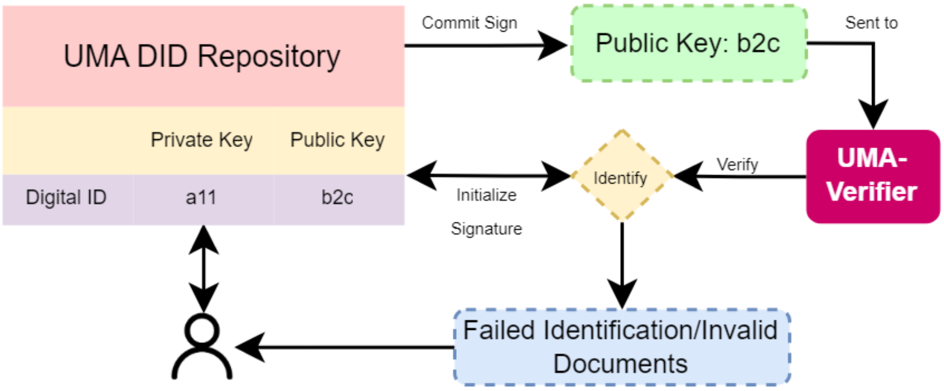

Fig. 1. DID Signing Procedure

The process as showcased in Fig.1 outputs a globally unique ID that is constituted through cryptography. A User Management Agency(UMA) such as a government verification institution, passport offices, etc., will be in charge of developing a private/public key pair. This process will be initiated right after a person possessing the nationality of that country proves his identification through any documentation like a driving license or national identity to a UMA. The private key securely stays in hand with the UMA. With this, the UMA can easily validate the provided documents from the required sources and then set up a DID for that specified document provided by the person. Having multiple documents in turn will allow users to have access to multiple DIDs which will also influence their trust factor in the system for the verifiers. After the process is completed the applicant will be provided access to the new DID with both public and private keys. This DID will also be stored within the UMA for future validation purposes and blockchain integration. It will also act as a pointer toward all future DIDs that citizens will possess. In other words, it can be considered a decentralized account for public documentation. The UMA-Verifiers will be in charge for identifying all the documents as assigned against the public key and if they tend to find any sort of misalignments in terms of legal issues then the user will be notified about the failed identification process. This will also include document requirements for the users to know the specific reason for the failure.

Different sources that mainly provide public documents and certifications will act as the issuers for Verifiable Credentials(VC). As demonstrated in Fig.2 whenever new DIDs will be issued by a citizen or a user the process will need to be validated by the UMA. The verification will also have proceeded through cross-referencing with the already documented VCs from previous DIDs that were initiated by the UMA. Furthermore, once a new DID application has been created by the user, this system automatically won't allow them to create a new one. They can only apply for a new DID once the current one has been processed. UMA in this system is the main central entity that controls the rights to provide the public with their unique DIDs. They hold the responsibility of verifying and validating the applications prior to approval. On a deeper level, this process is completed by employing Zero-Knowledge Proof(ZKP). This algorithm also allows using multiple VCs from different issuers for confirming validation. Also, they can access the VC repository for a particular user for better assessment.

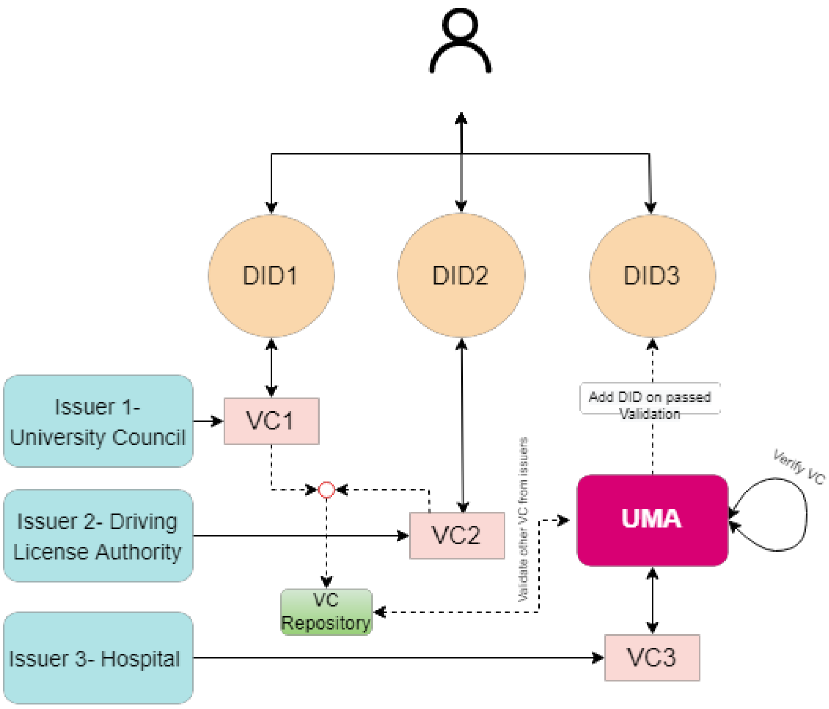
DID1
DID2
DID3
Issuer 1- University Council
VC1
Issuer 2- Driving License Authority
VC2
VC Repository
Issuer 3- Hospital
VC3
Add DID on passed Validation
Validate other VC from issuers
UMA
Verify VC

Fig. 2. VC Validation through Issuers

6. Proposed Architecture

6.1. System Architecture

There is a reason why we follow a 3-layer approach in the architecture of the system, as shown in Fig 3. It is mainly because each user in the UMA will have multiple DIDs with lots of personal information. They can access those DIDs through the global DID issued by the UMA. So, once we put this data into the blockchain, they cannot alter it anymore. That's why our approach tries to adopt a fixed global DID through which the system can optimally support components like VC repository and revocation simultaneously. Just storing the global DID in the blockchain allows users to access their identity easily. The blockchain layer has been thought out to deal with external verification for social, governmental, and travel purposes by external authorities.

6.2. Technical Analysis

The UMA will have access to all the public DIDs. But can only interact with outside sources for verification whenever the user allows it. This process is followed based on some preliminary stages before blockchain integration. Before the UMA can send the DID info to the blockchain, it needs to set up a process for revocation. In simpler terms, "Revocation" can be addressed as updating or deleting a credential. Issues regarding personal documentation and credential changing happen to be critical aspects of any identity infrastructure. A revocation registry can serve as the means for allowing updates to an already assigned credential in a DID. There is a reason why we follow a 3-layer approach in the architecture of the system, as shown in Fig 3. It is mainly because each user in the UMA will have multiple DIDs with lots of personal information. They can access those DIDs through the global DID issued by the UMA. So, once we put these data into the blockchain, they will not be able to alter it anymore. That's why our approach tries to adopt a fixed global DID through which the system can optimally support components like VC repository and revocation simultaneously. Just storing the global DID in the blockchain allow users to access their identity easily. The blockchain layer has been thought out to deal with external verification for social, governmental, and travel purposes by external authorities.

For the purpose of analyzing how the validation is sorted with external Verifiers, a schema was generated. It is formed of the required flows as discussed in the following,

- Users, UMA & Verifiers will possess DIDs.
- Identity Hubs will be linked to UMA & Verifier DIDs
- The requested VCs from Verifiers will be notified to the Users through UMA

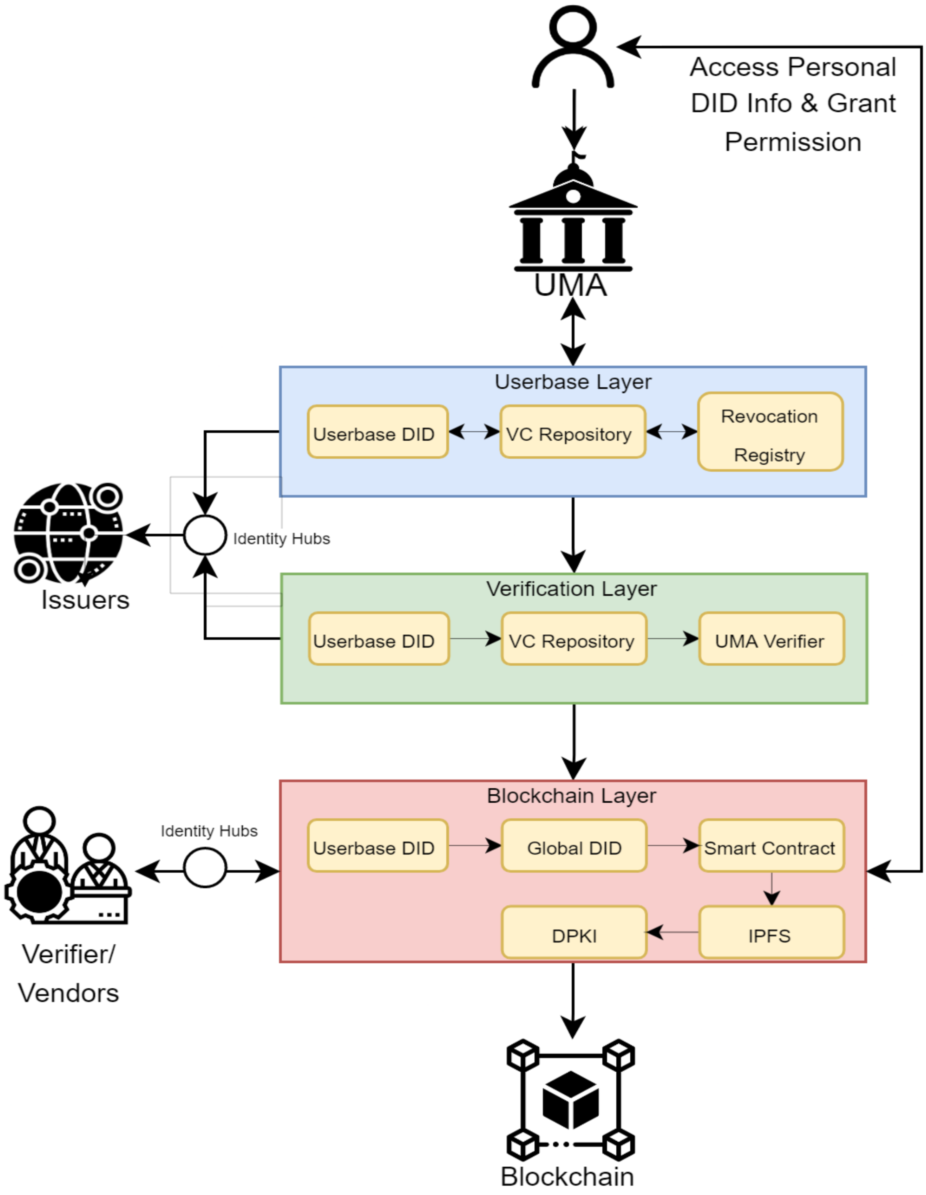

Fig. 3. System Architecture

The analysis of this process can be clarified according to the following statements as derived from Fig 4,

- UMA discovers the current keys and Identity Hub endpoints by recognizing the Verifier's DID. This is something that occurs on a periodic basis at UMA.
- Through a GUI, the user is notified about the request from the verifier and can select to proceed.
- A semantic message reflecting an ASK, encoded with parameters of the User's Request, is generated by the UMA after the option to advance is selected.
- UMA sends an ASK message to the Identity Hub of the Verifier
- Then the verifier responds to the ASK it receives with the list of requirements according to the "Check".
- After getting the originally signed hash of the "Check", the User will provide the credentials required by the "Check" through UMA.
- The verifier then shares the User's identification address with the agreed-upon VCs and publishes a smart contract on the UMA blockchain. This step employs the proof of an ability to settle.
- Once UMA receives a response from the User, it will retrieve the VCs from IPFS using the Original DID of the User and transmit them to the Verifier.
- Once the Verifier has validated the User's presentation and the credentials it contains, UMA provides the User with a final "Check."
- UMA will then review the contract to ensure that all the required documentation is present.
- The verifier can release the user's DPKI after a successful check by enforcing the associated smart contract.

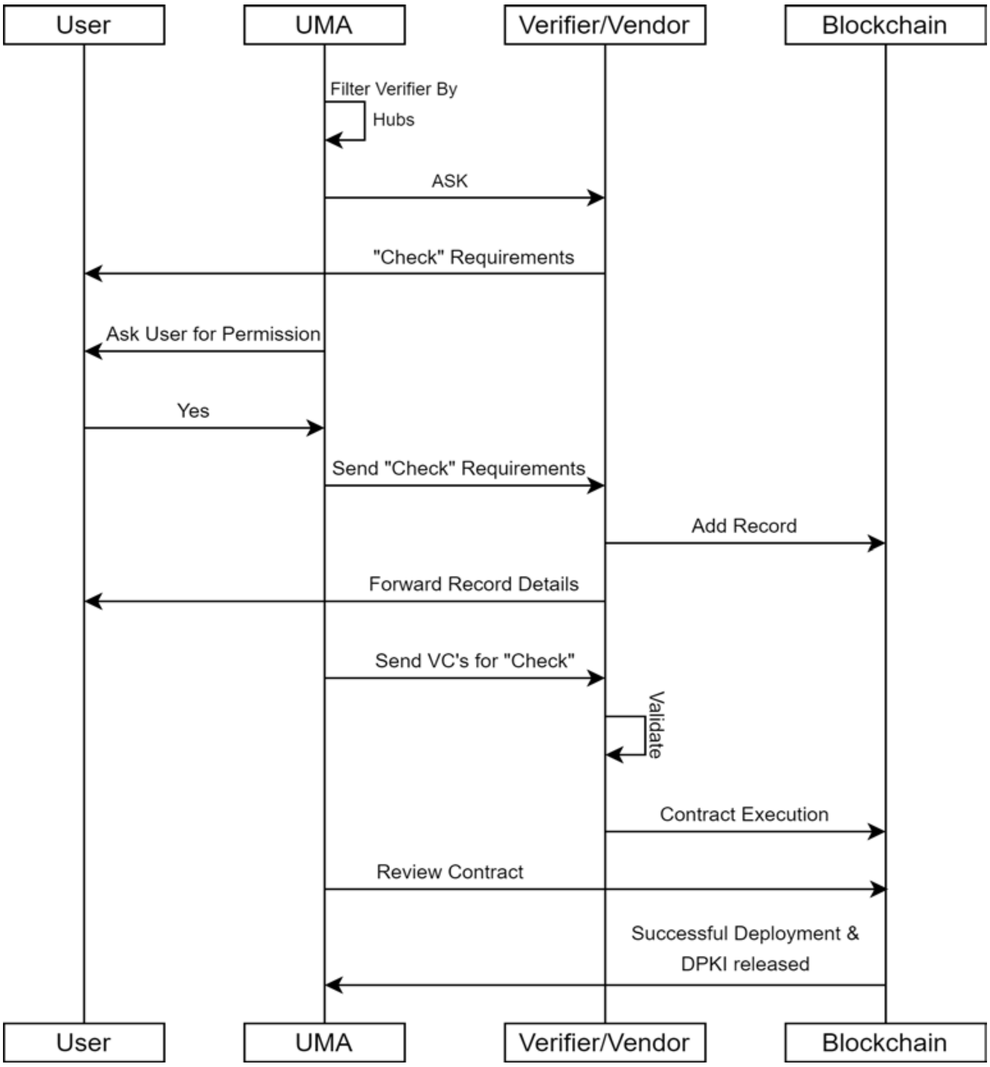

Fig. 4. Validation Analysis with Smart Contract Deployment

Through the schema provided in Fig.4, we are able to demonstrate the technical outline of our proposed architecture. Every event that takes place during this process is conducted through digital means so no form of paper documents is needed. Moreover, the goal to secure every form of verification is also defined in this process where we can observe how all the decisions proceed through UMA. Also, the final validation that utilizes blockchain is maintained through contract review from UMA. This schema tries to construct a foundation that ensures scalability factors for a paperless means of verification.

7. Limitations

The main parameters involved in constituting this framework namely blockchain, DID, VC and DPKI have their own characterized limitations. Looking at any DLT based technology such as blockchain, the immutability afforded by it is one of the most significant drawbacks of this proposed architecture [4]. According to research it suggests that during the testing phase any data that will be stored from the beginning can never be altered. So this hinders the data regulations policy regarding different government bodies and organizations. Moving towards the W3C protocols, there will be difficulty in resolving this issue to mitigate its impact. As from the documentations of W3C it suggests that further measures have to be adopted into our system to regulate how VCs and DIDs information will be kept via global DIDs. Also the DPKI procedure attempts to resolve this problem by referencing only the global DID within the hash to the verifiers. Therefore, the IPFS-saved internal documents are not required to be stored in the blockchain, as doing so would result in an optimization issue. Thirdly, this architecture lacks real-time implementation, which is the major limitation in this research. Technical aspects aside this proposed architecture would need good amounts of testing before going towards the implementation route. Since it includes a public user base, governmental institutions, NGOs and border check authorities. As the purpose of this research was to provide the groundwork for a Proof of Concept protocol, its implementation must occur in a sandbox setting with permissioned blockchain. The analysis of results and scopes for improvements and errors could be considered the final limitation. This is also due to not having a real-time testing POC ready at hand for simulations.

8. Results & Discussions

The main outcome from this research can be divided into 4 phases notably, public user, verifier, issuer and government phase. During the user phase all the functionalities will be involved in the Userbase layer where the verification services will be provided through governmental bodies to the public. This will in turn call for the issuer phase where the issuers like hospitals and institutions will provide the necessary things forwarded to the government body for authentication. In case of already having a DID the user can easily verify their authentication through the verifier phase. This flow of control easily automates the overall process that can result in a smooth processing of an already complicated system. Our goal in this research was to provide a paperless medium which is already achieved since this whole process of public identity validation is done via digital record.

9. Conclusion

This paper attempted to illustrate a novel strategy for adopting W3C standards using blockchain technology for public verification. But there are still many aspects in the works for this research that will be coming in the future. One such is ensuring the trust factor of the users and ranking their identity within the system. This will be accomplished by calculating the trust score identifier that will be governed by VCs. In addition, for future analytics, a real-time simulation of the proposed architecture will be developed utilizing hyperledger fabric for a proof of concept prototype. It can be presumed that this will result in the desired outcomes and allow for the resolution of issues and error logs. The impact of the problem mentioned in this research is crucial in the present state of the public management and identity verification domain. This proposed architecture aims to provide a sustainable and meaningful solution that can advance the current use cases in this sector. It can do so through the application of modern technology to revolutionize the traditional infrastructure for public verification in every scenario. There has never been a bigger opportunity to explore novel and more effective techniques for bolstering socioeconomic foundations than there is now. Despite the limits highlighted, future efforts will be able to accommodate the constraints identified by this research. SDG objectives have prioritized a robust paperless verification infrastructure for quite some time. Through this effort and our future POCs, it is capable of claiming that paperless verification has a bright future.

Acknowledgment

The work for this research was conducted during the Masters of Science Thesis period of the First Author “Samiur Rahman Khan”. Under the guidance of the supervisor and the second author “Md.Al-Amin”, the content of this research paper was justified and reviewed.

References

[1] Gulddal, Jesper. "The Novel and the Passport: Towards a Literary History of Movement Control." Comparative Literature 67.2 (2015): 131-144.

[2] Sekiguchi, Kenta, Makoto Chiba, and Mikari Kashima. The securities settlement system and distributed ledger technology. No. 18-E-2. Bank of Japan, 2018.

[3] Civelek, Mustafa Emre, and Abdurrahman Özalp. "Blockchain technology and final challenge for paperless foreign trade." Eurasian Academy of Sciences Eurasian Business & Economics Journal 15 (2018): 1-8.

[4] Khan, Samiur, et al. "A pragmatical study on blockchain empowered decentralized application development platform." Proceedings of the International Conference on Computing Advancements. 2020.

[5] Masood, Faraz, and Arman Rasool Faridi. "An overview of distributed ledger technology and its applications." International Journal of Computer Sciences and Engineering 6.10 (2018): 422-427.

[6] Sun, Cheng Hung, et al. "Paperless reporting and electronically verifying clinical investigations." International journal of health care quality assurance 27.5 (2014): 382-390

[7] Haque, AKM Bahalul, et al. "Towards a GDPR-compliant blockchain-based COVID vaccination passport." Applied Sciences 11.13 (2021): 6132.

[8] Panchamia, Sanket, and Deepak Kumar Byrappa. "Passport, VISA and immigration management using blockchain." 2017 23rd annual International Conference in advanced computing and communications (ADCOM). IEEE, 2017.

[9] Tang, Bo, et al. "Iot passport: A blockchain-based trust framework for collaborative internet-of-things." Proceedings of the 24th ACM symposium on access control models and technologies. 2019.

[10] Oliveira, Marco, et al. "Immunity Passport Ledger." International Conference on Innovations in Bio-Inspired Computing and Applications. Springer, Cham, 2021.

[11] ESCAP, UN. "International legal frameworks and best practices relevant to Cross-Border Paperless Trade." (2017).

[12] Kustov, V. N., and E. S. Silanteva. "Technological aspects of the trust in cross-border paperless exchange." Journal of Physics: Conference Series. Vol. 1703. No. 1. IOP Publishing, 2020.

[13] Sethy, Ambica, and Abhishek Ray. "Leveraging blockchain as a solution for security issues and challenges of paperless e-governance application." Progress in Computing, Analytics and Networking (2020): 651-658.

[14] Chaudhari, Sarang, et al. "Framework for a DLT based COVID-19 passport." Intelligent Computing. Springer, Cham, 2021. 108-12

[15] Garcia-Font, Victor. "Conceptual technological framework for smart cities to move towards decentralized and user-centric architectures using DLT." Smart Cities 4.2 (2021): 728-745.

[16] Papageorgiou, Alexander, et al. "DPKI: a blockchain-based decentralized public key infrastructure system." 2020 Global Internet of Things Summit (GIoTS). IEEE, 2020.

[17] Verifiable Credentials Data Model v1.1; W3C Recommendation 03 March 2022; https://www.w3.org/TR/vc-data-model/

[18] Decentralized Identifiers (DIDs) v1.0;Core architecture, data model, and representations;W3C Recommendation 19 July 2022; https://www.w3.org/TR/did-core/

[19] Verifiable Credentials Use Cases; W3C Working Group Note; 24 September 2019 ;https://www.w3.org/TR/vc-use-cases/

[20] Zhang, Yuwen, Yang Liu, and Cheng Chi. "BID-HCP: blockchain identifier based health certificate passport system." International Symposium on Cyberspace Safety and Security. Springer, Cham, 2020.

[21] Zetzsche, Dirk A., and Jannik Woxholth. "The DLT sandbox under the Pilot-Regulation." Capital Markets Law Journal 17.2 (2022): 212-236.

[22] Siringoringo, Hotniar, and Hany Maria Valentine. "Electronic passport system acceptance: an empirical study from Indonesia." International Journal of Electronic Governance 10.3 (2018): 261-275.

[23] Dunphy, Paul, and Fabien AP Petitcolas. "A first look at identity management schemes on the blockchain." IEEE security & privacy 16.4 (2018): 20-29.

[24] Breached Records More Than Doubled in H1 2018, Reveals Breach Level Index, Thales DIS, 2018; https://dis-blog.thalesgroup.com/security/2018/10/09/breached-records-more-than-doubled-in-h1-2018-reveals-breach-level-index/

[25] Shen, Xiang-Dong, et al. "The new ecosystem of cross-border e-commerce among Korea, China and Japan based on blockchain." Journal of Korea Trade 24.5 (2020): 87-105.

[26] Wang, Qiang, Min Su, and Rongrong Li. "Is China the world’s blockchain leader? Evidence, evolution and outlook of China’s blockchain research." Journal of Cleaner Production 264 (2020): 121742.

[27] De Meijer, Carlo RW. "The UK and Blockchain technology: A balanced approach." Journal of Payments Strategy & Systems 9.4 (2016): 220-229.

[28] Jalakas, Parol. "Blockchain from public administration perspective: Case of Estonia." Tallinn University of Technology: Tallinn, Estonia (2018).

[29] Subeh, Ibrahim. "BLOCKCHAIN AS A TECHNOLOGICAL IMAGINARY: MEDIA FRAMING AND THE VIEWS OF BLOCKCHAIN PROFESSIONALS IN THE ARAB WORLD." (2020).

[30] Zeadally, Sherali, and Jacques Bou Abdo. "Blockchain: Trends and future opportunities." Internet Technology Letters 2.6 (2019): e130.

[31] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. 2016. A Secure Sharding Protocol For Open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 17–30. https://doi.org/10.1145/2976749.2978389

[32] Na, D.; Park, S. IoT-Chain and Monitoring-Chain Using Multilevel Blockchain for IoT Security. Sensors 2022, 22, 8271. https://doi.org/10.3390/s22218271

Authors’ Profiles

Samiur Rahman Khan earned a Bachelor of Science in Computer Science (CS) from American International University-Bangladesh in 2019 (AIUB). He is currently employed as Lecturer in the Institute of Continuing Education Department, American International University-Bangladesh (AIUB). He has competed in various nationwide blockchain competitions. Professionally he has provided consultation & acted as business development lead to multiple Web3 client projects alongside developing whitepapers and litepapers.His research interests include decentralized systems, distributed computing, the Internet of Things (IoT), network automation, and blockchain. His undergraduate thesis research on Blockchain-Enabled Decentralized Application Development Platform was published in ACM Proceedings. His research focuses on innovation, compatibility, and scalability in the context of altering conventional systems. He has a Master of Science in Computer Science (MScs) from American International University-Bangladesh (AIUB).

MD. Al-Amin is currently working as a lecturer in the Computer Science Department, American International University-Bangladesh (AIUB). Besides his teaching profession, he is actively doing R&D projects on freelance platforms for different clients across the globe. He is also supervising research & development teams & providing technical consultancy. He received his Bachelor’s in Software Engineering and Master’s degree in Computer Science and Engineering (CSE) from American International University-Bangladesh(AIUB), Dhaka, Bangladesh in 2015 and 2017 respectively. During his Master’s degree, he was awarded the academic distinction Magna Cum Laude(Silver Medal) award for his academic results. He achieved two times ICT Fellowship Awards for the years 2015-16 & 2016-17 from the Ministry of ICT, Government of Bangladesh. He has also served as a registration committee member in the International Conference on Computing Advancements (ICCA 2020). He is a member of Bangladesh’s computer society. His research interest primarily focuses on Distributed Ledger Technology (DLT), Blockchain Technology, Web 3.0, Distributed Computing, Web of Things, Information Security, Web Assembly, and Knowledge base System.

How to cite this paper: Samiur Rahman Khan, Md. Al-Amin, "Towards a Novel Identity Check Using Latest W3C standards & Hybrid Blockchain for Paperless Verification", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.15, No.4, pp. 13-25, 2023. DOI:10.5815/ijieeb.2023.04.02