A Man-Vehicle e-Passport System using Biometric Blockchain towards Automated Border Control

Bing Xu, Qiang Ni, Ahmed Bouridane and Richard Jiang

***Abstract*—Since the mid-1990s, the evolution of internet technologies has significantly transformed global connectivity and digital interaction. Today, advances in computing and networking continue to support the development of emerging paradigms such as the Metaverse and digital twins—concepts that aspire to bridge physical and digital experiences. Parallel to this, blockchain technology is reshaping traditional notions of trust by enabling immutable transaction records and smart contract automation, thereby fostering the rise of decentralized autonomous organizations (DAOs). Building on these foundations, this paper presents a biometric blockchain-based e-passport system designed to improve the operational efficiency of automated border control (ABC) systems. At the core of our approach is the concept of a DAO-inspired framework for border control, wherein identity verification and management tasks are executed through atomic smart contracts and recorded immutably on the blockchain. Our system incorporates biometric authentication and decentralized identity features to digitize border documentation and automate verification processes. This creates a secure, verifiable digital representation of an individual's identity that can interact with automated border control workflows. Performance evaluations conducted using Hyperledger Caliper demonstrate the potential of the proposed system, showing a 3.5-fold improvement in processing efficiency compared to traditional ABC setups.**

***Index Terms*—Biometric Blockchain, DAO, Metaverse, Digital Twin, Autonomous border control, and e-Border.**

I. Introduction

During the COVID-19 pandemic in 2021 and very recent war-affair between Russia and Ukraine, border control has become an issue. It is not only because there is a sharp increase in border crossing demand but also a shortage in border control officers due to sick leave. Plus, in accordance with [1], the border crossing demand in 2025 will reach 887 million for land, air, and sea travellers in the EU, compared with 722 million in 2020 with an increase rate of about 5 percent per year. Similarly, the estimated number of individual(non-commercial) files to be stored in the border control agent system will be 128 million at 2025 compared with 104 million at 2020, which the annual growth rate is about 4.6%. That is, existing border agent capability is capped; therefore, the existing border control efficiency needs to be improved. See Fig. 1 for a 15km lorry queue waits at Dover border checkpoints, it is reported that lorry drivers is staled up for eight hours to get across the border [2].

Fig. 1. Dover 15km lorry queue queues to get cross the border [2].

To put more in detail, the causation of existing border control low efficiency can be summarized into two folds, which specifically are manual documentation verification and the existing static e-passport system. That is to say, proving border crossing legitimacy involves a good amount of documentation verification, such as identity credential e-passport, individual immigrant border crossing legitimacy proof visa, and commercial products border crossing legitimacy proof customs clearance documentation etc. Apart from existing e-passport, all the rest of documentation verification has to be manually conducted by border control officer, which is deemed very time-consuming. Most important, current e-passport contains static information that is locked in the e-passport book microchip, which does not only suffer all inconvenience embedded with distance but also makes binding dynamic border crossing legitimacy information to the identity extremely difficult.

Theoretically speaking, to improve existing border control efficiency and conquer the criticism of being a centralized system, smarter and further automatization and decentralization is indispensable [3]–[6]. With existing computing technology, it indeed is completely feasible to transform existing border control procedures into automatic, but two premises have to be fulfilled beforehand.

First, automatization in terms of documentation verification and border crossing events recording requires the digitization of border crossing documentation as the first compulsory premise. In the case of border control, the digitized border crossing documentation requires fidelity, which it has to be a genuine reflection of the real-world. Therefore, digital twin technology is deployed [7]. For a formal definition, digital

This work was supported in part by the UK EPSRC under Grant EP/P009727/2, and the Leverhulme Trust under Grant RF-2019-492.

Bing Xu, Qiang Ni and Richard Jiang are with LIRA Centre, Lancaster University, Bailrigg, Lancaster, Lancashire, UK, LA1 4WA

Ahmed Bouridane is with the College of Computing and Informatics, University of Sharjah, Sharjah, UAE.

Correspondent Author: Richard Jiang, e-mail: r.jiang2@lancaster.ac.uk.

Manuscript received Sept 7th, 2023; revised xxx xxx, 2024.

twin is a digital representation of an actual real world object that serves as the indistinguishable digital counterpart of it for the purpose of simulation, testing, and monitoring etc [8]. That is to say, digital twin is able to construct a veracity mapping from real-world object to the digital-world with high fidelity and consciousness, which requires existing attributes of the real-world object to be mapped to the digital-world as much as possible [9]. What is more, through enabling this duplication mapping, digital twin also enables computing artificial intelligence and computing assisted management, predictions and simulations applicable to real-world objects [10].

I addition to documentation digitization, the owner of the digitized document has to be accurately identifiable so that border crossing permit can be granted to the lawful right person after documentation verification. That is to say, constructing individual bodily person's digital twin is the second premise. However, a bodily person's digital twin can be difficult to construct due to the fact that verifying the present of a bodily person over open internet is problematic and digital identity is forgeable. As a well-known internet phrase claims "no one knows you are a dog if you are on internet [11]," it points the same problem out, which indicates that digital identity authentication is always a reasonable risk-based assurance process [12], [13]. Therefore, biometric Blockchain based e-passport system is proposed to construct individual bodily person's digital twin. Taking advantage of Blockchain transaction immutable property, online biometric identity authentication through Blockchain generated biometric e-passport does not only proving the present of a real human over internet but also improving the assurance of the digital identity authentication instance.

To add on about Blockchain, now it is a quite established computing technique in current literature since its initial publication in 2008. It applies cryptography to distributed network and builds a timestamped and immutable chain of hashed blocks. Blockchain has very favourable innate features that are derived from the system architecture, such as disintermediation, self-execution, immutable and irreversible transaction etc [14]. Most important, it shifts the root of trust from a system administrator to the computational power attached to a system, which brings new form of economy. Particularly, the decentralized autonomous organization(DAO) is one of them. DAO is to take advantage of Blockchain technology, constructing an easy to join, entirely digitally native, and global in reach organization [15]. Instead of conventional manager and managing board who are the central authority of an organization, DAO introduces Blcokchain self-execution smart contracts to automatically control the organization behaviour and reach organizational decision through Blockchain consensus rule.

In our work, we propose automating the border control system by constructing a Border Control Metaverse DAO on top of the Hyperledger Fabric Blockchain. This innovation enables the automation of border control procedures using blockchain smart contracts. Crucially, the immutable and atomic nature of smart contracts ensures that the system operates without human intervention, making the proposed Biometric Blockchain-based Automated Border Control (BBC ABC) system significantly more reliable and tamper-proof. Unlike typical Metaverse concepts involving immersive 3D or social media environments, our Metaverse DAO represents a comprehensive digital ecosystem that integrates all stakeholders involved in border control—such as van drivers, service providers, and HMRC officials—within a unified automated framework. This digital scenario facilitates secure and transparent interactions across all parties.

Our work on the Metaverse DAO innovatively explores the virtualization of border control by digitizing identity verification through cutting-edge technologies such as biometrics, blockchain, and e-passports. In response to the growing demand for border crossings and shortages in staffing, the proposed solution offers a groundbreaking transformation. By integrating a biometric blockchain-based e-passport system, border control processes can be seamlessly automated, greatly enhancing both efficiency and security. The use of digital identity twins allows for real-time traveler verification, while smart contracts within this decentralized autonomous organization (DAO) ensure autonomous, transparent border management. This system promises to alleviate bottlenecks, providing a scalable, tamper-proof solution that redefines the future of border control.

II. PRELIMINARIES

In this section, the preliminaries of this proposal's backbone subject will be covered, which include both Blockchain technology and digital twin in the Metaverse DAO. Specifically, atomic and self-executed smart contract and Blockchain innate properties will be particularly explained. What is more, to exercise the best conduct of constructing a Metaverse DAO, its construction framework and relationship with digital twin are both well introduced.

A. Blockchain

The price of Bitcoin, a blockchain-based cryptocurrency, was approximately $0.0009 per token at its inception in 2008. By 2023, its value had peaked at over $65,000 before stabilizing around $25,000, representing a dramatic increase over the past 15 years [16]. This exponential growth highlights the significant real-world impact and transformative potential of blockchain technology in decentralized financial systems and beyond.

Blockchain is a type of distributed ledger technology (DLT) that enables decentralized networks to reach consensus without relying on a central authority [17]. In traditional computing systems, a centralized trusted authority is typically required to resolve the problem of equivocation and to ensure data integrity and consistency. In contrast, blockchain replaces this central authority with a network of distributed nodes that use cryptographic algorithms and consensus mechanisms to validate and immutably record transactions in a time-stamped ledger [18]. This structure enhances transparency, resilience, and trust in decentralized systems.

Transactions are a fundamental component of blockchain systems, as they represent the core data operations being recorded and verified. Other blockchain components—including digital signatures, consensus mechanisms, and network protocols—are primarily designed to ensure that transactions are securely validated and consistently recorded across all nodes [19]. Each transaction consists of various subcomponents, such as scripts and cryptographic signatures, that enable a wide range of operations on the blockchain. The validated transactions are stored in a distributed ledger, which is shared across the network. These ledgers are cryptographically timestamped and designed to be tamper-evident. While blockchain is often described as “immutable,” this immutability is conditional—it is maintained so long as the majority of the network adheres to the existing consensus rules. In cases such as user-activated soft forks or contentious hard forks, previously recorded transactions can be altered or excluded, highlighting that consensus rules, rather than absolute immutability, underpin the trust model of blockchain systems [14], [20]. This makes consensus mechanisms critical, as they determine the legitimacy and permanence of recorded data.

1) Digital Signature: The function of a digital signature in Blockchain system are two folds. First, guarantee the integrity of the transaction. Second, verify the identity of the message sender. Unlike conventional cryptographic encryption, which discrete logarithm and integer factorization are normally imposed. Bitcoin Blockchain Elliptic curve digital signature algorithm (ECDSA)’s distinctive sub-exponential-time algorithm is no one as such yet. It is claimed that ‘. . . the strength-per-bit is substantially greater in an algorithm that uses elliptic curves [21].’ Most important, the digital signature verifier is able to verify a signature by signer’s public key, even though the signature itself is signed by private key.

2) Consensus Rule: In decentralized system, all nodes in Blockchain behave completely independent. They are fully connected with each other for the realization of system common goal [22]. When all nodes agree with “what is the current status of the system”, they reach a consensus, and the rule of how to reach the agreed current state of the system is called consensus rule [20].

Currently, there are two consensus rules dominate the Blockchain architecture. That is, proof of work (PoW) and proof of stake (PoS). Specifically, PoW updates the current global status of Blockchain system by doing some computational work, which the work specifically refers to nodes increment nonce value for every try that they have made until a satisfied block hash value is found. The quickest node will be the creator of that block and get rewards for maintaining the system consensus. As for proof of stake (PoS), the stake can be account balance and/or age of the cryptocurrency etc. After block being valid, node who has the most stake will be voted as the block creator and gets reward from the system.

3) Smart Contracts: Smart contracts are foundational components in many blockchain systems. While major platforms offer varying descriptions—Bitcoin describes them as “transactions which use the decentralized Bitcoin system to enforce financial agreements” [23]; Ethereum defines them as “a program that runs on the Ethereum blockchain” [24]; and Hyperledger refers to them as “business logic running on a blockchain” [25]—these definitions are not exhaustive. More accurately, a smart contract is a conditional computer program deployed on a blockchain, which automatically executes predefined actions only when specific conditions encoded in the contract are met [26]. The conditional execution mechanism ensures trustless automation and enforces agreed-upon rules without the need for intermediaries, making it a cornerstone of decentralized applications and processes.

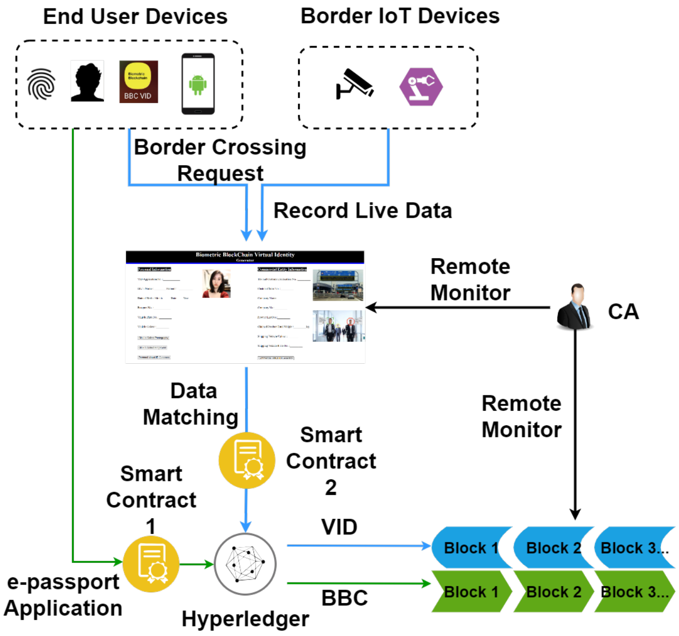


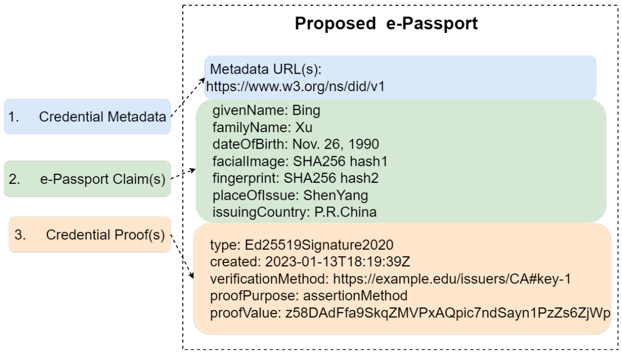
Fig. 2. Full workflow of the proposed BBC ABC system.

The aim of using smart contract is to enable non-intermediary, trusted, and peer-to-peer transaction [27]. Most important, comparing with conventional online banking and digital service, the benefits of deploying Blockchain smart contract are three folds:

- Trust. Trust of executing a specific contract is given to the computer program of the smart contract rather than any third party, and the security of a smart contract system is depends on computational power attached to the system but not any central authority who control the system any more [28].
- Non-intermediary. All smart contract initiated transactions are non-intermediary and peer-to-peer, which saves a lot of transaction fee compared with conventional business contract mode [29].
- Automatic execution. Smart contract will automatically execute as soon as new parameter is given, and due to its atomic nature, the transaction is either not started yet or otherwise completed after initiation [30].

B. Digital Twin in the Metaverse DAO

The Metaverse is commonly described as a persistent, interactive, and shared virtual space that integrates aspects of social interaction, gaming, work, and commerce [31]. It builds



Metadata URL(s):
https://www.w3.org/ns/did/v1

givenName: Bing
familyName: Xu
dateOfBirth: Nov. 26, 1990
facialImage: SHA256 hash1
fingerprint: SHA256 hash2
placeOfIssue: ShenYang
issuingCountry: P.R.China

type: Ed25519Signature2020
created: 2023-01-13T18:19:39Z
verificationMethod: https://example.edu/issuers/CA#key-1
proofPurpose: assertionMethod
proofValue: z58DAdFfa9SkqZMVPxAQpic7ndSayn1PzZs6ZjWp

Fig. 3. A demonstration of the proposed biometric e-passport identity digital credential, which includes credential metadata, claims and proofs three components.

upon 3D interfaces to extend traditional 2D computing environments, offering immersive simulations that enhance user engagement. While some companies, such as Meta (formerly Facebook), envision the Metaverse as a fully immersive digital realm [31], this ideal remains aspirational. In current research and development, the Metaverse is better understood as an evolving concept that aims to extend digital interactivity rather than fully merge digital and physical realities.

The term Metaverse originated in Neal Stephenson's 1992 science fiction novel Snow Crash, where it depicted a shared, immersive virtual world. In recent years, interest in the Metaverse has resurged, notably when Facebook rebranded as Meta in 2021 to emphasize its strategic focus on immersive digital environments. Conceptually, the Metaverse is associated with cross-reality (XR) technologies—including virtual reality (VR), augmented reality (AR), and mixed reality (MR)—which aim to enhance user interaction through three-dimensional, immersive interfaces [32]. These 3D environments are positioned as improvements over traditional 2D interfaces, especially in fields like online education. For instance, [32] highlights how limitations in 2D learning platforms, such as Zoom fatigue and emotional isolation, have contributed to disengagement and high dropout rates, thus motivating interest in 3D alternatives that offer immersive experiences and greater perceptual realism via XR.

As discussed above, the Metaverse emphasizes immersive interaction over an open internet. This involves not only the use of 3D user interfaces but also the accurate mapping of real-world entities into the digital environment to enhance user experience. This mapping, often referred to as a digital twin [10], represents a virtual replica of physical assets or processes. While Blockchain technology is proposed as a means to establish immutable links between real-world objects and their digital counterparts [33], practical implementation remains challenging. Creating reliable digital twins requires precise data acquisition methods—such as laser scanning or sensor integration—and robust identity verification to ensure data integrity and authenticity. These aspects are crucial to bridge the gap between physical reality and its Metaverse representation, and remain active areas of research and development.

For a formal definition of digital twin, it is a digital representation of an actual real world object that serves as the indistinguishable digital counterpart of it for the purpose of simulation, testing, and monitoring etc [8]. That is to say, the digital twin constructs the mapping from real world object to the Metaverse with high fidelity and consciousness, which requires existing attributes of the real world object to be mapped to the Metaverse as much as possbile [9]. What is more, through enabling this mapping, digital twin also enables first-hand data collections from digital twin devices so that artificial intelligence and computing assisted management, predictions and simulations can be enabled as well [10].

In relevant of our research, Metaverse application in logistics [3] and individual identity in the Metaverse are of interests. To put more in detail, digital twin based logistics and transportation system has significant impact on the visibility of a vehicle, which enables machine learning and other computing methods applicable to the logistics system overall [**?**], [5], [34]. It requires surveillance system such as sensors, actuators, and CCTV cameras etc to collect live data from the real world and then constantly sends to the digital Metaverse to reflect the current status of the object [34].

III. Privacy-aware Biometric Blockchain-based e-Passport System for Automatic Border Control

In this section, the privacy-aware biometric Blockchain(BBC) based e-passport system for automatic border control(ABC) solution is fully proposed. Specifically, the proposed system consists of two separate Blockchain: one is for e-passport privacy-preserving biometric Blockchain based identity digital twin, and the other is the automatic border control Metaverse DAO, see Fig. 2 for a demonstration of the proposed BBC ABC full workflow.

A. Main Participants in the BBC ABC

To make sure functions is able to be fulfilled in the proposed BBC ABC system, participants take different responsibilities in accordance with their different roles within the proposal. To be more precise, the main participants in the proposed system include:

- **Fabric Certificate Authority (Fabric CA).** Since BBC ABC is built upon the Hyperledger Fabric permissioned blockchain, a certificate authority is required to issue identity certificates based on users' public keys. These certificates enable users' access to the blockchain network; without a Fabric CA-issued certificate, access to BBC ABC is denied. Additionally, Fabric CA enforces transport layer security (TLS) protocols to secure internet communications.
- **System Central Authority (System CA).** BBC ABC employs a System CA as the orderer node responsible for transaction ordering and maintaining the global consensus of the Hyperledger Fabric blockchain. Importantly, the System CA is the sole entity authorized to issue border crossing permits and to immutably record border crossing events on the blockchain. This centralized authority reflects the permissioned and regulated nature of BBC

ABC, balancing decentralization benefits with operational and regulatory requirements.

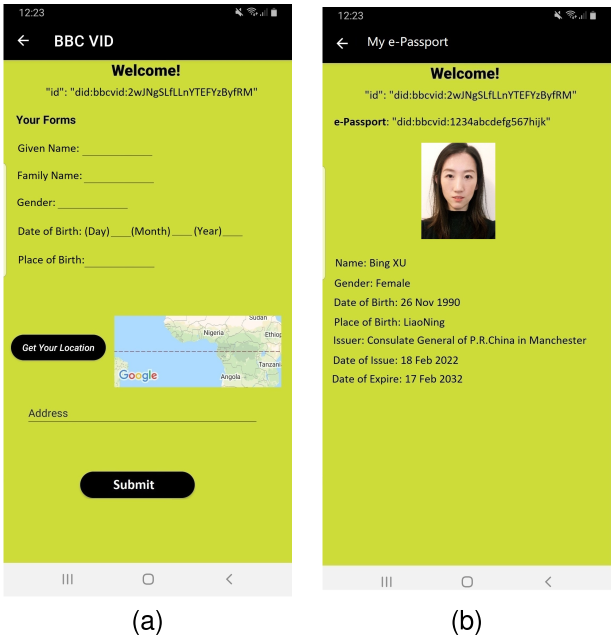
- **Driver and Vehicle Licensing Agency (DVLA)**. DVLA endorses border crossing permit applicant transactions and verifies vehicle-related documentation for border crossing legitimacy.
- **Her Majesty's Revenue and Customs (HMRC)**. HMRC endorses transactions related to customs clearance, verifying commercial product documentation and identifying missing clearance documents in border crossing applications.
- **Surveillance System**. The surveillance system endorses border crossing applications by reconciling applicant data with real-time checkpoint data from CCTV cameras, x-ray scanners, and weight sensors deployed at border crossings.
- **Applicants**. Applicants submit border crossing permit applications and identity credentials via an Android-based decentralized application developed specifically for BBC ABC.

B. BBCVID for Biometric e-Passport

As discussed above, the causation of existing border control procedure low efficiency is summarized into manual documentation and static identity credential. Therefore, BBCVID Blockchain is constructed, which particularly aims for digitizing border crossing documentations and creating dynamic identity credentials through deploying digital twin and Blockchain technology.

Creating a digital twin of an individual's identity for the Metaverse requires both interoperability across platforms and verifiable authenticity. Beyond enhancing immersive user experiences, a trustworthy digital twin bolsters security for the entire Metaverse community. By implementing decentralized identity management on a blockchain, these digital twins avoid the vulnerabilities of centralized identity systems. Traditional authentication methods—such as knowledge-based or challenge-response mechanisms—are susceptible to forgery and credential theft. In contrast, our proposed BBCVID e-passport leverages biometric authentication over the open internet, improving assurance of digital identity and proving the presence of a real person during online interactions.

Specifically, applicants have to install the proposed Android mobile DApp to obtain access to BBC ABC system first, and then submit e-passport application. BBCVID system CA verifies the application and invites applicant to visit biometric identity collection points, where is particularly specified by BBCVID system CA. After the applicant visiting the biometric identity collection point, BBCVID system CA is able to generate a decentralized identifier(DID) and its corresponding biometric DID documentation for the applicant, see Fig. 3 is for an illustration of BBCVID generated biometric e-passport main components. It complies W3C decentralized identifiers (DIDs) v1.0 and credential data model specifications [35], [36], which aims for improving cross-platform interoperability. Similarly, see Fig.4(a) for a demonstration of biometric e-passport application form in Android mobile DApp and Fig. 4(b) for biometric e-passport representation in Android mobile DApp.



12:23

BBC VID

Welcome!

"id": "did:bbcvid:2wJNgSLfLLnYTEFYzByfRM"

Your Forms

Given Name: ___________

Family Name: ___________

Gender: ___________

Date of Birth: (Day)___(Month)____(Year)___

Place of Birth:___________

Get Your Location

Address

Submit

(a)

12:23

My e-Passport

Welcome!

"id": "did:bbcvid:2wJNgSLfLLnYTEFYzByfRM"

e-Passport: "did:bbcvid:1234abcdefg567hijk"

Name: Bing XU

Gender: Female

Date of Birth: 26 Nov 1990

Place of Birth: LiaoNing

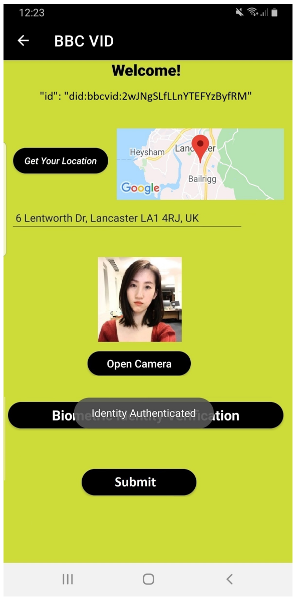
Issuer: Consulate General of P.R.China in Manchester

Date of Issue: 18 Feb 2022

Date of Expire: 17 Feb 2032

(b)

Fig. 4. A demonstration of Android mobile DApp. (a) Biometric e-passport application form. (b) Biometric e-passport representation.



12:23

BBC VID

Welcome!

"id": "did:bbcvid:2wJNgSLfLLnYTEFYzByfRM"

Get Your Location

6 Lentworth Dr, Lancaster LA1 4RJ, UK

Open Camera

Bio Identity Authenticated ation

Submit

Fig. 5. Facial biometric identity authentication at mobile DApp.

The biometric DID documentation is resolvable from the DID({"id": "did:bbcvid: 2wJNgSLfLLnYTEFYzByfRM"}), which specifically records three DID authentication methods including public key, facial image, and fingerprint. Apart from that, "credentialStatus" directs to BBCVID system CA maintained identity revoke list, which all entities are encouraged to consult this list before conducting the digital identity authentication. Most important, the "proof" component in the DID documentation is the digital signature of the BBCVID system CA, which all signature verification materials are included in this component.

After obtaining the biometric DID and DID documentation, it means that the applicant's identity digital twin construction is completed. That is to say, the DID is decentralized digital representation of the real-world bodily applicant, which their tie is constructed through BBCVID Blockchain immutable transaction. Particularly, different from traditional digital identity authentication, the DID can be authenticated by applicant's public key, facial image, and fingerprint biometric identity credentials, see Algorithm 1 for biometric identity authentication protocol through BBCVID DID documentation. What is more, after applicant's bodily person digital twin is constructed, generating real-world identity credential digital twin become straightforward, see Algorithm 2 for creating border crossing document digital twin protocol.

To put more details in about digital signature verification algorithm in BBCVID generated digital twin document, Edwards-Curve Digital Signature Algorithm (EdDSA) [37], [38] is adopted as it is recommended by W3C. Specifically, 32 octets private key is randomly generated, and the corresponding 32-byte public key A ($A \leftarrow encoding[s]B$) is generate, which s is a secret scalar and B is a fixed base parameter("publicKeyMultibase"). Therefore, to verify a digital signature in a BBCVID generated DID documentation, splitting the "signatureValue" into two 32-octet halves, which the first half as a pointer R, and the second half as an integer S. Decode the public key A as A', and computing $SHA512(dom2(0,context)||R||A||M)$ and interpret it as a little-endian integer k, which M is a message. Finally, checking if $[s]B \equiv R+[k]A'$ or not. If it is, signature is verified. If otherwise, signature verification fails [37], [38].

C. VS for Automatic Border Control Metaverse DAO

In current literature, there are a few on-going projects [39]–[41] knee to tackle existing border control low efficiency challenge by Blockchain technology as well. Due to the fact that they are government oriented projects and are still in development, the full technical report is not available at the moment. However, one common factor is that they all built upon permissioned Blockchain.

Since both the border crossing entity and documentation are digitized by BBCVID digital twin Blockchain, the generated digital twin has property of decentralized, verifiable, biometric authenticatable, and immutable. Therefore, to further improve existing border control efficiency, virtual stamping(VS) Blockchain is constructed as the border control Metaverse DAO.

The benefits of constructing Metaverse DAO are three folds. Specifically, automatizing: Deeply automatizing border control procedure through Blockchain atomic and self-executed smart contracts. Reliability: Completely eliminating human factors in distorting digital border crossing legitimacy verification by shifting the trust from a system administrator to computational power through the implementation of Blockchain Metaverse DAO system. Immutable records: The VS border control Metaverse DAO is able to immutably record all border crossing events on the VS Blockchain, which can clear disputes between the DAO and the border crossing entity.

Most important, existing border e-gate is only available to a small group of people who do not require visa verification nor customs clearance. That is because the e-gate can only retrieve static information locked in the microchip of existing e-passport book, which makes the e-gate is completely ignorant about if the person has the border crossing permit or not.

After BBCVID digital twin Blockchain digitizing all border crossing documentation, e-gate is able to be made aware of dynamic information through digital twin duplicate effects. That is to say, if a real-world bodily person has obtained border crossing permit from the border agency, his digital twin identity projected into the digital-world should be able to reflect this dynamic change as well.

Therefore, after imposing our proposal, two major changes will occur to the e-gate system. First, E-gate is available for all travellers regardless visa and customs clearance documentation are required or not. Second, rather than reading static microchip information from existing e-passport book, the proposed VS border control Metaverse DAO generates dynamic quick response(QR) code [42] as border crossing permit for immigrants to pass through the e-gates.

Before offering a comprehensive description about how a border crossing permit is generated by VS Metaverse DAO, understanding both individual immigrant and commercial business vehicle loaded with commercial products border crossing processes are very important as well.

To understand the automatic border crossing process for individual immigrant control, it has to compile the immigration law of the country as the foremost premise; therefore, both the legitimacy of entering the specific country and the identity of the immigrant have to be confirmed and verified before the border crossing event happening. To breakdown this process, it can be described as:

1) Allow individual immigrant to obtain border crossing legitimacy credential(e.g. visa, customs clearance documents) and identity credential(e.g. passport).
2) Immigrants bring these credentials to the airport or land border checkpoints.
3) Upon the present of the immigrant, border crossing legitimacy documentation, and identity credentials at the border crossing checkpoint, border officer has to conduct:
    a) Border crossing legitimacy documentation verification.
    b) Identity authentication.
    c) Granting border crossing permit.
    d) Stamping and recording the border crossing event on passport book.

Therefore, to automatize above individual immigrant border crossing process, VS Metaverse DAO is able to complete all above procedures through smart contracts.

To understand the automatic border crossing process for customs inspection, the main task is to ensure the *data consistency* between customs clearance documentations and the real time live in-situ border crossing events, which inspected objects include the vehicle identity, driver identity, and products declared to enter the country [43]. To put more in detail, the main target subjects should be inspected include:

- Driver. The identity of the driver, and driver's legitimacy of entering.
- Vehicle. The identity of the vehicle, and vehicle legitimacy of border crossing etc.
- Products. The products related documentations such as packaging list, invoices, product model and category etc, the origin of the products, import permits, licenses and certificates, and customs clearance documentations etc.

To enable automatic reconciliation of information beyond the BBCVID digital twin on the blockchain, a border checkpoint surveillance system is essential. This system is responsible for collecting live, in-situ data from border checkpoints. Specifically, it gathers data through Internet of Things (IoT) devices deployed at these checkpoints, making the overall system a combined IoT and blockchain solution.

- CCTV camera for vehicle number plate and vehicle colour.
- Weight sensor to weight vehicle's weight. The output is the weight of the vehicle in kilogram.
- X-ray scanner for loaded product inspections. The output is a Boolean to suggest if further inspection is required or not: either Yes or No.

These four data elements will be grouped as a tuple, e.g. a JSON data object {"vehicle number plate": "AB12CDE", "vehicle colour": "blue", "weights": 1250, "further inspections": "No"}, and then send to VS Blockchain as border crossing permit transaction endorsement.

Algorithm 1 Biometric Identity Authentication.

```
REQUIRE:
$DID,\ DID\ Documentation,\ collected\ biometric\ sample(CBC)$
Smart Contract Initiation
if$(1)\ proofValue \equiv SignAlgo(verificationMethod)$
then$(2)\ hash1 \leftarrow SHA256(bio\_template)$
    if$(3)\ hash1 \equiv SHA256(bio\_template)$
    then$(4)\ dist_i \leftarrow match\ CBCwith\ bio\_template.$
        for $i \leq 2$
        if$(5)\ dist_i \leq controlled\ threshodl\ \sigma$
        then$(6)\ `success' \leftarrow\ identity\ is\ authenticated.$
        else
        $(6)\ `fail' \leftarrow\ identity\ is\ not\ authenticated.$
        $(7)\ ask\ CBC\ re-submission$
        $(8)\ repeat\ (1)-(5)$
        end if
        end for
    else
    $(4)\ `fail' \leftarrow\ identity\ is\ not\ authenticate.d$
    $(5)\ bio\_template\ is\ modified,\ report\ to\ system\ CA.$
    $(6)\ system\ CA\ recollect\ bio\_template.$
    $(7)\ system\ CA\ update\ DID\ and\ DID\ Documentation.$
    end if
else
$A\ fake\ DID\ documentation\ is\ found.$
end if
$Biometric\ identity\ authentication\ is\ completed.$
```

To offer a comprehensive description about how an individual immigrant uses the proposed biometric e-passport to get across the border through VS Metaverse DAO smart contracts transactions, the immigrant is required to submit border crossing permit application to VS Blockchain first over the mobile application. The application indeed is a Hyperledger transaction proposal, which the application data is digitally signed by immigrant's private key. VS system CA(the same entity with BBCVID system CA) gateway service receives the transaction proposal from mobile client and then transfers it to one of the VS peer node to execute the transaction.

To put more details in, the smart contract will initiate facial identity authentication first via e-passport over mobile application by Algorithm 1, see Fig. 5 for facial image identity authentication at the mobile DApp. Then verify the visa document if the immigrant has one. If all verification goes well, the VS peer node will sign on the transaction to make an endorsement, and then return it back to the immigrant. Immigrant will pack endorsed transaction, sign on it, and then sent it to VS system CA for transaction validation. VS system CA is also the orderer of the VS Blockchain, who validates the transaction, generates border crossing permit, orders the transaction into VS Blockchain block, and broadcast it to the rest of peer nodes for validation and commitment. That is to say, the immigrant's border crossing permit application will initiate a corresponding smart contract which is able to accomplish above process. The validated transaction is the specific border crossing permit documentation, which its representation is the QR code.

Explanation of SHA-256 Usage: The SHA-256 cryptographic hash algorithm is applied here to securely hash the biometric template (bio_template) collected from the individual. By hashing, the system ensures that the biometric data cannot be tampered with or reverse-engineered, protecting user privacy and data integrity. During authentication, the freshly captured biometric sample is hashed and compared to the stored hashed template to verify identity without exposing raw biometric data. This process strengthens the security and authenticity of the biometric e-passport system by integrating cryptographic guarantees into biometric matching.

Upon arrival at airport or land border e-gates, immigrants use a QR code to initiate crossing by undergoing fingerprint identity authentication. After successful authentication, the e-gate returns a digitally signed endorsement transaction to the immigrant's mobile client. The client packages this endorsed transaction into an envelope, digitally signs it, and submits it to the VS system CA for ordering service. The VS system CA validates the endorsements and signatures, orders the transaction into a new VS Blockchain block, and broadcasts it to peer nodes for validation and commitment. The immigrant then receives an immutable, timestamped blockchain record of the border crossing for future reference. This process, similar to existing systems like Clear, aims to streamline border crossings for enrolled individuals. However, initial enrollment and identity verification remain rigorous to ensure security, meaning significant time savings occur primarily for pre-registered travelers.

To offer a comprehensive description about how customs inspection is conducted at border checkpoint through VS Metaverse DAO smart contracts, the border crossing permit should be obtained beforehand before a vehicle driving through the border booth-like e-gate. For a private vehicle to drive through the border checkpoint, apart from all individual immigrants border crossing permits, vehicle's border crossing permit should be obtained from DVLA beforehand as well. For a commercial vehicle to drive through the border checkpoint, apart from individual and vehicle border crossing permit, the loaded products on the commercial vehicle should obtain border crossing permit as well from HMRC for customs clearance.

To start with, in order to submit the border crossing permit application, the commercial business entity who owns the commercial vehicle is required to obtain the digital twin for both the vehicle and the business entity in accordance with Algorithm 2. To put more in detail, the owner of the commercial vehicle and the business entity is the 'controller' of the corresponding digital twin, who is assumed to have full control over the subject that the DID referent to(e.g. vehicle and the commercial business entity).

Algorithm 2 Border Crossing Document Digital Twin

```
REQUIRE:
DID, document application data form
Smart Contract Initiation
(1) Application form information verification.
if application form information is verified
    (2) Biometric identity authentication.
    (3) Generate document DID.
    (4) Generate document DID′s docmentation.
    (5) Digital sign on DID docmentation.
else
Ask applicant to resubmit data form.
end if
Generating border crossing document digital twin
 is completed.
```

Then both the commercial and the private vehicle border crossing permit application can be made through the proposed mobile DApp. To add more details in, the commercial border crossing permit application starts with a form which the loaded products invoice, packaging lists, vehicle number plate, driver's visa (if required), and driver's e-passport number are to be filled. The mobile client collects those data and allows the commercial entity owner to digitally sign the border crossing permit application (transaction proposal), and then sends it to VS system CA peer nodes to execute the transaction through the VS gateway service. The VS system CA peer node initiates the corresponding smart contract and re-directs the transaction proposal to the rest of organizations who are required to endorse this transaction in accordance with the endorsement policy in the smart contract.

The smart contracts in our framework are implemented using **Solidity**, the widely adopted programming language for Ethereum-compatible blockchain platforms. Solidity enables the definition of endorsement policies, validation logic, and transaction state updates in a secure and transparent manner. This choice supports compatibility with the underlying permissioned blockchain network used in the VS system and facilitates flexible, modular smart contract deployment and upgrades.

Specifically, by running the corresponding smart contract, below four maneuvers are taken in parallel:

- Individual person biometric identity authentication and border crossing legitimacy verification. Driver's facial identity will be authenticated in accordance with driver's biometric e-passport, which the facial image will be collected through driver's own mobile DApp. In the case a visa is also required for the driver to pass through the border, VS Metaverse DAO is able to make visa verification as well. If all goes well, the VS system CA peer node will digitally sign on it to make an endorsement and return it back to business entity's mobile client.
- Products border crossing legitimacy verification. Upon receiving the products invoice number and packaging lists, HMRC is able to automatically identify what customs clearance documentations are required from the commercial business entity. HMRC then verifies customs clearance documents accordingly. After all verification is completed, HMRC is required to endorse the transaction as well and then sends the endorsement back.
- Vehicle border crossing legitimacy verification. DVLA verifies vehicle border crossing legitimacy by verifying vehicle digital twin documentation and searching if the vehicle has been reported lost or has any illegal records etc. If all goes well, DVLA will endorse this transaction and sends it back to the commercial business entity mobile client.
- Border checkpoint surveillance system live data collection. There is a border road surveillance unit constructed which is about 2-3 kilometers away from the border e-gate. Surveillance system collects vehicle number plate, vehicle colour, weights, and x-ray scan live data. The surveillance system then endorses the commercial business border crossing transaction proposal, and sends it back to the business entity.

The applicant mobile client collects all digitally signed endorsements and packs them into a data envelope to let applicant (commercial business owner) digitally sign it. The data envelope then is sent to VS system CA for validation. VS system CA validates all digital signatures in the envelope and then reconciles all endorsements. If all goes well, VS system CA issues the border crossing permit (QR code) for the commercial business entity specified vehicle driver.

The VS generated QR code is the border crossing permit which is able to allow the commercial vehicle driver to complete fingerprint identity authentication at border e-gate. After driver's fingerprint is authenticated, driver is able to drive the vehicle to get across the e-gate. VS system CA then is able to this instance as an immutable transaction recorded on VS Blockchain.

IV. System Implementation and Evaluation

To properly evaluate our proposal, the system is implemented and simulated using a permissioned private blockchain based on Hyperledger Fabric. Both BBCVID and VS frameworks are deployed as separate Fabric networks. Specifically, the BBCVID network consists of two organizations, DVLA and HMRC, each with a single peer node. An ordering service, referred to as BBCVID system CA, manages consensus and transaction ordering. Docker containers are used to create independent peer databases as persistent "volumes". Similarly, the VS network includes three organizations: DVLA, HMRC, and the border surveillance system, sharing the same ordering service (BBCVID system CA)[1]. Both networks use the Raft consensus protocol [44] and maintain a single channel for transaction communication. To benchmark and validate the performance characteristics of these Fabric-based networks, such as throughput, latency, and transaction consistency, we utilize Hyperledger Caliper. Caliper acts as a performance evaluation tool to measure the efficiency of our Fabric deployments, while Fabric itself serves as the permanent blockchain platform to securely store government records and execute smart contracts. This distinction ensures both rigorous testing and robust, immutable data storage suitable for border control applications.

All BBC ABC system user are connected through developed Android mobile DApp(JAVA) user interface and communicate to BBC ABC Hyperledger Fabric test network through Fabric Gateway Service. Most important, to this project system implementation, the local Hyperledger test network is build upon Ubuntu 20.04.3 LTS sub-system in Window 10 Version 22H2(OS Build 19045.2846) through Windows-Subsystem-for-Linux 2(WSL 2).

A. Transactions

For private Hyperledger Fabric Blockchain, the standardized transaction is made through three phases [17], which specifically are:

Phase 1: Transaction proposal and endorsement.

Phase 2: Transaction submission and ordering.

Phase 3: Transaction validation and commitment.

For transactions on BBCVID , the entire procedure are proposed in accordance with the border control workflow. To put more in detail, in *BBCVID*, a transaction is made to obtain either the proposed e-passport or other digital verifiable credential such as visa and customs documentations etc. A valid BBCVID transaction is defined as in below steps:

Phase 1: E-passport, visa, and customs documentation applicants submit a signed transaction proposal through our mobile application client to the relevant node by connecting to the corresponding gateway service. Like for instance, if the applicant is to obtain digital verifiable customs documentation, the gateway service should offered by HMRC's node. The gateway service will forward applicant's transaction proposal to all relevant nodes to execute the transaction in accordance with the endorsement policy[2] of the smart contract. Finally all nodes return a digitally signed response back to applicant's client.

Phase 2: The mobile client pack all responses obtained from Phase 1 into an envelop and let applicant to sign it. Application client submit the signed envelop to CA's gateway service, and a 'success' message will be delivered back to the client if the submission is successful. Upon receiving the response, CA will verify all the signatures in the envelop and then orders the transaction. The transaction will be ordered into a new block of the BBCVID.

Phase 3: CA will broadcast the ordered transaction to the rest of peer nodes to validate the transaction and then commit it to BBCVID. Applicant will get full access permit to this new ledger.

By similar token, in *VS*, a transaction is made to obtain a border crossing permit, and a immutable, time stamped digital record of the border crossing event for future references. Compared with BBCVID, VS transactions always have an endorsement police of 4 of 4, compared with 1 of 2 in BBCVID. Apart from that, the rest transaction procedures are very similar.

B. Android Mobile DApp

Android mobile operation system runs on Linux kernel that connects its hardware with its software stack. To preserve private data privacy and security, Android has built-in trusted execution environment, which indicates that the biometric information is encrypted and stored in a separated part of the Android smart phone [45]. Most important, it is completely inaccessible to the regular operating system. To make the system even more secure and privacy-preserving, "permissions" are used in Android whenever an access to sensitive and protected information is raised, such as GPS location and open camera etc. If user does not grant the permission, the access will be denied straightaway [46].

To start with, the Android mobile application access is granted to registered user only. To add on more detail, user name, email address and a six-digits PIN number are required to complete the new user registration process.

After obtain the access to mobile application, the access to BBCVID and VS Blockchain should be obtained as well. To put more details in, the Hyperledger Fabric certificate authority(Fabric CA) has three main functions in our proposed system, which include:

- User identity connects to lightweight directory access protocol(LDAP) as the user registry.
- Public key based identity certificate issuance for users, and TLS certificate issuance for nodes and clients.
- Certificate renewal, revoked, and management.

C. BBC ABC Hyperledger Blockchain Performance

[47] also claims that below metrics can be used to evaluate Blockchain network performance. First, transaction latency.

[1] BBCVID system CA and VS system CA refer to the same ordering service entity, here called BBC ABC system CA.

[2] Endorsement policy is a compulsory part of Hyperledger smart contract, and it clarifies which specific organization(s) must sign the transaction in order to make it valid [25].

From a network-wide side, the amount of time that a transaction costs from its initiation to the point of its validation form is available to the whole network, which also includes the time for broadcasting. Most important, [47] also recommends to use all nodes in the system under test(SUT) to get a better evaluation of transaction latency. Specifically,

$$transaction\ latency = (confirmation\ time\ @\ network\ threshold) - submit\ time \tag{1}$$

Second, transaction throughput. It is the rate of validate transaction are committed to the Hyperledger Fabraic Blockchain during defined time scope. In most cases, it is represented by transactions per second. Specifically,

$$transaction\ throughput\ =\ total\ committed\ transactions/\ total\ time\ in\ seconds \tag{2}$$

To add on, Hyperledger Caliper [48], which is an established Blockchain use case based performance evaluation tool, is used to evaluate the BBCVID and VS Hyperledger Fabric Blockchain performance. Specifically, the Hyperledger Caliper parameters are:

- Hyperledger Caliper version 0.5.0;
- Hyperledger Fabric 2.4 is bound to the Hyperledger Caliper;
- There are four bare metal machines to host Caliper workers;
- Endorsement policy is 1 of Any in BBCVID but 3 of 4 in VS;
- 200 Caliper worker are used in both BBCVID and VS;
- TLS is enabled in both BBCVID and VS.

Most important, some block cutting parameters are also introduced to both BBCVID and VS. Specifically,

- Block cut time. [3]: 2 seconds.
- Block size. [4]: 500.
- Preferred maximum bytes: 2Mb.

The proposed Android mobile application uses Google Firebase as user database and LevelDB as Hyperledger Fabric state databases, gateway service concurrency limit manually sets to 20,000 per second.

With above testing environment being declared, since Hyperledger Fabric private Blockchain does not suffer scalability issue and transaction throughput can be manually adjusted as a system parameter, only transaction latency is assessed and discussed. To put more in detail, since both BBCVID and VS Hyperledger Blockchain transactions are mostly to write blind key value in its transaction; therefore, assessed blind write per 1000 and per 100 byte performance is listed as in Table I for BBCVID Blockchain and Table II for VS Blcokchain with a fixed TPS at 3000.

That is to say, since both BBCVID and VS Hyperledger Blockchain runs on test network with Raft consensus rule, the transaction is finalized as soon as the orderer validates the transaction, which refers to the orderer has immediate finality. Therefore, the latency performance is evaluated for each peer node in the terms of how long it takes to commit a validated transaction, which leads to a “minimum latency”, “maximum latency”, and “average latency”. Even though Hyperledger Fabric test network has pre-defined concurrency limit for 20,000 transaction per second(TPS), this assessment fixes it to 3000 to make it compatible with our hardware system. Therefore, the “send rate(TPS)” and “throughput” are both around 3000 in both cases. However, the general performance of “blind write 100 byte” outperforms the “blind write 1000 byte”.

Indeed, the performance in BBCVID and VS is closely related with the peer node size, which each node has the potential to make an impact on the entire system performance based on endorsement policy. Therefore, the average transaction latency performance is assessed based on 1, 4, 7, and 10 nodes. Specifically, see Fig. 6 for the average latency performance in terms of the number of the BBCVID orderer node changes, and Fig. 7 is for VS Blockchain. Similarly, Fig. 8 for the minimum and maximum transaction latency performance in terms of 1, 4, 7, and 10 orderer nodes in BBCVID, and Fig. 9 is for VS Blockchain.

Last but not least, packet loss is another relevant assessment criteria to be evaluated in Blockchain network. In BBCVID, the packet loss is 0.15% by Equation 3 blind write per 1000 bytes compared with 0.09% per 100 bytes. In VS, the packet loss is 0.06% blind write per 1000 bytes compared with 0.04% per 100 bytes. That is to say, blind write per 100 bytes has lower packet loss rate in both BBCVID and VS Blockchain, and VS packet loss performance is better than BBCVID overall. That is because VS has four peer nodes collecting packets from message sender but BBCVID has one node only, see Table III for a demonstration of the packet loss rate comparison between BBCVID and VS.

$$packet\ loss = (1 - throughput \div send\ rate) \times 100\% \tag{3}$$

Explanation of Contribution: The proposed BBCVID system is designed to demonstrate utility in terms of speed, consistency, and fraud reduction. Unlike the current manual border control process—where vehicles are individually checked and documented by hand, leading to logistical delays—our system enables automated, real-time vehicle identification and verification. This contributes to more efficient border crossing, reduced human error, and improved resistance to fraudulent activities.

D. BBC ABC Border Control Efficiency Performance

In accordance with [1], soft border system can be analyzed through cost and leveraging existing system criteria. In this proposal, the computational cost and the duration of border crossing are specifically evaluated.

First, transaction cost. Blockchain as a distributed network constructed from open source codes, the system security is always crucial. In chapter 5, it has been well explained that public Blockchain like Bitcoin and Ethereum Blockchain charge transaction fees and gas fee to protect system security and constrain the public resources wastage. However, Hyperledger

[3] Cut time: Cut time is the upper bound for how long a new block has to be cut even it is still not full by then.

[4] Block size: How many transactions per block should be ordered before the block is cut.

TABLE I
PERFORMANCE COMPARISON OF BLIND WRITE 1000 AND 100 BYTE KEY VALUE ON BBCVID.

Name	Send Rate (TPS)	Max Latency (Seconds)	Min Latency (Seconds)	Avg. Latency (Seconds)	Throughput TPS
Blind Write 1000B	2989.2	3.9	0.46	2.16	2984.8
Blind Write 100B	2992.3	2.8	0.34	1.58	2989.5

TABLE II
PERFORMANCE COMPARISON OF BLIND WRITE 1000 AND 100 BYTE KEY VALUE ON VS.

Name	Send Rate (TPS)	Max Latency (Seconds)	Min Latency (Seconds)	Avg. Latency (Seconds)	Throughput TPS
Blind Write 1000B	2988.7	4.21	3.75	4.02	2986.8
Blind Write 100B	2991.3	3.23	2.25	2.78	2990.1

TABLE III
BLIND WRITE PACKET LOSS RATE COMPARISON BETWEEN BBCVID AND VS.

Packet Loss Rate	Blind Write per 1000B	Blind Write per 100B
BBCVID	0.15 %	0.09%
VS	0.06%	0.04%

TABLE IV
A COMPARISON BETWEEN EXISTING AND THE PROPOSED BORDER CONTROL SYSTEM IN THE REGARD OF BORDER CROSSING DURATION.

Dur.(minutes)	Indiv. Immigrants	Pvt. Vehicle	Cml. Vehicle
Existing ABC	1.25	5.25	20.25
Proposed ABC	0.33	2.47	2.62
Improvement	278.79%	112.55%	672.90%

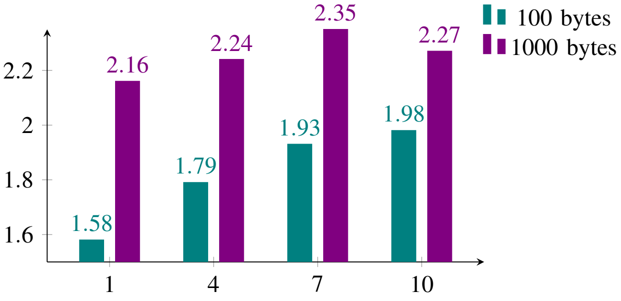


Fig. 6. BBCVID: Average latency for 1, 4, 7, and 10 orderer nodes.

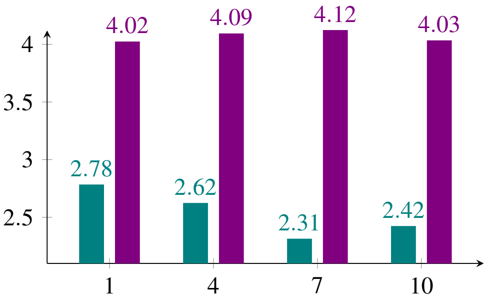


Fig. 7. VS: Average latency for 1, 4, 7, and 10 orderer nodes.

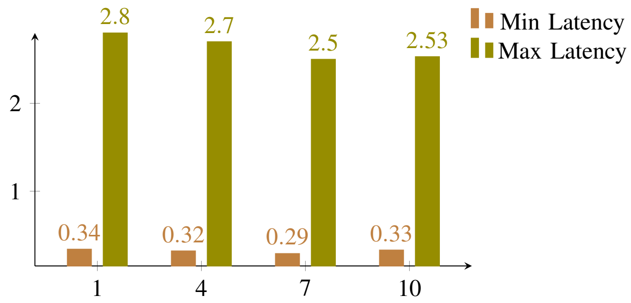


Fig. 8. BBCVID:Min. and max.latency for 1, 4, 7, and 10 orderer nodes of 100 byte blind write.

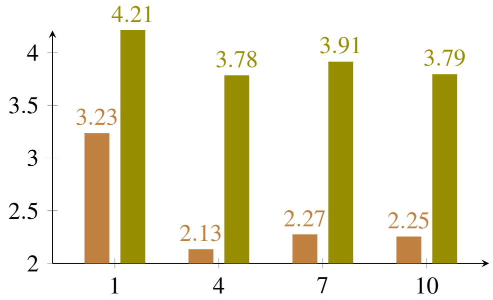


Fig. 9. VS:Min. and max.latency for 1, 4, 7, and 10 orderer nodes of 100 byte blind write.

Fabric Blockchain as private Blockchain, it uses user identity authentication tactic to secure the system security, which makes zero transaction fee possible. That is to say, transaction has zero fee for all operations on Hyperledger Fabric regardless energy costs [47], compared with Bitcoin Blockchain has an average of USD 5.10 and Ethereum Blockchain has an average of USD 4.19 per transaction fee in March 2023 [49].

Second, running a full node cost. Both BBCVID and VS are Hyperledger Fabric private Blockchain. Therefore, to run a full node, there are some minimum requirements in terms of hardware and network performance [50]. Specifically, since each full nodes has a potential of making an impact on the entire Blockchain network performance in accordance with consensus rule and endorsement policy, persistent and fastest disk storage, a minimum of 1 Gbps network connection between all nodes and organizations, and 1 CPU with 2 GB of memory for orderer nodes are all encouraged [50].

Third, the computational costs in the proposed BBC ABC system include:

(1)Digital verifiable documentation verification including proposed e-passport, visa, and customs clearance documentations etc. To be more precise, in this proposal, Edwards-Curve Digital Signature Algorithm (EdDSA) [51] is used to generate the digital signature attached to all BBCVID generated digital verifiable document, as this algorithm is recommended by W3C DID core [35] and EdDSA Cryptosuite [37] particularly for DID credentials. Specifically, in our test environment, the digital signature verification only takes an average of 0.27 seconds for accumulated 100 document(file size 1.9KB to 2.1KB) verification simulation instances.

(2)Biometric identity authentication through proposed e-passport. That is, Facial image identity authentication. VGG-face recognition method [52] to conduct facial image authentication, which the image size is limited to 100 x 32 bits. It takes 9.52 seconds to complete the facial identity authentication over proposed e-passport. As facial image is captured live over mobile application camera, the majority time is spent on the facial image collection, which is estimated about 3-4 seconds minimum. The test results is achieved through author simulates 20 instances by her own mobile client.

what is more, fingerprint identity authentication is only conducted at border checkpoint e-gates, which minutiae-based two dimensional feature vector matching is deployed. Since fingerprint data is *not* available in a large scale, author uses her own fingerprint data collected from U.are.u 5300 fingerprint scanner(USB 2.0, FIPS 201/PIV, FAP 30, optical, resolution: 500 dpi, 256 levels of gray) to do the test for simulating 20 instances. By initiating 'biometric identity authentication' smart contract on BBCVID Blockchain, it takes an average of 4.75 seconds.

(3)Border crossing permit generation. Starting from the border crossing applicant submits the border crossing permit application, VS BA is not able to generate the border crossing permit until all required endorsement is received. To put more in detail, there are three organizations are required to endorse a border crossing permit transaction, which include HMRC, DVLA, and the Surveillance system. Indeed, as soon as applicant submits the application, HMRC and DVLA is able to endorse the transaction straightaway; however, the surveillance system has to wait the applicant drive the declared vehicle to the border checkpoints so that the endorsement can be conducted. Therefore, the gap time of waiting the vehicle to drive-through the border checkpoint road unit will not be count into the computational cost.

Therefore, for commercial entity to obtain a border crossing permit with 20 documents to be verified altogether, the estimated computation cost is:

$$20 \times 0.27 + 9.52 + 120 + 4.02 \times 4 = 2.52\, minutes \tag{4}$$

which is the sum time of 20 documentation verification, facial image identity authentication over mobile application by e-passport, assumed surveillance system required time to collect live data from border checkpoint units(120 seconds), required 3 endorsements from three different organizations, and one transaction commitment from VS BA. Particularly, the average transaction latency for 1000 bytes blind write is adopted as the transaction time.

For individual immigrant to obtain a border crossing permit with one visa documentation, the computational cost is:

$$0.27 \times 2 + 9.52 + 4.02 = 0.23\, minutes \tag{5}$$

Which is the sum time of visa and e-passport two documentation verification, facial identity authentication over mobile application by e-passport, and one transaction commitment from VS BA.

For individual immigrants to obtain a border crossing permit with one personal vehicle, the computational cost is:

$$0.27 \times 3 + 9.52 + 120 + 4.02 \times 3 = 2.37\, minutes \tag{6}$$

Which is the sum time of visa, vehicle DID documentation, e-passport three documentation verification, facial identity authentication over mobile application, assumed surveillance system required time to collect live data from border checkpoint units(120 seconds), required two endorsement from DVLA and the surveillance system, and the VS BA transaction commitment.

For VID Blockchain border crossing event recording. The border crossing event recording refers to use the border crossing permit at the border e-gate to conduct fingerprint biometric identity authentication, and then recording it by committing this transaction on VS Blcokchain. Therefore, the computational cost is:

$$0.27 + 4.75 + 1 = 6.02\, seconds \tag{7}$$

Which is the sum time of one e-passport verification, fingerprint identity authentication at e-gate through the e-passport, and estimated time cost to scan the QR code(1 second).

In accordance with [1], existing border crossing e-gate requires 20 to 30 seconds to complete fingerprint identification and 15 to 20 second for photo facial image identity authentication. Plus, additional manual registration would be required in many occasions, which costs about 30 to 60 seconds per instance.

Therefore, a reasonable estimation of border crossing duration can be made in existing border control system. Specifically, for commercial vehicle getting across the border with 20 documents to be verified all together, the border crossing duration is 20.25 minutes($30 \times 20 + 15 + 10\, minutes$) including the time of 20 documentation verification, facial identity authentication at e-gate, and estimated vehicle loaded products inspection time(10 minutes). For individual immigrants getting across the border, the border crossing duration is 1.25 minutes($15 + 30 \times 2$) including facial image identity authentication at border e-gate and passport and visa documents manual verification. For individual immigrants getting across the border with private vehicle, the border crossing duration duration is 5.25 minutes($15 + 30 \times 4 + 3\, minutes$) including facial image identity authentication at border e-gate, visa, passport, driving license, and vehicle registration four document verification, and estimated vehicle inspection time at border checkpoints(3 minutes). Comparing with our proposed system which is discussed in above 'computational cost', the corresponding duration is 2.62 minutes, 0.33 minutes, and 2.47 minutes which including the time of obtaining the border crossing permit and obtaining the border crossing event immutable records, see Table IV for a comparison between existing border control system and the proposed border control system in the regard of border crossing duration.

V. Conclusion and Future Works

In this paper, sorting existing border control low efficiency issue is targeted as the main goal. Through our research, the causation of that can be summarized into two folds, which specifically are manual documentation verification and the static identity credential. To be more precise, proving border crossing legitimacy involves a good amount of documentation verification, such as identity credential passport, individual immigrant border crossing legitimacy proof visa, and commercial products border crossing legitimacy proof customs clearance documents etc. Apart from existing e-passport, all the rest of documentation verification has to be manually conducted by border control officer, which is deemed very time-consuming. Most important, current e-passport contains static information that is locked in the e-passport book microchip, which does not only suffer all inconvenience embedded with distance but also makes binding dynamic border crossing legitimacy to the passport extremely difficult.

To transform existing border control manual documentation verification into automatic process, the tangible border crossing legitimacy documentation has to be digitized. Therefore, a real world verifiable documentation digital twin data model is constructed.

To further automatizing the border control process, a border control Metaverse DAO is constructed. To be more precise, through the construction of BBC ABC Metaverse DAO system, the border crossing efficiency is improved by 354.75% on average, which specifically has 112.55% minimum improved efficiency under individual immigrants with private vehicle border crossing scenario and 672.90% highest improved efficiency under commercial vehicle loaded with commercial products border crossing scenario.

References

[1] PwC, "Technical study on smart borders: Final report," European Commission, Tech. Rep., 2014. [Online]. Available: https://home-affairs.ec.europa.eu/system/files/2020-09/smart_borders_technical_study_en.pdf

[2] F. Brown. (2022) Huge 15km lorry queues at dover blamed on brexit. Metro.co.uk. [Online]. Available: https://metro.co.uk/2022/01/22/huge-15km-lorry-queues-at-dover-blamed-on-brexit-15964763/

[3] B. Xu, T. Agbele, and R. Jiang, "Biometric blockchain a better solution for the security and trust of food logistics," *IOP Conference Series: Materials Science and Engineering*, vol. 646, 2019.

[4] B. Xu *et al.*, "Biometric blockchain (bbc) based e-passports for smart border control," in *Big Data Privacy and Security in Smart Cities: Advanced Sciences and Technologies for Security Applications*, 2022, ch. 13, pp. 235–248.

[5] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (bbc) to prevent attacks in vanet," *IEEE Access*, vol. 9, pp. 87 299–87 309, 2021.

[6] A. Alharthi, Q. Ni, R. Jiang, and M. A. Khan, "A computational model for reputation and ensemble-based learning model for prediction of trustworthiness in vehicular ad hoc network," *IEEE Internet of Things Journal*, 2023.

[7] K. Aleksi, H. Antti *et al.*, "Empowering citizens with digital twins: A blueprint," *IEEE Internet Computing*, vol. 26, no. 5, pp. 7–16, 2022.

[8] L. H. Lee, T. Braud *et al.*, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," arXiv preprint arXiv:2110.05352, 2021.

[9] Y. T. Wang, Z. Su *et al.*, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, 2022.

[10] S. B. Far and A. I. Rad, "Applying digital twins in metaverse: User interface, security and privacy challenges," *Journal of Metaverse*, vol. 2, no. 1, pp. 8–15, 2022.

[11] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, "On the internet, nobody knows you're a dog," *New Yorker*, vol. 69, 1993.

[12] P. Grassi, M. Garcia, and J. Fenton, "Nist digital identity guidelines," National Institute of Standards and Technology (NIST), 2020.

[13] NIST FIPS, "Standards for security categorization of federal information and information systems," NIST FIPS, Tech. Rep. 199, 2004.

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.

[15] A. Wright, "The rise of decentralized autonomous organizations: Opportunities and challenges," *Stanford Journal of Blockchain Law & Policy*, vol. 4, no. 2, pp. 152–176, 2021.

[16] Yahoo! (2023, Feb) Bitcoin historical data. Yahoo Finance. [Online]. Available: https://finance.yahoo.com

[17] L. Anthony *et al.* (2021) An overview of hyperledger foundation. Hyperledger.org. [Online]. Available: https://www.hyperledger.org

[18] Y. N. Li *et al.*, "Non-equivocation in blockchain: Double-authentication-preventing signatures gone contractual," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 859–871.

[19] A. Omar *et al.*, "A comparative study: Blockchain technology utilization benefits, challenges and functionalities," *IEEE Access*, vol. 9, pp. 12 730–12 749, 2021.

[20] U. Bodkhe *et al.*, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79 764–79 800, 2020.

[21] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–639, 2014.

[22] L. Kleinrock, "Distributed systems," *Communications of the ACM*, vol. 28, no. 11, pp. 1200–1213, 1985.

[23] (2023) Bitcoin developer guide: Contract. Bitcoin.org. [Online]. Available: https://developer.bitcoin.org/devguide/contracts.html

[24] P. Wackerow. (2023) Introduction to smart contracts. Ethereum.org. [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/

[25] V. Bharathan *et al.* (2021) Hyperledger architecture, volume ii: Smart contracts. Hyperledger.org. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

[26] H. Konstantinos and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[27] Z. L. Wang *et al.*, "Ethereum smart contract security research: survey and future research opportunities," *Frontiers of Computer Science*, vol. 15, no. 2, 2020.

[28] N. Lu *et al.*, "Neucheck: A more practical ethereum smart contract security analysis tool," *Software: Practice and Experience*, vol. 51, no. 10, pp. 2065–2084, 2020.

[29] S. Wang *et al.*, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[30] F. Matheus *et al.*, "Dynamic posted-price mechanisms for the blockchain transaction-fee market," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 86–99.

[31] L. Kashif, "Metaverse: why, how and what," 2022, how and What.

[32] M. Stylianos, "Metaverse," *Encyclopedia*, vol. 2, no. 1, pp. 486–497, 2022.

[33] H. Thien *et al.*, "Blockchain for the metaverse: A review," *Future Generation Computer Systems*, 2023.

[34] T. D. Moshood *et al.*, "Digital twins driven supply chain visibility within logistics: A new paradigm for future logistics," *Applied System Innovation*, vol. 4, no. 2, p. 29, 2021.

[35] M. Sporny *et al.* (2022) Decentralized identifiers (dids) v1.0 core architecture, data model, and representations. W3C.org. [Online]. Available: https://www.w3.org/TR/did-core/

[36] M. Sporny, D. Longley, and D. Chadwick. (2022) Verifiable credentials data model v1.1. W3C.org. [Online]. Available: https://www.w3.org

[37] S. Josefsson, "Edwards-curve digital signature algorithm (eddsa)," Internet Research Task Force (IRTF), 2020. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8032

[38] O. Steele, M. Sporn, and T. Looker, "Eddsa cryptosuite v2020," W3C.org, 2022. [Online]. Available: https://www.w3.org/community/reports/credentials/CG-FINAL-di-eddsa-2020-20220724/

[39] W. A. Ahmed and A. Rios, “Digitalization of the international shipping and maritime logistics industry: a case study of tradelens,” in *The Digital Supply Chain*. Elsevier, 2022, pp. 309–323.

[40] T. I. Kang, “Korea pilots blockchain technology as it prepares for the future,” World Customs Organization news, 2023.

[41] S. C. Santamaria, “Cadena, a blockchain enabled solution for the implementation of mutual recognition arrangements/agreements,” World Customs Organization news, 2023.

[42] B. Muthukumar, M. J. Albert, G. Nambiar, and D. Nair, “Qr code and biometric based authentication systems for trains,” *IOP Conference Series: Materials Science and Engineering*, 2019.

[43] M. K. Khoshons, C. C. Clark, and S. Tarek, “Simulation and evaluation of international border crossing clearance systems: a canadian case study,” *Transportation Research Record*, vol. 1966, no. 1, pp. 1–9, 2006.

[44] D. Y. Huang, X. L. Ma, and S. L. Zhang, “Performance analysis of the raft consensus algorithm for private blockchains,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 172–181, 2019.

[45] J. E. Ekberg, K. Kostiainen, and N. Asokan, “Trusted execution environments on mobile devices,” in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 2013, pp. 1497–1498.

[46] S. Rajinder, “An overview of android operating system and its security,” *International Journal of Engineering Research and Applications*, vol. 4, no. 2, pp. 519–521, 2014.

[47] M. Adulla *et al.* (2023) Hyperledger blockchain performance metrics. Hyperledger.org. [Online]. Available: https://www.hyperledger.org/learn/publications/blockchain-performance-metrics

[48] (2023) Hyperledger caliper: Getting started. Hyperledger.github.io. [Online]. Available: https://hyperledger.github.io/caliper/v0.5.0/getting-started

[49] (2023) Average transaction fee chart. Etherscan.io. [Online]. Available: https://etherscan.io/chart/avg-txfee-usd

[50] (2023) Hyperledger fabric: Performance considerations. hyperledger-fabric.readthedocs.io. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/performance.html

[51] S. Josefsson and I. Liusvaara, “Edwards-curve digital signature algorithm (eddsa),” Tech. Rep., 2017.

[52] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep face recognition,” in *Proceedings of the British Machine Vision Conference (BMVC)*. BMVA Press, 2015, pp. 41.1–41.12. [Online]. Available: https://dx.doi.org/10.5244/C.29.41

Bing Xu reveived the BSc degree in Business Administration with first degree in Dongbei University of Fiance and Economics, Dalian, China, MA degree in Philosophy, politics and economics in York University, York, U.K. She current is a PhD candidate with Department of Computing and Communications, Lancaster University, Lancaster, U.K. Her research focus on Blockchain and biometric Blockchain based identity system.

Qiang Ni is currently a Professor at the School of Computing and Communications, Lancaster University, Lancaster, U.K. His research interests include the area of future generation communications and networking, including green communications and networking, millimeter-wave wireless communications, cognitive radio network systems, non-orthogonal multiple access (NOMA), heterogeneous networks, 5G and 6G, SDN, cloud networks, energy harvesting, wireless information and power transfer, IoTs, cyber physical systems, AI and machine learning, cyber security, big data analytics, and vehicular networks. He has authored or co-authored 300+ papers in these areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to various IEEE wireless standards.

Ahmed Bouridane (Senior Member, IEEE) received the “Ingenieur d’Etat” degree in electronics from the École Nationale Polytechnique of Algiers (ENPA), El Harrach, Algeria, in 1982, the M.Phil. degree in electrical engineering (VLSI design for signal processing) from the University of Newcastle upon Tyne, Newcastle upon Tyne, U.K., in 1988, and the Ph.D. degree in electrical engineering (computer vision) from the University of Nottingham, Nottingham, U.K., in 1992. From 1992 to 1994, he was a Research Developer in telesurveillance and access control applications. In 1994, he joined Queen’s University Belfast, Belfast, U.K., initially as a Lecturer in computer architecture and image processing and later on he was promoted to a Reader in computer science. He is currently a Full Professor with the Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates. He has authored or coauthored more than 350 publications and one research book on imaging for forensics and security. His research interests are imaging for forensics and security, biometrics, homeland security,image/video watermarking, medical engineering, cryptography, and mobile and visual computing.

Richard Jiang is currently a Senior Lecturer (Associate Professor) with the School of Computing and Communications, Lancaster University, U.K. His recent research has been supported by grants from EPSRC, the Leverhulme Trust, the Qatar Science Foundation, and other indus-try/international funders. He has supervised and co-supervised 12 Ph.D. students. He has authored over 80 publications. His research interests include artificial intelligence, AI ethics, privacy and securi-ty, quantum AI, neuronal computation, and biomedical image analy-sis. He was the Lead Editor of three Springer books. He served as a PC/Editorial Member and a Reviewer for various international con-ferences and journals.