frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 25 July 2025
DOI 10.3389/fbloc.2025.1596567

OPEN ACCESS

EDITED BY
Raul Zambrano,
Independent Researcher, New York, United States

REVIEWED BY
Larry C. Bates,
Independent Researcher, Detroit, United States
Nasurudeen Ahamed N,
United Arab Emirates University, United Arab Emirates

*CORRESPONDENCE
Richard Jiang,
r.jiang2@lancaster.ac.uk

RECEIVED 19 March 2025
ACCEPTED 04 June 2025
PUBLISHED 25 July 2025

CITATION
Xu B, Bouridane A, Ni Q and Jiang R (2025) A man–vehicle e-passport system using biometric blockchain for automated border control.
Front. Blockchain 8:1596567.
doi: 10.3389/fbloc.2025.1596567

A man–vehicle e-passport system using biometric blockchain for automated border control

Bing Xu[1], Ahmed Bouridane[2], Qiang Ni[1] and Richard Jiang[1]*

[1]LIRA Centre, Lancaster University, Lancaster, United Kingdom, [2]Center for Cybersecurity and Data Analytics, University of Sharjah, Sharjah, United Arab Emirates

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 study 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 ABC 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.

KEYWORDS

Brexit, ePassport, blockchain, biometrics, metaverse, digital twin, automated border control

1 Introduction

Due to the COVID-19 pandemic in 2021 and the recent war between Russia and Ukraine, border control has increasingly become an issue. This is not only because there is a sharp increase in border crossing demand but also because of a shortage in border control officers due to sick leave. Moreover, according to PwC (2014), border crossing demand in 2025 will reach 887 million for land, air, and sea travelers in the EU compared with 722 million in 2020, with an increase rate of approximately 5% per year. Similarly, the estimated number of individual (non-commercial) files to be stored in border control agent systems will be 128 million in 2025 compared with 104 million in 2020, with an annual growth rate of approximately 4.6%. Existing border agent capability is thus capped, so border control efficiency needs to be improved. Figure 1 shows a 15-km lorry queue waiting at the Dover border checkpoints, with lorry drivers stalled for up to 8 hours to cross the border (Brown, 2024).

The causes of existing low border control efficiency are twofold: manual documentation verification and the existing static e-passport system. Establishing border crossing

FIGURE 1
Dover 15-km lorry queue to cross the border (Brown, 2024).

legitimacy involves a substantial amount of documentation verification, such as identity credential e-passports, individual immigrant border visas to prove legitimacy, and customs clearance documentation to establish the legitimacy of commercial products crossing borders. Apart from existing e-passports, all other documentary verification must be manually conducted by border control officers, which is very time-consuming. Most importantly, current e-passports contain static information that is locked in the e-passport book microchip, which is not only inconvenient due to distance but also makes linking dynamic border crossing legitimacy information to identities extremely difficult.

Theoretically speaking, to improve existing border control efficiency and counter the criticism of being a centralized system, smarter and further automatization and decentralization are indispensable (Xu et al., 2022; Xu et al., 2019; Xu et al., 2020). With existing computing technology, it is quite feasible to automate existing border control procedures, but two requirements must be fulfilled.

First, automatization of documentation verification and border crossing recording requires digitization of border crossing documentation. In the case of border control, digitized border crossing documentation requires fidelity, which must be a genuine reflection of the real world; therefore, digital twin technology is deployed (Aleksi et al., 2022). For a formal definition, digital twin technology is a digital representation of a real-world object that serves as its indistinguishable digital counterpart for purposes such as simulation, testing, and monitoring (Lee et al., 2021). Digital twins are thus able to construct a veracity map from a real-world object to the digital world with high fidelity and consciousness, requiring existing attributes of the real-world object to be best mapped to the digital world (Wang et al., 2022). Moreover, by enabling this duplication mapping, digital twins also enable artificial intelligence and computing-assisted management, predictions, and simulations applicable to real-world objects (Far and Rad, 2022).

Second, apart from documentation digitization, the owner of the digitized document has to be accurately identifiable so that a border

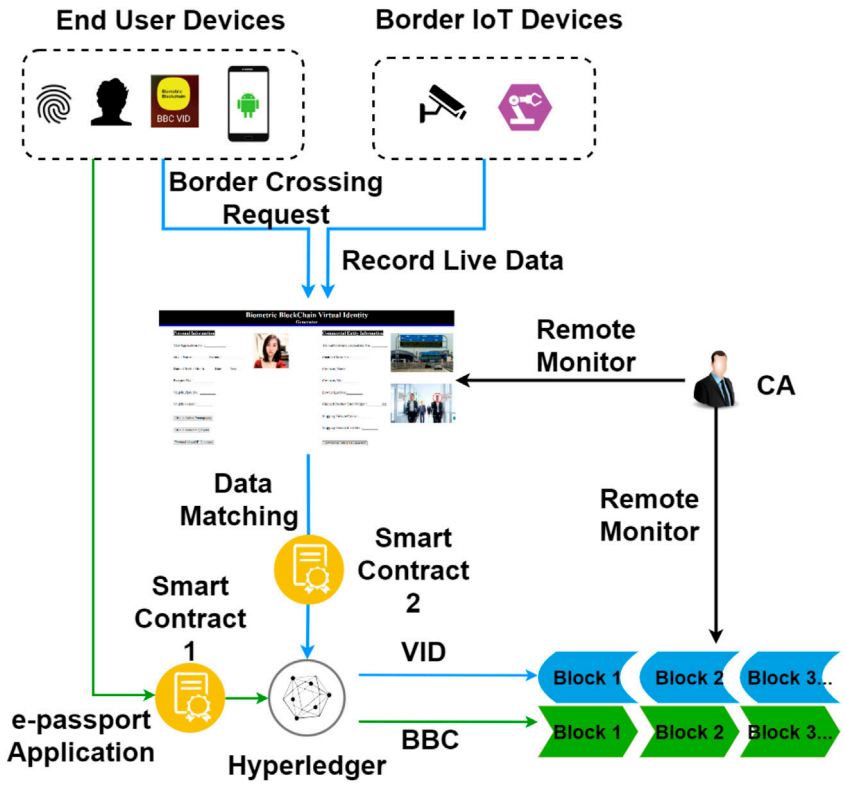

FIGURE 2
Full workflow of the proposed BBC ABC system.

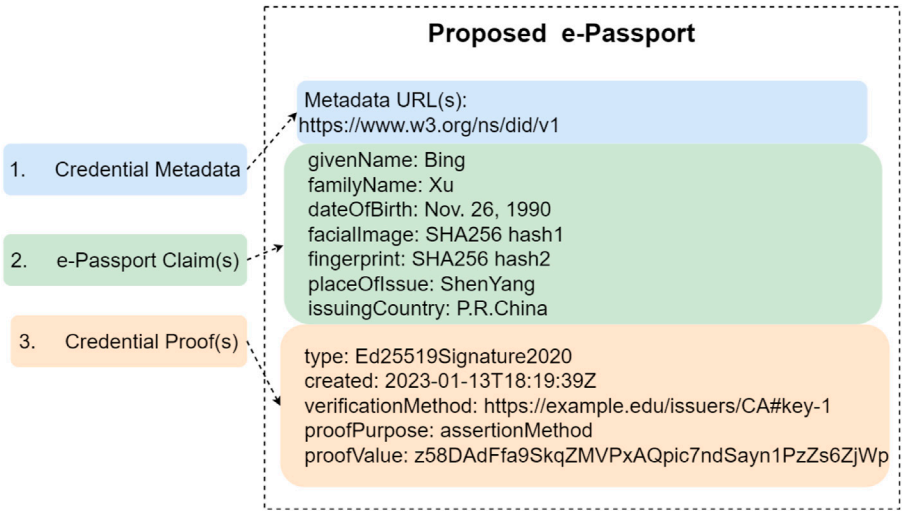

FIGURE 3
Demonstration of the proposed biometric e-passport identity digital credential, including the three components of credential metadata, claims, and proofs.

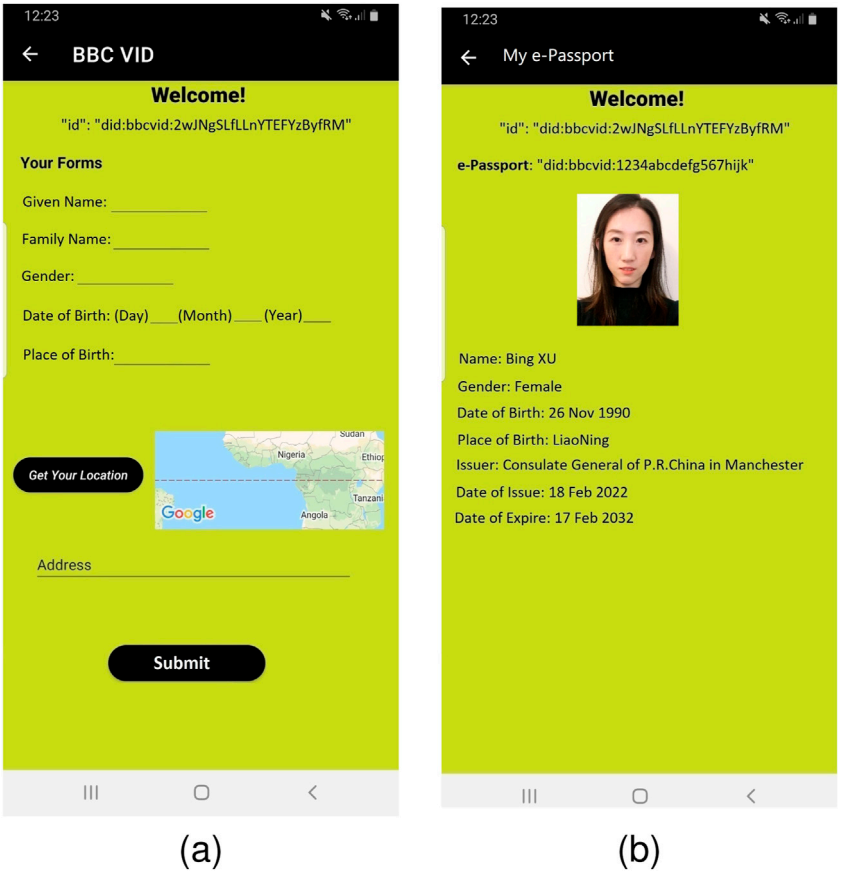

FIGURE 4
Demonstration of Android mobile DApp. **(a)** Biometric e-passport application form. **(b)** Biometric e-passport representation.

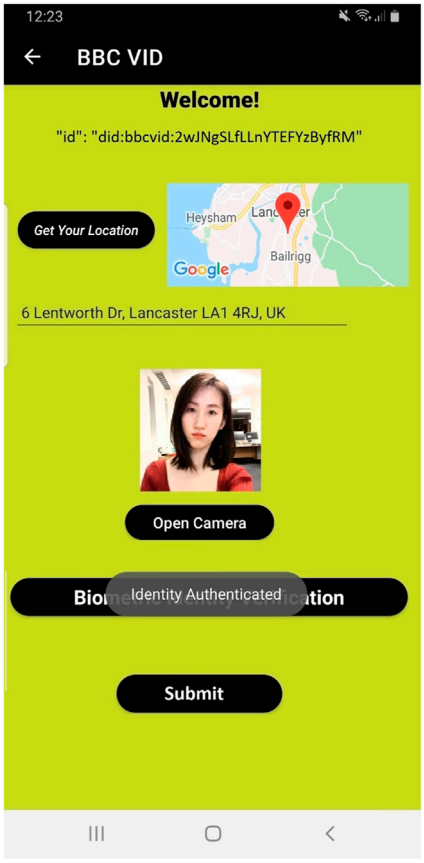

FIGURE 5
Facial biometric identity authentication at mobile DApp.

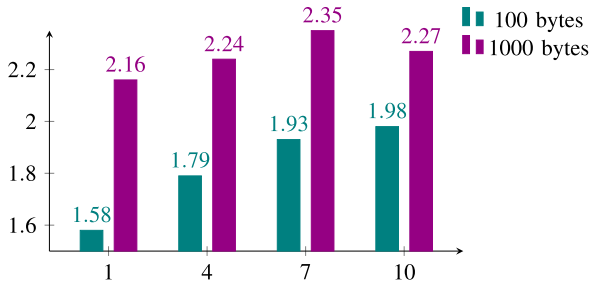

FIGURE 6
BBCVID: average latency for one, four, seven, and ten orderer nodes.

FIGURE 7
VS: average latency for one, four, seven, and ten orderer nodes.

TABLE 1 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 2 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

crossing permit may be granted to the lawfully correct person after documentation verification. Thus, constructing an individual's bodily digital twin is the second premise. However, a person's digital twin can be difficult to construct because verifying a physical person over the 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" (Dmitrienko et al., 1993), alluding to the same problem: digital identity authentication is always a risk-based assurance process (Grassi et al., 2020; NIST FIPS, 2004). Therefore, we propose a biometric blockchain-based e-passport system to construct an individual person's digital twin. Taking advantage of the blockchain transaction's immutable

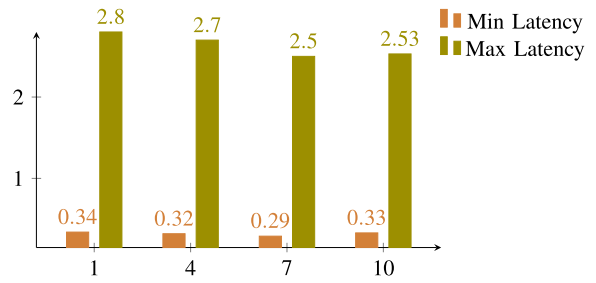

FIGURE 8
BBCVID: minimum and maximum latency for one, four, seven, and ten orderer nodes of 100-byte blind-write.

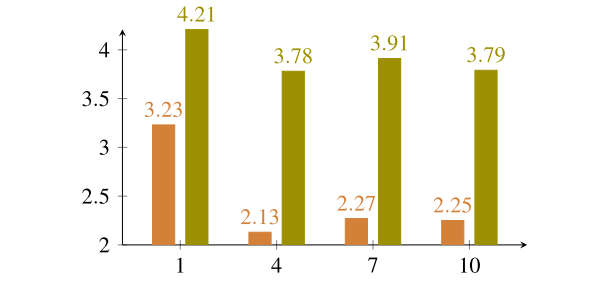

FIGURE 9
VS: minimum and maximum latency for one, four, seven, and ten orderer nodes of 100-byte blind-write.

property, online biometric identity authentication through a blockchain-generated biometric e-passport not only establishes the presence of a real human over the internet but also improves the assurance of digital identity authentication.

Blockchain has been an established computing technique since its introduction in 2008. It applies cryptography to a distributed network and builds a timestamped and immutable chain of hashed blocks. Blockchain has very favorable innate features that are derived from the system architecture, such as disintermediation, self-execution, and immutable and irreversible transactions (Nakamoto, 2008). Most importantly, it shifts the root of trust from a system administrator to the computational power attached to a system, creating a new form of economy. Decentralized autonomous organization (DAO) takes advantage of the blockchain technology, being easy to join, entirely digitally native, and global in reach (Wright, 2021). Instead of a conventional manager and managing board who are the central authority of an organization, DAO introduces blockchain self-execution smart contracts to automatically control an organization's behavior and organizational decision-making through blockchain's consensus mechanism.

This study proposes automating border control systems 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 properties of smart contracts ensure that the system operates without human intervention, making our 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 the efficiency and security. The use of digital twins allows for real-time traveler verification, while smart contracts within this decentralized autonomous organization ensure autonomous, transparent border management. This system promises to alleviate bottlenecks, thus providing a scalable, tamper-proof solution that redefines the future of border control.

TABLE 3 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 4 Comparison of existing and proposed border control systems regarding 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%

2 Preliminaries

This section covers the preliminaries of this proposal, including both blockchain and digital twin technologies in the metaverse DAO. Specifically, atomic and self-executed smart contract and blockchain innate properties will be explained. Moreover, to best construct a metaverse DAO, its construction framework and relationship with digital twins are both introduced.

2.1 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 at approximately $25,000, representing a dramatic increase over the last 15 years (Yahoo, 2023). 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 a consensus without relying on a central authority (Anthony et al., 2021). 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 create immutable records of transactions in a time-stamped ledger (Li et al., 2021). This structure enhances the 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—digital signatures, consensus mechanisms, and network protocols—are primarily designed to ensure that transactions are securely validated and consistently recorded across all nodes (Omar et al., 2021). Each transaction consists of various subcomponents, such as scripts and cryptographic signatures, enabling a wide range of operations on the blockchain. 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 (Nakamoto, 2008; Bodkhe et al., 2020). This makes consensus mechanisms critical as they determine the legitimacy and permanence of recorded data.

2.1.1 Digital signature

The function of a digital signature in a blockchain system is twofold. It guarantees the integrity of the transaction, and it verifies the identity of the message sender. Unlike conventional cryptographic encryption, in which discrete logarithm and integer factorization are normally imposed, the Bitcoin Blockchain elliptic curve digital signature algorithm (ECDSA)'s distinctive sub-exponential-time algorithm uses a different approach. It is claimed that "...the strength-per-bit is substantially greater in an algorithm that uses elliptic curves" (Johnson et al., 2014). Most importantly, the digital signature verifier is able to verify a signature by the signer's public key, even though the signature itself is created using the private key.

2.1.2 Consensus rule

In a decentralized system, all nodes in a blockchain behave completely independently. They are fully connected with each other so as to realize the system's common goal (Kleinrock, 1985). When all nodes agree with the current status of the system, they reach a consensus; the rule of how to reach the agreed current state of the system is called the "consensus rule" (Bodkhe et al., 2020).

Currently, there are two consensus rules that dominate the blockchain architecture: proof of work (PoW) and proof of stake (PoS). PoW updates the current global status of a blockchain system by doing some computational work, which specifically refers to a node increment nonce value for every try made until a valid block hash value is found. The quickest node will be the creator of that block and will be rewarded for maintaining the system consensus. In PoS, the stake can be the account balance and/or the age of the cryptocurrency. After the block is validated, the node with the most stakes will be voted the block creator and be rewarded from the system.

2.1.3 Smart contracts

Smart contracts are foundational components in many blockchain systems. Major platforms offer varying descriptions—Bitcoin describes them as "transactions which use the decentralized Bitcoin system to enforce financial agreements" (Bitcoin developer Guide, 2024); Ethereum defines them as "a program that runs on the Ethereum blockchain" (Wackerow, 2024); Hyperledger refers to them as "business logic running on a blockchain" (Bharathan, 2024)—but 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 (Konstantinos and Devetsikiotis, 2016). 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.

The aim of using a smart contract is to enable non-intermediary, trusted, and peer-to-peer transactions (Wang et al., 2020). Compared with conventional online banking and digital services, the benefits of deploying blockchain smart contracts are three fold:

- 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 the smart contract system depends on the computational power attached to the system rather than any central authority controlling the system (Lu et al., 2020).
- Non-intermediary: all smart contract-initiated transactions are non-intermediary and peer-to-peer, saving a lot of transaction fees compared to a conventional business contract mode (Wang et al., 2019).

- Automatic execution: smart contracts will automatically execute as soon as a new parameter is given; due to its atomic nature, the transaction has either not yet started or is otherwise completed after initiation (Matheus et al., 2021).

2.2 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 (Kashif, 2022). It builds 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 (Kashif, 2022), 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 (Stylianos, 2022). These 3D environments are positioned as improvements over traditional 2D interfaces, especially in fields like online education. For instance, Stylianos (2022) 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 (Far and Rad, 2022), represents a virtual replica of physical assets or processes. While blockchain technology is proposed as a means of establishing immutable links between real-world objects and their digital counterparts (Thien et al., 2023), practical implementation remains challenging. The creation of 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 are crucial to bridging the gap between physical reality and its metaverse representation and remain active areas of research and development. Formally, a digital twin is a digital representation of an actual real-world object that serves as its indistinguishable digital counterpart for the purpose of simulation, testing, and monitoring (Lee et al., 2021). The digital twin constructs the mapping from a real-world object to the metaverse with high fidelity and consciousness, and this requires existing attributes of the real-world object to be mapped to the metaverse as much as possible (Wang et al., 2022). Furthermore, by enabling this mapping, digital twins also enable first-hand data collection from digital twin devices so that artificial intelligence and computing-assisted management, predictions, and simulations can be enabled (Far and Rad, 2022).

Metaverse applications in logistics (Xu et al., 2019) and individual identity are of interest to our research. Digital twin-based logistics and transportation systems have a significant impact on the visibility of a vehicle, and this enables machine learning and other computing methods applicable to the overall logistics system (Moshood et al., 2021; Alharthi et al., 2023). It requires surveillance systems such as sensors, actuators, and CCTV cameras to collect live data from the real world and then constantly send these to the digital metaverse to reflect the current status of the object (Moshood et al., 2021).

3 Privacy-aware biometric blockchain-based e-passport system for automatic border control

This section proposes an e-passport system based on privacy-aware biometric blockchain (BBC) for automatic border control (ABC). The proposed system consists of two separate blockchains: one is for e-passport privacy-preserving biometric blockchain-based identity digital twins, and the other is automatic border control metaverse DAO (see Figure 2 for a demonstration of the proposed BBC ABC full workflow).

3.1 Main participants in the BBC ABC

To ensure that functions can be fulfilled in the proposed BBC ABC system, participants take different responsibilities in accordance with their different roles within the proposal. The main participants in the proposed system are as follows.

- Fabric Certificate Authority (Fabric CA). Since BBC ABC is built upon the Hyperledger Fabric permission blockchain, a certificate authority is required to issue identity certificates based on the public keys of users. These certificates enable user 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.
- The Driver and Vehicle Licensing Agency (DVLA) endorses border crossing permit applicant transactions and verifies vehicle-related documentation for border crossing legitimacy.
- Her Majesty's Revenue and Customs (HMRC) endorses transactions related to customs clearance, verifying

commercial product documentation and identifying missing clearance documents in border crossing applications.
- 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 submit border crossing permit applications and identity credentials via an Android-based decentralized application developed specifically for BBC ABC.

3.2 BBCVID for biometric e-passport

As discussed above, the causes of the low efficiency of existing border control procedures can be summarized as manual documentation and static identity credentials. Therefore, BBCVID blockchain can aim to digitize border crossing documentation and create dynamic identity credentials by deploying digital twin and blockchain technologies.

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 prevent 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 digital identity assurance and validating the presence of a real person during online interactions. Applicants first install the proposed Android mobile DApp to obtain access to the BBC ABC system and then submit an e-passport application. The BBCVID system CA verifies the application and invites applicants to visit biometric identity collection points particularly specified by the BBCVID system CA. After an applicant visits the biometric identity collection point, the BBCVID system CA is able to generate a decentralized identifier (DID) and its corresponding biometric DID documentation for the applicant—see Figure 3 for an illustration of BBCVID-generated biometric e-passport main components. This complies with W3C decentralized identifiers (DIDs) v1.0 and credential data model specifications (Sporny et al., 2022) which aim to improve cross-platform interoperability. Similarly, see Figure 4a for a demonstration of a biometric e-passport application form in Android mobile DApp and Figure 4b for a biometric e-passport representation in Android mobile DApp.

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

After obtaining the biometric DID and DID documentation, the applicant's digital twin is constructed. The DID thus decentralizes the digital representation of the real-world bodily applicant, which constructs their tie through the BBCVID blockchain immutable transaction. The DID differs from traditional digital identity authentication because it can be authenticated by an applicant's public key, facial image, and fingerprint biometric identity credentials; see Algorithm 1 for the biometric identity authentication protocol through BBCVID DID documentation. Moreover, after an applicant's bodily person digital twin is constructed, it is straightforward to generate a real-world identity credential digital twin; see Algorithm 2 for creating the border crossing document digital twin protocol.

In the digital signature verification algorithm in the BBCVID-generated digital twin document, the Edwards-curve Digital Signature Algorithm (EdDSA) (Steele et al., 2022) is adopted, as recommended by W3C, where a 32 octet private key is randomly generated, as well as the corresponding 32-byte public key A ($A \leftarrow encoding[s]B$), where 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, "signatureValue" is split into two 32-octet halves, with the first half as a pointer R and the second half as an integer S. The public key A is decoded as A', and $SHA512(dom2(0, context)\|R\|A\|M)$ is computed and interpreted as a little-endian integer k and M as a message. Finally, we check if $[s]B \equiv R + [k]A'$. If so, the signature is verified; if not, signature verification fails (Steele et al., 2022).

3.3 VS for automatic border control Metaverse DAO

In the current literature, there are a few other ongoing projects (Ahmed and Rios, 2022; Kang, 2023; Santamaria, 2023) that address the existing challenge of low border control efficiency by blockchain technology. They are government-oriented projects and are still in development, so their full technical reports are not yet available. However, one common factor is that they all build upon permissioned blockchain.

Since both the border crossing entity and documentation are digitized by BBCVID digital twin blockchain, the generated digital twin is 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.

There are three benefits to constructing metaverse DAO. The first is deeply automatizing border control procedures through blockchain atomic and self-executed smart contracts. The second is the reliability of completely eliminating human factors that distort digital border crossing legitimacy verification by shifting the trust from a system administrator to computational power through the implementation of the blockchain metaverse DAO system. The third is immutable records; the VS border control metaverse DAO can immutably record all border crossing events on the VS blockchain, which can clear disputes between the DAO and the border crossing entity.

Most importantly, the existing border e-gate is only available to the small group of people who do not require visa verification or customs clearance. This is because the e-gate can only retrieve static information locked in the microchip of an existing e-passport book,

which makes the e-gate completely ignorant of whether the person has a border crossing permit.

After BBCVID digital twin blockchain digitizes all border crossing documentation, the e-gate can be aware of dynamic information through digital twin duplicate effects. That is to say, if a real-world person has obtained a border crossing permit from the border agency, their digital twin identity projected into the digital world should also be able to reflect this dynamic change.

Therefore, after imposing our proposal, two major changes will occur to the e-gate system. First, the e-gate will be available for all travelers regardless of whether a visa and customs clearance documentation are required. Second, rather than reading static microchip information from an existing e-passport book, the proposed VS border control metaverse DAO generates a dynamic quick response (QR) code (Muthukumar et al., 2019) as a border crossing permit for immigrants to pass through the e-gates.

Before offering a comprehensive description of how a border crossing permit is generated by VS metaverse DAO, it is important to understand the processes for both an individual immigrant and a commercial business vehicle loaded with commercial products to cross the border.

The automatic border crossing process for individual immigrant control must first comply with the immigration law of the country; therefore, both the legitimacy of entering the specific country and the identity of the immigrant have to be confirmed and verified before a border crossing event happens. These processes can be broken down as follows.

1) Allow individual immigrants to obtain border crossing legitimacy (e.g., visa and customs clearance documents) and identity (e.g., passport) credentials.
2) Immigrants bring these credentials to the airport or land border checkpoints.
3) Upon presentation of the person, border crossing legitimacy documentation, and identity credentials at the border crossing checkpoint, the border officer conducts the following:
   (a) border crossing legitimacy documentation verification.
   (b) identity authentication.
   (c) granting border crossing permit.
   (d) stamping and recording the border crossing event in the passport book.

Therefore, to automate the above individual immigrant border crossing process, VS metaverse DAO can complete the above procedures through smart contracts.

The main task of the automatic border crossing process for customs inspection is to ensure *data consistency* between customs clearance documentations and the real time *in situ* border crossing event, in which inspected objects include vehicle identity, driver identity, and products declared to enter the country (Khoshons et al., 2006). The main target subjects to be inspected include the following:

- the identity of the driver and the driver's legitimacy for entering.
- the identity of the vehicle and the vehicle's legitimacy for border crossing.
- product-related documentation such as packaging lists, invoices, product models, and categories, the origin of the products, import permits, licenses and certificates, and customs clearance documentations.

A border checkpoint surveillance system is essential to enable automatic reconciliation of information beyond the BBCVID digital twin on the blockchain,. This system is responsible for collecting live, *in situ* data from border checkpoints. It gathers data through internet of things (IoT) devices deployed at these checkpoints to make the overall system a combined IoT and blockchain solution.

- CCTV camera for vehicle number plate and vehicle color.
- Weight sensor for the vehicle's weight. The output is the weight of the vehicle in kilograms.
- X-ray scanner for loaded product inspections. The output is Boolean to suggest whether further inspection is required—Yes or No.

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

```
Require:
DID, DID Documentation, collected biometric sample(CBC)
Smart Contract Initiation
if(1) proofValue ≡ SignAlgo(verificationMethod)
then(2) hash1 ← SHA256(bio_template)
  if(3) hash1 ≡ SHA256(bio_template)
  then(4) dist_i ← match CBCwith bio_template.
    for i ≤ 2
    if(5) dist_i ≤controlled threshodl σ
    then(6) 'success' ← identity is authenticated.
    else
    (6) 'fail' ← identity is not authenticated.
    (7) ask CBC re – submission
    (8) repeat (1) – (5)
    end if
    end for
  else
  (4) 'fail' ← 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
```

Algorithm 1. Biometric identity authentication.

To comprehensively describe how an individual immigrant would use the proposed biometric e-passport to cross the border through VS metaverse DAO smart contracts transactions, they would first be required to submit a border crossing permit application to VS blockchain over the mobile application. The application is a Hyperledger transaction proposal, in which the application data are digitally signed by the immigrant's private key.

The VS system CA (the same entity with a BBCVID system CA) gateway service receives the transaction proposal from a mobile client and then transfers it to one of the VS peer nodes to execute the transaction.

The smart contract will first initiate facial identity authentication via e-passport using the mobile application in Algorithm 1 (Figure 5) for facial image identity authentication at the mobile DApp. It then verifies whether the individual has a visa document. If all verification goes well, the VS peer node will endorse the transaction and then return it to the individual. The person signs the endorsed transaction and will then send it to the VS system CA for transaction validation. The VS system CA also orders the VS blockchain, which validates the transaction, generates a border crossing permit, orders the transaction into a VS blockchain block, and broadcasts it to the other peer nodes for validation and commitment. Thus, the immigrant's border crossing permit application initiates a corresponding smart contract which is able to accomplish the above process. The validated transaction is the specific border crossing permit documentation, which is represented by a QR code.

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 the 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 would use a QR code to initiate crossing by undergoing fingerprint identity authentication. After successful authentication, the e-gate would return a digitally signed endorsement transaction to the individual 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 would then validate the endorsements and signatures, order the transaction into a new VS blockchain block, and broadcast it to peer nodes for validation and commitment. The immigrant would then receive 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 would remain rigorous to ensure security, meaning that significant time savings occur primarily for pre-registered travelers. To offer a comprehensive description of how customs inspection is conducted at border checkpoint through VS metaverse DAO smart contracts, the border crossing permit should be obtained before a vehicle drives through the border-booth-like e-gate. For a private vehicle to drive through the border checkpoint, in addition to the person's border crossing permits, the vehicle's border crossing permit should also be obtained from the DVLA beforehand. For a commercial vehicle to drive through the border checkpoint, apart from individual and vehicle border crossing permits, the loaded products on the commercial vehicle should also obtain a border crossing permit from HMRC for customs clearance.

When first submitting the border crossing permit application, the commercial business entity which owns the commercial vehicle would be required to obtain the digital twin for both the vehicle and the business entity, in accordance with Algorithm 2. The owner of the commercial vehicle and business entity would be the "controller" of the corresponding digital twin and be assumed to have full control over the subject to which the DID refers (e.g., vehicle and commercial business entity).

```
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.
```

Algorithm 2 Border crossing document digital twin

Then both the commercial and the private vehicle border crossing permit application can be made through the proposed mobile DApp. The commercial border crossing permit application starts with a form recording the loaded products invoice, packaging lists, vehicle number plate, driver's visa (if required), and driver's e-passport number. The mobile client collects these 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 remaining organizations, which is 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, a widely adopted programming language for Ethereum-compatible blockchain platforms. Solidity enables the definition of endorsement policies, validation logic, and transaction state updates securely and transparently. This choice supports compatibility with the underlying permissioned blockchain network used in the VS system and facilitates flexible, modular smart-contract deployment and upgrades. By running the corresponding smart contract, the following four maneuvers occur in parallel.

- Individual person biometric identity authentication and border crossing legitimacy verification. The driver's facial identity will be authenticated in accordance with their biometric e-passport, and their facial image will be collected through the driver's own mobile DApp. If a visa is also required for the driver to pass through the border, VS metaverse DAO is also able to verify the visa . If all goes well, the VS system CA peer node will digitally endorse it and return it to the business entity's mobile client.

- Products' border crossing legitimacy verification. Upon receiving the products' invoice number and packaging lists, HMRC can automatically identify the customs clearance documentations 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 and then sends it back.
- Vehicle border crossing legitimacy verification. The DVLA verifies vehicle border crossing legitimacy using the vehicle's digital twin documentation and searching whether the vehicle has been reported lost or has any illegal records. If all goes well, the DVLA will endorse this transaction and send it back to the commercial business entity mobile client.
- Border checkpoint surveillance system live data collection. There is a border road surveillance unit approximately 2–3 km away from the border e-gate. This collects the vehicle's number plate, color, weight, 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's mobile client collects all digitally signed endorsements and packs them into a data envelope to let the applicant (commercial business owner) digitally sign it. The data envelope is then sent to the VS system CA for validation. The latter 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's specified vehicle driver.

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

4 System implementation and evaluation

To properly evaluate our proposal, the system was 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." The VS network also includes three organizations, namely the DVLA, HMRC, and the border surveillance system, all sharing the same ordering service (BBCVID system CA)[1]. Both networks use the Raft consensus protocol (Huang et al., 2019) 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 utilized 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 users are connected through a developed Android mobile DApp (JAVA) user interface and communicate with the BBC ABC Hyperledger Fabric test network through the Fabric Gateway Service. Most importantly for this project system implementation, the local Hyperledger test network is built upon the Ubuntu 20.04.3 LTS sub-system in Windows 10 Version 22H2(OS Build 19045.2846) through Windows-Subsystem-for-Linux 2(WSL 2).

4.1 Transactions

For private Hyperledger Fabric blockchain, the standardized transaction occurs in three phases (Anthony et al., 2021):

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 is proposed in accordance with the border control workflow. In *BBCVID*, a transaction is made to obtain either the proposed e-passport or other digitally verifiable credentials, such as visa and customs documentation. A valid BBCVID transaction is defined below.

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. For instance, if the applicant is to obtain digital verifiable customs documentation, the gateway service is offered by HMRC's node. The gateway service will forward the 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 to the applicant's client.

Phase 2: The mobile client packs all responses obtained from Phase 1 into an envelope and the applicant signs it. The application client submits 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 signatures in the envelope and then order the transaction. The transaction will be ordered into a new block of the BBCVID.

Phase 3: CA will broadcast the ordered transaction to the other peer nodes to validate the transaction and then commit it to BBCVID. The applicant will obtain a full access permit to this new ledger. By a similar token in VS, a transaction is made to obtain

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's smart contract, and it clarifies which specific organization(s) must sign the transaction in order to make it valid (Bharathan, 2024).

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

4.2 Android mobile DApp

The Android mobile operation system runs on a Linux kernel that connects its hardware with its software stack. To preserve data privacy and security, Android has a built-in trusted execution environment, which indicates that the biometric information is encrypted and stored in a separated part of the Android smart phone (Ekberg et al., 2013). Most importantly, it is completely inaccessible to the regular operating system. To make the system even more secure and private, "permissions" are used in Android whenever an access to sensitive and protected information is raised, such as GPS location and open camera. If the user does not grant permission, access will be denied (Rajinder, 2014).

Android mobile application access is granted only to the registered; a user name, email address, and six-digit PIN are required to complete new user registration.

After obtaining access to the mobile application, access to BBCVID and VS Blockchain should also be obtained. The Hyperledger Fabric certificate authority (Fabric CA) has three main functions in our proposed system.

- 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, revocation, and management.

4.3 BBC ABC hyperledger blockchain performance

Adulla Reddy (2024) also claims that the following metrics can be used to evaluate blockchain network performance. The first is transaction latency. Network-wide, 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 importantly, Adulla Reddy (2024) also recommends using all nodes in the system under test (SUT) to get a better evaluation of transaction latency.

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

The second metric is transaction throughput. This is the rate at which validated transactions are committed to the Hyperledger Fabric blockchain over a defined time scope. In most cases, it is represented by transactions per second.

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

In addition, Hyperledger Caliper (Caliper, 2023), an established blockchain use case-based performance evaluation tool, is used to evaluate the BBCVID and VS Hyperledger Fabric blockchain performance. The Hyperledger Caliper parameters are

- Hyperledger Caliper version 0.5.0;
- Hyperledger Fabric 2.4 bound to the Hyperledger Caliper;
- Four bare metal machines to host Caliper workers;
- Endorsement policy is one of any in BBCVID but three out of four in VS;
- 200 Caliper workers are used in both BBCVID and VS;
- TLS is enabled in both BBCVID and VS.

Most importantly, some block cutting parameters are also introduced to both BBCVID and VS:

- block cut time[3]: 2 s.
- block size[4]: 500.
- preferred maximum bytes: 2 Mb.

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

With the above testing environment, only transaction latency as in Equation 1 assessed and discussed since Hyperledger Fabric private blockchain does not suffer scalability issues, and transaction throughput as in Equation 2 can be manually adjusted as a system parameter. Since both BBCVID and VS Hyperledger blockchain transactions are mostly to write the blind key value in its transaction, an assessed blind-write per 1000 and 100 byte performance is listed, as in Table 1 for BBCVID Blockchain and in Table 2 for VS blockchain with a fixed TPS at 3000.

Therefore, since both BBCVID and VS Hyperledger Blockchain run on a test network with the Raft consensus rule, the transaction is finalized as soon as the orderer validates the transaction; thus, the orderer has immediate finality. Therefore, the latency performance is evaluated for each peer node in terms of how long it takes to commit a validated transaction, which leads to a "minimum latency," "maximum latency," and "average latency." Even though the Hyperledger Fabric test network has a predefined 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 approximately 3000 in both cases. However, the general performance of "blind write 100 byte" outperforms the "blind write 1000 byte."

The performance in BBCVID and VS is closely related with the peer node size, in which each node has the potential to make an impact on the entire system performance based on the

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

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

endorsement policy. Therefore, the average transaction latency performance is assessed based on one, four, seven, and ten nodes. See Figure 6 for the average latency performance in terms of the number of BBCVID orderer node changes, Figure 7 for VS blockchain, Figure 8 for the minimum and maximum transaction latency performances in terms of one, four, seven, and ten orderer nodes in BBCVID, and Figure 9 for VS blockchain.

Packet loss is another relevant assessment criterion to be evaluated in a 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, packet loss is 0.06% blind-write per 1000 bytes compared with 0.04% per 100 bytes. Thus, blind-write per 100 bytes has a lower packet loss rate in both BBCVID and VS blockchain, and VS packet loss performance is better than that of BBCVID overall. This is because VS has four peer nodes collecting packets from the message sender but BBCVID has only one node; see Table 3 for a demonstration of the packet loss rate comparison between BBCVID and VS.

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

To explain this contribution further, 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 activity.

4.4 BBC ABC border control efficiency performance

In accordance with PwC (2014), soft border systems can be analyzed through cost and by leveraging existing system criteria. In this proposal, the computational cost and duration of border crossings are evaluated.

First, the transaction cost. As blockchain is a distributed network constructed from open-source codes, system security is always crucial. Section 5 explains that public blockchains like Bitcoin and Ethereum charge transaction fees to protect system security and constrain the waste of public resources. However, Hyperledger Fabric blockchain as a private blockchain uses user identity authentication to secure system security, making zero transaction fees possible. Thus, there are no transaction fees for all operations on Hyperledger Fabric, regardless of the energy cost (Adulla Reddy, 2024), compared to Bitcoin blockchain at an average of USD 5.10 and Ethereum blockchain at USD 4.19 per transaction fee in March 2023 (Average Transaction Fee Chart, 2023).

Second, running a full node cost is evaluated. Both BBCVID and VS are Hyperledger Fabric private blockchains. Therefore, to run a full node, there are some minimum requirements in terms of hardware and network performance (Hyperledger Fabric, 2023). Since each full node may potentially impact the entire blockchain network's performance in accordance with the consensus rule and endorsement policy, for 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 encouraged (Hyperledger Fabric, 2023).

Third, the computational costs in the proposed BBC ABC system.

(1) Digital verifiable documentation verification, including proposed e-passport, visa, and customs clearance documentation. In this proposal, the Edwards-curve Digital Signature Algorithm (EdDSA) (Josefsson and Liusvaara, 2017) is used to generate the digital signature attached to all BBCVID generated digital verifiable documents as this algorithm is recommended by W3C DID core (Sporny et al., 2022) and EdDSA Cryptosuite (Steele et al., 2022), particularly for DID credentials. In our test environment, digital signature verification only takes an average of 0.27 s for accumulated 100-document (file size 1.9 KB to 2.1 KB) verification simulation instances.

(2) Biometric identity authentication through the proposed e-passport. In facial image identity authentication, VGG-face recognition (Park et al., 2015) is used for facial image authentication, where the image size is limited to 100 × 32 bits. It takes 9.52 s to complete the facial identity authentication over the proposed e-passport. As the facial image is captured live over a mobile application camera, most time is spent on the facial image collection, estimated at approximately 3–4 s minimum. The test results achieved 20 instances by our own mobile client.

Moreover, fingerprint identity authentication is only conducted at border checkpoint e-gates, in which minutiae-based two-dimensional feature vector matching is deployed. Since fingerprint data are *not* available on a large scale, we used our own fingerprint data collected from a U.are.u 5300 fingerprint scanner (USB 2.0, FIPS 201/PIV, FAP 30, optical, resolution: 500 dpi, 256 levels of gray) to simulate 20 instances. Initiating "biometric identity authentication" smart contract on BBCVID blockchain took an average of 4.75 s.

(3) Border crossing permit generation. Starting from when a border crossing applicant submits a border crossing permit application, VS BA is not able to generate the border crossing permit until all required endorsements are received. Three organizations are required to endorse a border crossing permit transaction: HMRC, DVLA, and the surveillance system. As soon as an applicant submits the application, HMRC and DVLA can endorse the transaction immediately; however, the surveillance system must wait until the applicant drives the declared vehicle to the border checkpoint so that it can be endorsed. Therefore, the time spent waiting for the vehicle to drive through the border checkpoint road unit will not be counted into the computational cost.

For a commercial entity to obtain a border crossing permit with 20 documents to be verified, the estimated computation cost is

$$20 \times 0.27 + 9.52 + 120 + 4.02 \times 4 = 2.52\ minutes \quad (4)$$

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

For an individual to obtain a border crossing permit with one visa document, the computational cost is

$$0.27 \times 2 + 9.52 + 4.02 = 0.23\ minutes \quad (5)$$

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

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

$$0.27 \times 3 + 9.52 + 120 + 4.02 \times 3 = 2.37\ minutes \quad (6)$$

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

VID blockchain border crossing event recording refers to use of a border crossing permit at the border e-gate to conduct fingerprint biometric identity authentication and then record it by committing this transaction on VS blockchain. Therefore, the computational cost is

$$0.27 + 4.75 + 1 = 6.02\ seconds \quad (7)$$

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

In accordance with PwC (2014), an e-gate existing border crossing requires 20–30 s to complete fingerprint identification and 15–20 s for photo facial image identity authentication. Additional manual registration would be required on many occasions, costing approximately 30–60 s per instance.

Therefore, a reasonable estimation of border crossing duration can be made in the existing border control system. For a commercial vehicle to cross the border with 20 documents to be verified, the border crossing duration is 20.25 min ($30 \times 20 + 15 + 10$ *minutes*), including the time for 20 document verification, facial identity authentication at e-gate, and estimated vehicle-loaded products inspection time (10 min). For individuals crossing the border, the border crossing duration is 1.25 min ($15 + 30 \times 2$), including facial image identity authentication at the border e-gate and passport and visa documents manual verification. For individuals crossing the border with a private vehicle, the border crossing duration is 5.25 min ($15 + 30 \times 4 + 3$ *minutes*), including facial image identity authentication at the border e-gate, visa, passport, driving license, vehicle registration four-document verification, and estimated vehicle inspection time at border checkpoints (3 min). Compared with our proposed system discussed in "Computational cost" above, the corresponding duration is 2.62 min, 0.33 min, and 2.47 min, including the time to obtain the border crossing permit and immutable records as in Equations 4–7; see Table 4 for a comparison of the existing and the proposed border control systems regarding border crossing duration.

5 Conclusion and future research

Resolving the issue of low border control efficiency is the main goal of this study. The causes of this are manual documentation verification and static identity credentials. Establishing border crossing legitimacy involves a great amount of documentation verification, such as identity passports, visas that prove the legitimacy of immigrants crossing the border, and clearance documents for customs for commercial products crossing the border. Apart from existing e-passports, all other documentary verification must be manually conducted by border control officers, which is very time-consuming. Most importantly, current e-passports contain static information that is locked in the e-passport book microchip, which is not only inconvenient given distance but also makes binding dynamic border crossing legitimacy to the passport extremely difficult.

To automate existing border control manual documentation verification, the documentation that establishes the legitimacy of border crossing must be digitized. Therefore, we constructed a real-world verifiable documentation digital twin data model.

To further automate the border control process, a border control metaverse DAO was constructed. By constructing a BBC ABC metaverse DAO system, border crossing efficiency is improved by 354.75% on average, with 112.55% minimum improved efficiency for individual immigrants with private vehicles crossing the border and 672.90% maximum improved efficiency for commercial vehicles loaded with commercial products crossing the border.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

BX: Formal Analysis, Methodology, Writing – original draft, Validation, Investigation, Data curation, Software, Visualization. AB: Writing – review and editing, Conceptualization, Supervision, Methodology, Project administration, Funding acquisition. QN: Resources, Project administration, Supervision, Conceptualization, Writing – review and editing. RJ: Conceptualization, Funding acquisition, Methodology, Writing – review and editing, Supervision, Project administration.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This work was supported

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

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

The author(s) declared that they were an editorial board member of Frontiers, at the time of submission. This had no impact on the peer review process and the final decision

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

References

Adulla Reddy, M. (2024). *Hyperledger blockchain performance metrics*. Hyperledger.org. Available online at: https://www.hyperledger.org/learn/publications/blockchain-performance-metrics.

Ahmed, W. A., and Rios, A. (2022). "Digitalization of the international shipping and maritime logistics industry: a case study of TradeLens," in *The digital supply chain*. Elsevier, 309–323.

Aleksi, K., Antti, H., Kettunen, P., Mikkonen, T., Makitalo, N., Nurmi, J., et al. (2022). Empowering citizens with digital twins: a blueprint. *IEEE Internet Comput.* 26 (5), 7–16. doi:10.1109/mic.2022.3159683

Alharthi, A., Ni, Q., Jiang, R., and Khan, M. A. (2023). A computational model for reputation and ensemble-based learning model for prediction of trustworthiness in vehicular *ad hoc* nework. *IEEE Internet Thing J.*

Anthony, L., et al. (2021). An overview of hyperledger foundation. *Hyperledger. Org.*

Average Transaction Fee Chart (2023). Etherscan.io. Available online at: https://etherscan.io/chart/avg-txfee-usd.

Bharathan, V. (2024). *Hyperledger architecture, volume II: smart contracts*. Hyperledger.org. Available online at: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_Smart.

Bitcoin developer Guide (2024). *Bitcoin developer Guide: contract*. Bitcoin.org. Available online at: https://developer.bitcoin.org/devguide/contracts.html

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., et al. (2020). Blockchain for industry 4.0: a comprehensive review. *SIEEE Access* 8, 79764–79800. doi:10.1109/access.2020.2988579

Brown, F. (2024). Huge 15km lorry queues at Dover blamed on Brexit. Available online at: https://metro.co.uk/2022/01/22/huge-15km-lorry-queues-at-dover-blamed-on-brexit-15964763/.

Caliper, H. (2023). *Getting Started*. Hyperledger.github.io. Available online at: https://hyperledger.github.io/caliper/v0.5.0/getting-started.

Dmitrienko, A., Liebchen, C., Rossow, C., and Sadeghi, A.-R. (1993). On the internet, nobody knows you're a dog. *New Yorker* 69.

Ekberg, J. E., Kostiainen, K., and Asokan, N. (2013). "Trusted execution environments on mobile devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security*, 1497–1498.

Far, S. B., and Rad, A. I. (2022). Applying digital twins in metaverse: user interface, security and privacy challenges. *J. Metaverse* 2 (1), 8–15.

Grassi, P., Garcia, M., and Fenton, J. (2020). *NIST digital identity guidelines*. National Institute of Standards and Technology NIST.

Huang, D. Y., Ma, X. L., and Zhang, S. (2019). Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Trans. Syst. Man, Cybern. Syst.* 50 (1), 172–181. doi:10.1109/tsmc.2019.2895471

Hyperledger fabric (2023). *Hyperledger fabric: performance considerations*. Hyperledger-fabric. Available online at: https://hyperledger-fabric.readthedocs.io/en/latest/performance.html

Johnson, D., Menezes, A., and Vanstone, S. (2014). The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* 1 (1), 36–63. doi:10.1007/s102070100002

Josefsson, S. (2024). Dwards-curve digital signature algorithm (EdDSA). *Internet Res. Task Force (IRTF)*. Available online at: https://www.rfc-editor.org/rfc/rfc8032.

Josefsson, S., and Liusvaara, I. (2017). Edwards-curve digital signature algorithm (EdDSA).

Kang, T. I. (2023). *Korea pilots blockchain technology as it prepares for the future*. World Customs Oragnization news.

Kashif, L. (2022). "Metaverse: why, how and what," in *How and what*.

Khoshons, M. K., Clark, C. c., and Tarek, S. (2006). Simulation and evaluation of international border crossing clearance systems: a Canadian case study. *Transp. Res. Rec.* 1966 (1), 1–9.

Kleinrock, L. (1985). Distributed systems. *Commun. ACM* 28 (11), 1200–1213. doi:10.1145/4547.4552

Konstantinos, Hr., and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of Things. *IEEE Access* 4, 2292–2303. doi:10.1109/access.2016.2566339

Lee, L. H., Braud, T., et al. (2021). "All one needs to know about metaverse: a complete survey on technological singularity," in *Virtual ecosystem, and research agenda*. arXiv preprint arXiv:2110.05352.

Li, Y. N., et al. (2021). "Non-equivocation in blockchain: double-authentication-preventing signatures gone contractual," in *Proceedings of the 2021 ACM asia conference on computer and communications security*, 859–871.

Lu, N., Wang, B., Zhang, Y., Shi, W., and Esposito, C. (2020). NeuCheck: a more practical Ethereum smart contract security analysis tool. *Softw. Pract. Exp.* 51 (10), 2065–2084. doi:10.1002/spe.2745

Matheus, F., et al. (2021). "Dynamic posted-price mechanisms for the blockchain transaction-fee market," in *Proceedings of the 3rd ACM conference on advances in financial technologies*, 86–99.

Moshood, T. D., Nawanir, G., Sorooshian, S., and Okfalisa, O. (2021). Digital twins driven supply chain visibility within logistics: a new paradigm for future logistics. *Appl. Syst. Innov.* 4 (2), 29. doi:10.3390/asi4020029

Muthukumar, B., Albert, M. J., Nambiar, G., and Nair, D. (2019). QR code and biometric based authentication systems for trains. *IOP Conf. Ser. Mater. Sci. Eng.*

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. *Decentralized Bus. Rev.*, 21260.

NIST FIPS (2004). Statement on the physician acting as an expert witness, *J. Am. Coll. Surg*, vol.199, 746, 747. doi:10.1016/j.jamcollsurg.2004.07.015

Omar, A., Jaradat, A., Kulakli, A., and Abuhalimeh, A. (2021). A comparative study: blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* 9, 12730–12749. doi:10.1109/access.2021.3050241

Parkhi, O. M., Vedaldi, A., and Zisserman, A. (2015). *Deep face recognition*. British Machine Vision Association.

PwC (2014). *Technical study on smart borders: final report*. European Commission. Available online at: https://home-affairs.ec.europa.eu/system/files/2020-09/smart_borders_technical_study_en.pdf.

Rajinder, S. (2014). An overview of android operating system and its security. *Int. J. Eng. Res. Appl.* 4 (2), 519–521.

Santamaria, S. C. (2023). *CADENA, a blockchain enabled solution for the implementation of Mutual Recognition Arrangements/Agreements*. World Customs Oragnization news.

Sporny, M. (2024). Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. Available online at: https://www.w3.org/TR/did-core/.

Sporny, M., Longley, D., and Chadwick, D. (2022). *Verifiable credentials data model v1*, 1. *W3C.org*.

Steele, O., Sporn, M., and Looker, T. (2022). *EdDSA Cryptosuite v2020*. W3C.org. Available online at: https://www.w3.org/community/reports/credentials/CG-FINAL-di-eddsa-2020-20220724/.

Stylianos, M. (2022). Metaverse. *Encyclopedia* 2 (1), 486–497. doi:10.3390/encyclopedia2010031

Thien, H., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., et al. (2023). Blockchain for the metaverse: a review. *Future Gener. Comput. Syst.* 143, 401–419. doi:10.1016/j.future.2023.02.008

Wackerow, P. (2024). *Introduction to smart contracts*. Ethereum.org. Available online at: https://ethereum.org/en/developers/docs/smart-contracts/.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Trans. Syst. Man, Cybern. Syst.* 49 (11), 2266–2277. doi:10.1109/tsmc.2019.2895123

Wang, Y. T., Su, Zh., Zhang, N., Xing, R., Liu, D., Luan, T. H., et al. (2022). A survey on metaverse: fundamentals, security, and privacy. *IEEE Commun. Surv. and Tutorials* 25, 319–352. doi:10.1109/comst.2022.3202047

Wang, Z. L., Jin, H., Dai, W., Choo, K. K. R., and Zou, D. (2020). Ethereum smart contract security research: survey and future research opportunities. *Front. Comput. Sci.* 15 (2), 152802. doi:10.1007/s11704-020-9284-9

Wright, A. (2021). The rise of decentralized autonomous organizations: opportunities and challenges. *Stanf. J. Blockchain Law and Policy* 4 (2), 152–176.

Xu, B., Agbele, T., and Jiang, R. (2019). Biometric blockchain A better solution for the security and trust of food logistics. *IOP Conf. Ser. Mater. Sci. Eng.* 646, 012009. doi:10.1088/1757-899x/646/1/012009

Xu, B., Agbele, T., Ni, Q., and Jiang, R. (2020). *Biometric blockchain A secure solution for intelligent vehicle data sharing*. Springer Cham.

Xu, B., Ni, Q., Jiang, R., and Bouridane, A. (2022). "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*, 13, 235–248. doi:10.1007/978-3-031-04424-3_13*Chapter*

Yahoo (2023). *Bitcoin historical data*. Yahoo Finance.