Using blockchain with biometric security to create a secure virtual world

Stefan Dejanovic*, Dion Croom*, Stevan Stankovski*
OVII TECH RESEARCH & DEVELOPMENT
Novi Sad, Serbia
stefan@ovii.tech, dcroom@ovii.tech, stevan@uns.ac.rs

Abstract—
In this paper, we will analyze how we can use blockchain, biometric security, and virtual worlds to create a secure environment for immersive interaction. The current model, is either not immersive, does not have digital avatars, or the system is not protected in a secure way to ensure full trust between participants We describe an immersive system that is fully secured using blockchain and biometric security to ensure users are the owners and controllers of their data and that they are fully verified on the system. Finally, we will analyze how the process is being performed and are some of the use cases of that kind of immersive environment that industries/participants can benefit from.

I. INTRODUCTION

The current hottest research topics, both in industry and academia, are blockchain, metaverse, and security. Defined as a shared distributed ledger, blockchain uses a set of nodes to maintain the data structure, organized in blocks. Reality telepresence, or digital persona (avatar), is becoming a very popular way of interaction in social and business applications.

A digital identity arises organically from the use of personal information on the web and from the shadow data created by the individual's actions online. A digital identity may be a pseudonymous profile linked to the device's IP address, for example, or a randomly generated unique ID. Digital identity is the network or Internet equivalent to the real identity of a person or entity (like a business or government agency) when used for identification in connections or transactions from PCs, cell phones or other personal devices.

We are in the Virtual era, new forms of interactions are emerging and disrupting the way we interact in social and business space. Organizations are using new forms of interaction in virtual space to improve user experience. Now, data is one of the most valuable assets in economy [5]. On the other end, while we are data-driven society, storing lots of data and creating virtual spaces as a way of interaction with digital avatars, one of the growing public concerns is user privacy. One of the growing public concerns is authentication and verification of the user. The government and business sector are seeking for the right solution to perform better way of authentication and verification to improve security. Motivation in this paper is about using multiple technologies - blockchain, virtual worlds, and biometric security combining them as a stack for solutions to improve security, authentication, and trustworthiness between the parties in interaction.

The remainder of this paper is organized as follows: Section II reviews related works regarding blockchain, biometric and virtual technology and securing e-identity. Section III describes methods used in this analysis. Section IV presents results obtained in this analysis. Section V summarizes our testing and gives a scope for future work.

II. RELATED WORKS

Urban centres and metropolitan areas are increasingly integrating cyber-physical technologies to optimise the use of resources and enable a higher quality of life. Innovative business models and metaverse virtual technologies will transform how services are delivered in cities and regions. The development of these new metaverse virtual solutions has the ability to address the challenges brought by an increasing urban population. However, key investments and the existence of critical physical infrastructures are required to develop and successfully implement many of those capabilities.

Vast number of industries have shown interest in virtual technologies and these privacy issues, both from a legislative point of view and from a technological point of view [6]. Leading examples of companies and organizations chose to implement their own proprietary authentication methods based on the OAuth protocol [4].

Many of the technologies that are creating the metaverse already exist, but many of them are still far away.

There are various solutions and techniques targeting privacy concerns that are focusing personal data. Data anonymization methods are aiming to protect personal and sensitive data. K-anonymity is a common property of anonymized datasets, and it requires that sensitive information of each record is indistinguishable from at least k-1 different records [3]. Furthermore, there is l-diversity that is used to ensure that sensitive data is represented by a diverse enough set of possible values [2]. Also, t-closeness is used for distribution of sensitive data [1].

Lastly, in recent years, virtual technology emerged which allows users to use new ways of activities – virtual

universe can support and interconnect a number of different applications, immersiveness – switching from static 2D profile images to 3D avatars, interoperability – virtual world can be identified as a unifying framework that connects multiple applications and services. Users will be able to interact simultaneously with multiple applications.

A. *Our Work*

We are using combination of blockchain technology, biometric security, and virtual world technology to create a secure e-identity with focus on maintaining and securing user privacy and security. We will describe our solution and discuss future improvements, how technologies can be used as a core resource in trusted computing.

III. METHODS

In this section methodology that is used to evaluate the solution is going to be described.

A. *Research Questions*

In order to analyze the main benefits of the above technologies to create secured and verified e- identity, certain concepts must be comprehended.

The first one is identity ownership. Our model focuses on ensuring that the identity of the user must be verified by a trusted authority, this is performed as KYC (Know Your Customer). The trusted authority will confirm the identity of the user in the system with the user photograph.

The second is biometric security. The system needs to perform biometric authentication before the user can join the virtual world.

The third one is user-sensitive information. The system recognizes users as the owners of the data and the service applications as guests with permissions. Forth is data transparency and audibility. Every user has complete transparency over data that is being collected about him and how that data is being processed.

B. *Methodology*

We will rely on the blockchain to be tamper-free and no misuse can be made because it requires a large network of untrusted peers to compromise blockchain security. Also, we assume that trusted authority is legitimate and does KYC accordingly to the rules. We will rely on the third-party avatar creation mechanisms for creating user avatars. We will concentrate on analyzing the process and implications of biometric authentication and joining the virtual world. We will analyze what is written on the blockchain and data storage and analyze if data is encrypted(hashed) and how user identity acts in the virtual world. Test scenarios will be created where processes and data will be analyzed:

1. User enters the virtual world – goes through a process
    a. KYC
    b. Avatar creation
2. User initiates interactions within a virtual world
3. User verifies other user's data

C. *Solution*

System is illustrated in Figure 1. It is consisted of five entities and one auxiliary structure:

1. Users - using virtual worlds as a way of interaction and managing their personal data;
2. Service providers – providing services to users in the virtual world and using their data
3. Blockchain – storing records of user interaction
4. KYC – 3rd party secure user id verification service
5. Virtual world – immersive platform for interaction between users/service providers through the use of 3D avatar navigation
6. Avatar creation system – avatar creation from biometric data

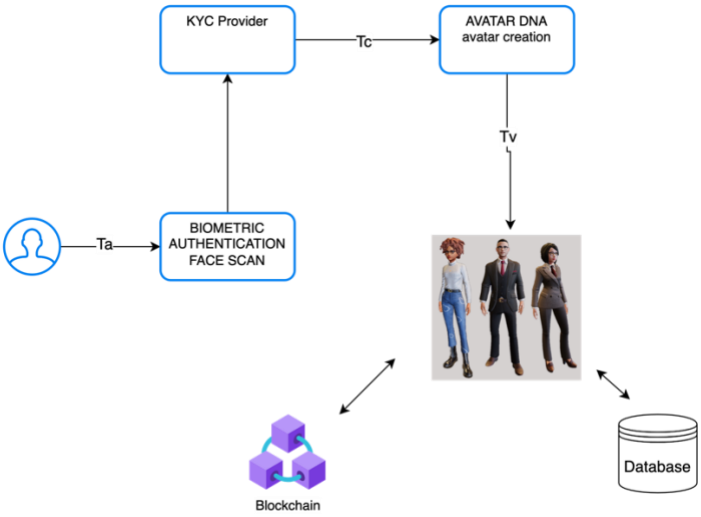

Figure 1. – Solution design

The solution has three transactions:

- Ta – user scans his face to authenticate to the virtual world platform
    - Result: Face image
- Tc – user data, is used to create a user avatar with avatar creation system
    - Result: Avatar character
- Tv – avatar interacts with people, places and things within a virtual world with a verified Unique ID
    - Input Avatar character, ID
    - Output: Transaction hash

All interactions of verified avatar are stored on the blockchain.

Example of the process:

User scans his face to authenticate to the virtual world platform, Ta will be generated and sent to the biometric authentication face scan. Ta transactions is used to generate face image of the user and send it to KYC provider. KYC provider verifies user's identity. Once user is verified from KYC, UID is generated – hashed value. Key pair of UID and access permissions will be stored on the blockchain. That will represent permissions for that service for using user's personal data. User data that is collected from the user side – face image and UID is used to create a user avatar with Avatar creation system as a Tc transaction. When avatar interacts with people, places and things within a virtual world with UID Tv transactions is created and results with a hash value – transactions hash, that is stored on the blockchain.

Now users can interact with secure e-identity, knowing exactly with who they are interacting with.

The Blockchain part of the system is used to protect user-sensitive data and avatar interactions on the system. Transactions that include blockchain are used for storing and fetching sensitive and essential data. When a user successfully registers and created his e-identity, storing that identity on the blockchain will secure it from tampering or malicious actions on that data.

A biometric security service is used to facilitate the secure authentication of the user, where the user will provide biometric data on sign-in/register and the service will validate that data. That information is being used firstly to be verified by a trusted authority and then for user e-identity that will be stored on the blockchain – the system is secured, and the user is verified. Essential actions on the system will create transactions that will store data on the blockchain. Those transactions are about user-sensitive data and his ownership of digital assets. Data, collected from the user side is encrypted and sent to the blockchain, also a portion of the data will be stored off- chain for better performance. Services in the system will only access data that is verified. Biometric information is provided as an uploaded picture from a mobile device or pc camera. The personalized avatar that is created from an uploaded photo is then matched with the uploaded photo used to create the biometric ID is unambiguously linked to them, and are taken to reproduce, in case of future claims, the way in which the user signed as well as validate its authorship. This combined avatar and biometric information of the signature is stored, in order to facilitate the future interoperability of this data with any verification tool.

The solution will be created as a demo virtual world where users will have demo functions that are needed to perform test scenarios. The user will have a dashboard as a web app where he can handle all his data and where he can join the virtual world.

IV. RESULTS

A. Privacy & Security Analysis

We measured results by test scenarios:

1. When user creates an avatar, he needs to provide face photo and will be verified by KYC.
2. KYC is trusted to know user identity and stores user ID info. KYC provider returns UID which is a hash value pointer for user records.
3. When user is verified with KYC provider, he will go through Avatar DNA™ process to use photo from KYC to create avatar. This process ensures that user matches his avatar with KYC providing info.
4. User is a controller of his data, and can revoke permissions, delete his data (remove hash pointer).
5. Interactions of a avatar are stored on the blockchain as transactions – being transparent and verifiable for parties.

B. GDPR Analysis

We analyze GDOR compliance with following test case:

- Data stored on the blockchain is UID, which is hashed value pointer, so it can be GDPR compliant (Art. 16 & Art. 17).

The model that is designed this way, ensures that in the virtual world there is complete trust for user identities. Parties in the system can interact with each other in a safe way with numerous use- cases of interactions in the virtual world. Also, the model will ensure the user will control his sensitive data. Blockchain as decentralized technology combined with biometric security and virtual world will ensure that services and participants cannot access with false claims or corrupt the network. An intruder can't have a different avatar rather than the one created from his biometric information (face), meaning that other parties will know who that user is, because of the immersiveness of the virtual world. Also, other parties can't steal or learn anything from user data because it's being stored on the blockchain as encrypted value.

V. DISCUSSION

The virtual world is a new immersive place where users are interacting and it's important for that world to be secured in the right way, so every participant can know with who he is collaborating. Without that kind of security, virtual worlds are susceptible to attacks and misuse. Users need to own and control their personal data without compromising security. The key benefit is that blockchain and biometric security service recognizes users as verified participants and owners of their sensitive data.

Our model provides that solution with biometric security to create user facial data and send it to virtual world for creating an avatar with storing all user avatar data to immutable ledger. With that model, doing interactions in virtual worlds are much safer, because user is verified through KYC and Avatar creation system.

Our solution allows users to own, manage, and control their online identity and its use. Every Avatar belongs to a real person and is part of a global community of verified and known users. Instead of actually showing their ID to the respective authority for verification, digital identity will allow people to show that the ID has been verified, whiteout sharing sensitive personal data. The Avatars are part of a global ecosystem that supports the verification and creation of a digital or Self Sovereign Identity (SSI) where the user, not corporations or other parties, own the information.

Some examples of interactions that need this protection are:

- Signing a contract
- Interaction with banks
- Health records

REFERENCES

[1] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In ICDE, volume 7, pages 106–115, 2007

[2] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity.ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3, 2007.

[3] Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557–570, 2002.

[4] Juan Perez. Facebook, google launch data portability programs to all, 2008.

[5] K Schwab, A Marcus, JO Oyola, W Hoffman, and M Luzi. Personal data: The emergence of a new asset class. In An Initiative of the World Economic Forum, 2011.

[6] R. Di Pietro and S. Cresci, "Metverse: Security and privacy issues

[7] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105, 2006.

[8] J. Horgan, "Should big tech's plan for a metaverse scare us?" Scientific American, 2021

[9] A. Woodgate, "The metaverse," DUBIT Exclusive Report, Tech. Rep., 2021.