Eye Tracking Data Collection Protocol for VR for Remotely Located Subjects using Blockchain and Smart Contracts

Efe Bozkir, Shahram Eivazi, Mete Akgün and Enkelejda Kasneci
Department of Computer Science, University of Tübingen
Tübingen, Germany
Email: {efe.bozkir, shahram.eivazi, mete.akguen, enkelejda.kasneci}@uni-tuebingen.de

***Abstract*—Eye tracking data collection in the virtual reality context is typically carried out in laboratory settings, which usually limits the number of participants or consumes at least several months of research time. In addition, under laboratory settings, subjects may not behave naturally due to being recorded in an uncomfortable environment. In this work, we propose a proof-of-concept eye tracking data collection protocol and its implementation to collect eye tracking data from remotely located subjects, particularly for virtual reality using Ethereum blockchain and smart contracts. With the proposed protocol, data collectors can collect high quality eye tracking data from a large number of human subjects with heterogeneous socio-demographic characteristics. The quality and the amount of data can be helpful for various tasks in data-driven human-computer interaction and artificial intelligence.**

***Keywords*-virtual reality; eye tracking; data collection; blockchain; smart contract;**

I. Introduction

Over past decades, head-mounted display (HMD) technologies have taken advantage of innovations from imaging and eye tracking research to improve image quality and utility of user interfaces. To date, several consumer level HMDs have integrated eye trackers, providing opportunity for researchers to collect eye movement data for user behavior analysis and data-driven interaction.

In the virtual reality (VR) context, it has been shown that eye tracking is helpful for assessing human attention [1], detecting human stress [2], assessing cognitive load [3], predicting human future gaze locations [4], supporting evaluation and diagnosis of diseases [5], motion sickness detection [6], foveated rendering [7], [8], continuous authentication [9], gaze-based interaction [10], training [11], and redirected walking [12]. Many of these tasks are data-driven and require a large quantity of eye tracking data which are usually collected in laboratory settings. Subjects are frequently compensated with some amount of money or gifts for their participation. Two drawbacks of these settings are the lack of heterogeneity in socio-demographic characteristics of data collected subjects and potential for unnatural behaviors of subjects due to the constraints of the laboratory settings. While VR is a unique and controlled environment and requires dedicated hardware such as HMDs, as personal usage of such devices increases, we foresee that it should be possible to collect data from remotely located subjects, i.e., at their homes. Especially in situations such as COVID-19, this possibility could help experimental works continue in a remote setting. Currently, for crowd-sourcing or similar purposes, platforms such as Amazon Mechanical Turk[1] are used. While it is not possible to collect VR data with such platforms, for other types of data collection significant compensations are paid to manage the remote subjects' work. In addition, these third-party platforms store and manage data. In fact, as eye tracking and movement data represent unique information about the subjects, the data manipulation possibility of the third parties should be prevented. Third parties should only act as a bridge between the data collector and the subjects in case there is no direct communication between the parties.

To overcome the disadvantages of the laboratory setting and enable remotely located subject participation in eye tracking experiments in the VR context, we propose a blockchain-based protocol on the Ethereum blockchain using smart contracts, where we use the blockchain for validation of data integrity and smart contract for compensation management. For this study, we focus mainly on collecting eye tracking data in VR environments as many modern HMDs come with integrated eye trackers. This means that subjects do not need any additional effort to integrate any sensor into their setup. It is relatively easier to control environmental configurations in HMDs when compared to other setups such as illumination and light-sources which may affect subject behaviors or eye movement patterns. However, the proposed protocol can also be used in similar setups as long as identical experiment configurations are guaranteed.

While the first prominent usage of the blockchains is Bitcoin [13] and most of the applications are in the financial domain, blockchains also draw attention of the human-computer interaction (HCI), eye tracking, and VR communities. Opportunities and challenges for the HCI and interaction design and the role of HCI community were discussed in [14] and [15], respectively. An augmented reality (AR)-based cryptocurrency wallet was developed

[1] https://www.mturk.com/

in [16] to familiarize users with blockchain wallet services. In addition, GazeCoin is a cryptocurrency for VR/AR which is exchanged between content makers, advertisers, and the users [17]. Apart from the financial use-cases, due to their immutability blockchains are used as notary. Additionally, Ethereum platform brings the smart contract [18] concept to the blockchains [19]. One of the straightforward usages of smart contracts is escrow services. For the remote purchase of goods, buyer and seller parties use the smart contracts without trusting one another and a trusted centralized party during the escrow. The smart contracts that are deployed on the blockchains distribute the money to the parties once buyer and seller parties fulfill their obligations in the remote purchase. In our protocol, we treat recorded eye tracking data as digital good so that compensation distribution is done by the smart contracts. To assure that the recorded data are not altered by the subjects, the hash of the recorded data using white-box cryptography [20] is stored in the blockchain, which enables the blockchain as a notary for data integrity. Our major contributions are as follows.

- A blockchain-based eye tracking data collection protocol for remotely located subjects that can be used for eye tracking experiments in VR, which presents the opportunity to collect data from a various number of subjects.
- Delegation of mutual trust issues for compensation management and integrity of the recorded eye tracking data to smart contracts and blockchains, respectively.
- Elimination of the centralized third parties for compensation management, data collection and manipulation, which is optimal from a privacy perspective.

II. Preliminary Definitions

As our protocol consists of interdisciplinary work from different domains such as virtual reality, blockchains, and cryptography, we provide some definitions that are used throughout the paper.

Blockchain [13]: An immutable ledger that consists of a chain of blocks that keeps records of transactions, maintained by several machines in a peer-to-peer network. Each block consists of a timestamp, transaction data, and the cryptographic hash of the previous block. As each block consists of the cryptographic hash of the one prior, immutability is automatically preserved unless one party has the majority of the computational power.

Ethereum [19]: Public, open-source, blockchain-based, and smart contract supporting distributed platform.

Ether (ETH) [19]: The cryptocurrency of the Ethereum platform.

Smart Contract [19]: A self-executing, irreversible, and transparent contract between buyer and seller, implemented in the code.

White-box cryptography [21]: "Software protection technology which allows for the application of cryptographic operations without revealing any critical information such as secret keys."

III. Protocol

In this section, we discuss our protocol and its flow, assumptions, and details of the implementation.

A. Flow

Our proposed protocol consists of two parties as data collector and subjects. The data collector is responsible for providing the VR application for eye tracking data collection and subjects are tasked with carrying out the experiment and providing the recorded eye tracking data. At the end of a valid experiment, subjects are compensated for their participation. Let us assume that each subject is compensated with X unit of ETH for the valid data recorded from an experiment session. A relevant amount can be set for compensation depending on the experiment.

Figure 1 shows the overall flow and short descriptions of each step of the protocol. As the **step 1**, subjects fetch the application from the data collector and carry out the experiment. While the content of the stimuli changes depending on the use-case, the VR application validates the eye tracking data quality at the end of each experimental session by using tracking rates or confidence intervals that are provided by the eye tracker. If the recorded eye tracking data are too noisy, subjects are not supposed to send the data to the data collector, where they are informed by the VR application. This obligation forces the subjects to follow the instructions of the VR experiment, such as eye tracker calibration, carefully while the data collector obtains better quality data in the end. After the validation success, the VR application calculates the hash output of the recorded eye tracking data and saves it. Saving the hash output is required for assessing the data integrity; however, adversarial subjects can easily find out the hashing algorithm using the executable of the VR application on their own devices. Therefore, we opt for a white-box [20], [21] paradigm for calculating the data hash. In the white-box paradigm, the adversary is supposed to have visibility of the inputs, outputs, and other intermediate steps. White-box cryptography achieves protection of confidential information such as secret keys while keeping the application semantically the same. Even if adversaries infer the hash function, due to the lack of secret key, it is not possible to generate a hash output for altered data. Consequently, subjects are obliged to behave honestly, where honest behavior means not altering the recorded data. In the end of the first step, once the recorded data is validated and hash value is saved, the subjects are informed by the VR application that the recorded eye tracking data is reportable.

As the **step 2**, the subjects initiate the smart contract and stake double the amount of compensation, which is $2X$ ETH for our case. Staking double the amount of compensation that they will obtain from the smart contract forces subjects

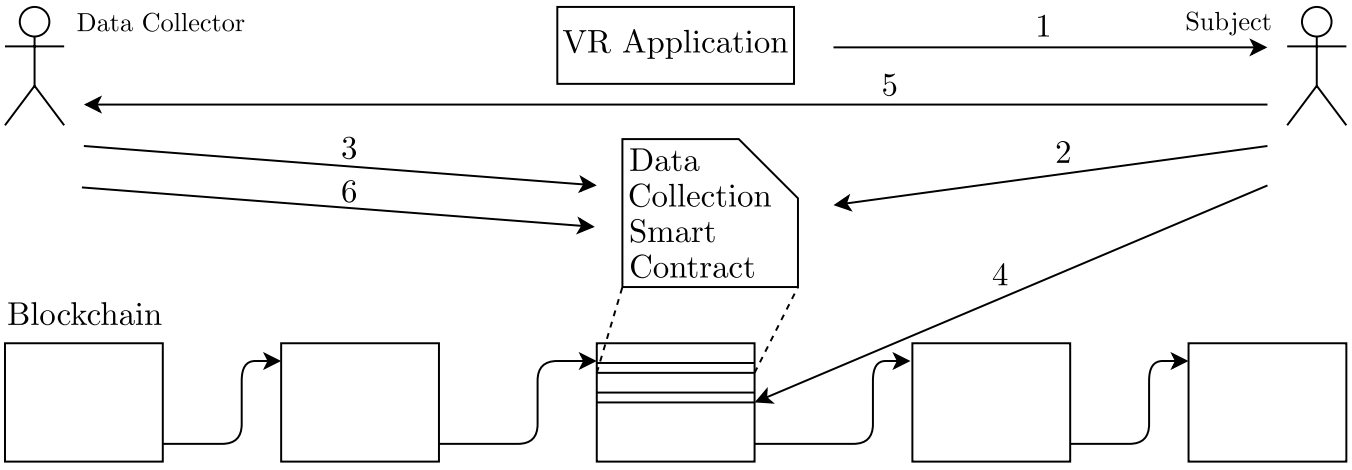

Figure 1. Blockchain-based protocol and its steps. (1) Subject fetches the application and carries out the experiment. (2) Subject initiates the smart contract. (3) Data collector confirms the contract creation and stakes. (4) Subject stores the recorded data hash in blockchain. (5) Subject transfers the recorded data to the data collector. (6) Data collector confirms the data collection.

to act honestly; otherwise, they lose the amount that they stake. As the **step 3**, the data collector confirms the data collection and stakes the same amount as the subject, which is $2X$ ETH to the smart contract. While the compensation is X ETH per experiment, the data collector is supposed to stake double the amount of compensation so that it also becomes an obligation to behave honestly. Otherwise, the doubled amount of compensation will be lost without obtaining the recorded data. As the **step 4**, the subjects store the hash output that is reported by the VR application in the blockchain and, as the **step 5**, they send the recorded data along with the transaction hash of the transaction for storing the data hash in the blockchain to the data collector. If subjects try to alter the data, the hash in the blockchain and the altered data will not match and it will be discovered by the data collector. As the **step 6**, the data collector obtains the recorded eye tracking data and transaction hash of the data hash and checks whether or not the obtained data and the hash provided by the subjects overlap using the hash function that is implemented in the VR application and secret keys. If the reported data and hash value stored in the blockchain overlap, the data collector confirms the smart contract and that the obtained data are valid. Then, the smart contract automatically distributes $3X$ and X ETH to the subject and the data collector, respectively. In the end, each subject earns X unit of ETH for participation in the experiment, where the data collector obtains the recorded eye tracking data. Due to the immutable nature of blockchains and smart contracts, none of the parties can alter the values in the blockchain and behave as an adversary.

In the protocol, as both parties stake more than the amount they are supposed to spend or earn, they have to act honestly in order to achieve successful data collection and compensation distribution, otherwise data collection is not finalized and parties lose the amount they stake. In particular, the subjects have to stake double the amount of compensation that they will receive whereas the data collectors have to stake double the amount of compensation that they will give. Since the smart contracts are immutable and stored in the blockchain, a third-party application is not needed for compensation distribution or data manipulation, which is useful from a privacy preservation point of view.

B. Assumptions

We have three main assumptions in our protocol. Firstly, validation of the quality of the recorded eye tracking data is automatically completed by the VR application at the end of each experiment by using metrics such as tracking ratio or confidence levels reported by the eye tracker. Due to poor calibration for eye tracking, removal of the head-mounted display (HMD) in the middle of experiment, or similar reasons, recorded eye tracking data may have an extensive amount of noise level. Instead of cleaning data offline extensively after the experiments, our protocol assumes that data validity is checked at the end of each experiment by the VR application and the application informs the subjects whether the quality of the data is valid and reportable.

Secondly, the recorded eye tracking data is hashed using white-box cryptography and stored at the end of the experiment by the VR application to be stored in the blockchain for validation of the data integrity. In traditional eye tracking experiments, subjects participate in the experiments on the devices that are provided by the data collectors. However, in the remotely located subject participation, subjects run the applications on their own devices. Therefore, they have direct access to the provided application and if any adversarial subject analyzes the binary implementation of an application that does not use white-box paradigm, they can easily infer the used hash function and generate hash output for fake

data. On the contrary, when using white-box cryptography, the secret keys are not leaked even if adversaries analyze the binary implementation. Even if an adversary infers the hash function, a hash output for fake data cannot be generated without secret keys. Therefore, white-box paradigm is used by the VR application. If subjects alter the recorded data or send fake data to the data collector, the generated hash value will not match the recorded data, which leads subjects to lose their staked compensation in the smart contract.

Lastly, as our protocol does not use any centralized third party, a secure direct communication is needed for exchanging the application and the recorded data between the data collector and subjects. In case it is not available, a bridging third party only for communication purposes can be implemented.

C. Implementation

We select the Ethereum platform for our proof-of-concept due to its public blockchain, relatively higher number of nodes, and status as one of the most mature platforms in the blockchain domain. However, any blockchain-based platform that supports smart contracts can be opted in.

We implement the blockchain related part of the protocol, particularly the steps 2, 3, 4, and 6 discussed in Section III-A, using Solidity[2] and a simple purchase smart contract [22] on the Ropsten Testnet of the Ethereum platform. In the beginning of the data collection, both the data collector and the subject hold 1 ETH in their wallets. We select the compensation amount as 0.025 ETH. For the calculation of the hash output of the recorded eye tracking data, we use synthetic data; however, any eye tracker integrated to modern HMDs can be used in a real-world implementation. The hash value of the data is calculated using Keyed-Hashing for Message Authentication (HMAC) [23] and Secure Hash Algorithm3-512 (SHA3-512) [24] as it is possible to have white-box implementation of the HMAC. The calculated hash value is stored in the input data field of a self transaction from the subject. After the protocol execution, the data collector and the subject hold ≈ 0.975 and ≈ 1.025 ETH when the transaction fees are subtracted, respectively. The smart contract, overall procedure, the data collector, and the subject parties are available on the Ropsten Testnet via following link: https://ropsten.etherscan.io/address/0x0e937a4a4618dd8d5a12ec4a9f8fd61d6bfd13e4.

In the above link, there are three transactions in chronological order that correspond to steps 2, 3, and 6 of our protocol. The subject (address starting with $0x89$) and the data collector (address starting with $0x44$) of our implementation are available in the source of the first and the second transactions of the smart contract, respectively. There are three transactions in the subject address. The first and second transactions are for depositing the test ETH and initiating the smart contract, respectively. The third transaction in the subject address is a self transaction and corresponds to step 4 of our protocol. In the "Input Data" field of the self-transaction, the calculated data hash is available.

[2]https://docs.soliditylang.org/

IV. Conclusion and Discussion

We proposed a blockchain-based protocol for collecting eye tracking data in VR from remotely located subjects. As eye tracking experiments are usually conducted in laboratory settings with a limited number of subjects from similar backgrounds in terms of socio-demographic characteristics, it is a challenge to draw generic data-driven conclusions. Due to the laboratory settings, subjects may not behave naturally. While our protocol overcomes the drawbacks of the traditional eye tracking data collection setups without needing a centralized third party for data collection and compensation management, it also creates an opportunity to carry out the data collection anonymously, which is optimal for the privacy of subjects. We focused on the eye tracking data collection in VR setups as validation of the eye tracking data and generation of the controlled environments with VR can be done easily. In addition, current availability of eye tracker integrated HMDs in the consumer market supports our protocol for VR and eye tracking data; however, the proposed protocol may be useful for other types of eye trackers, sensors, or environments as long as identical configurations between subjects can be generated. In contrast to traditional eye tracking experiments, subject consent, additional questionnaire, or similar information should be collected digitally using our protocol. Our protocol may also require an application-level effort to have one-to-one mapping between subjects and experiments.

As future work, we plan to have an end-to-end implementation of our protocol along with a real VR application and HMD-integrated eye tracker. In addition, while transactions are applied anonymously on the public blockchains, it is possible to track them. Recent work on eye tracking, HCI, and VR [25]–[29] emphasize the importance of privacy preservation. Combining privacy-preserving methods with our protocol remains as part of future work.

Acknowledgments

E.B. thanks Batuhan Sarıoğlu for useful discussions on blockchains.

References

[1] E. Bozkir, D. Geisler, and E. Kasneci, "Assessment of driver attention during a safety critical situation in VR to generate vr-based training," in *ACM Symposium on Applied Perception 2019*, ser. SAP '19. New York, NY, USA: ACM, 2019.

[2] C. Hirt, M. Eckard, and A. Kunz, "Stress generation and non-intrusive measurement in virtual environments using eye tracking," *Journal of Ambient Intelligence and Humanized Computing*, Mar 2020.

[3] E. Bozkir, D. Geisler, and E. Kasneci, "Person independent, privacy preserving, and real time assessment of cognitive load using eye tracking in a virtual reality setup," in *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 2019, pp. 1834–1837.

[4] Z. Hu, S. Li, C. Zhang, K. Yi, G. Wang, and D. Manocha, "DGaze: CNN-Based gaze prediction in dynamic scenes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 5, pp. 1902–1911, 2020.

[5] J. Orlosky, Y. Itoh, M. Ranchet, K. Kiyokawa, J. Morgan, and H. Devos, "Emulation of physician tasks in eye-tracked virtual reality for remote diagnosis of neurodegenerative disease," *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 4, pp. 1302–1311, 2017.

[6] T. M. Lee, J.-C. Yoon, and I.-K. Lee, "Motion sickness prediction in stereoscopic videos using 3d convolutional neural networks," *IEEE Transactions on Visualization and Computer Graphics*, vol. 25, no. 5, pp. 1919–1927, 2019.

[7] E. Arabadzhiyska, O. T. Tursun, K. Myszkowski, H.-P. Seidel, and P. Didyk, "Saccade landing position prediction for gaze-contingent rendering," *ACM Trans. Graph.*, vol. 36, no. 4, Jul. 2017.

[8] X. Meng, R. Du, and A. Varshney, "Eye-dominance-guided foveated rendering," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 5, pp. 1972–1980, 2020.

[9] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous authentication using eye movement response of implicit visual stimuli," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 1, no. 4, Jan. 2018.

[10] M. Khamis, C. Oechsner, F. Alt, and A. Bulling, "VRpursuits: Interaction in virtual reality using smooth pursuit eye movements," in *Proceedings of the 2018 International Conference on Advanced Visual Interfaces*, ser. AVI '18. New York, NY, USA: ACM, 2018.

[11] Y. Lang, L. Wei, F. Xu, Y. Zhao, and L.-F. Yu, "Synthesizing personalized training programs for improving driving habits via virtual reality," in *2018 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, 2018, pp. 297–304.

[12] E. Langbehn, F. Steinicke, M. Lappe, G. F. Welch, and G. Bruder, "In the blink of an eye: Leveraging blink-induced suppression for imperceptible position and orientation redirection in virtual reality," *ACM Trans. Graph.*, vol. 37, no. 4, Jul. 2018.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[14] M. Foth, "The promise of blockchain technology for interaction design," in *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, ser. OZCHI '17. New York, NY, USA: ACM, 2017, p. 513–517.

[15] C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed, and J. Vines, "Making sense of blockchain applications: A typology for HCI," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: ACM, 2018, p. 1–14.

[16] Y.-P. Chen and J.-C. Ko, "CryptoAR wallet: A blockchain cryptocurrency wallet application that uses augmented reality for on-chain user data display," in *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '19. New York, NY, USA: ACM, 2019.

[17] GazeCoin, "Gazecoin: A unit of exchange between advertisers, content makers and users based on 'gaze'/eye tracking," Oct 2017. [Online]. Available: https://www.gazecoin.io/s/GazeCoin_WhitePaper.pdf

[18] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, Sep 1997. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/548

[19] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum, 2014.

[20] A. Biryukov and A. Udovenko, "Attacks and countermeasures for white-box designs," in *ASIACRYPT (2)*, ser. Lecture Notes in Computer Science, vol. 11273. Springer, 2018, pp. 373–402.

[21] B. Wyseur, "White-box cryptography: hiding keys in software," MISC magazine, Apr 2012. [Online]. Available: https://whiteboxcrypto.com

[22] J. Ng, "Escrow service as a smart contract: The execution," May 2018, Accessed: 2020-09. [Online]. Available: https://jacksonng.org/escrow-service-smart-contract-execution

[23] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," Internet RFC2104, 1997.

[24] M. J. Dworkin, "SHA-3 standard: Permutation-based hash and extendable-output functions," NIST FIPS - 202, Aug. 2015.

[25] E. Bozkir, A. B. Ünal, M. Akgün, E. Kasneci, and N. Pfeifer, "Privacy preserving gaze estimation using synthetic images via a randomized encoding based framework," in *ACM Symposium on Eye Tracking Research and Applications*, ser. ETRA '20 Short Papers. New York, NY, USA: ACM, 2020.

[26] J. Steil, I. Hagestedt, M. X. Huang, and A. Bulling, "Privacy-aware eye tracking using differential privacy," in *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, ser. ETRA '19. New York, NY, USA: ACM, 2019.

[27] W. Fuhl, E. Bozkir, and E. Kasneci, "Reinforcement learning for the privacy preservation and manipulation of eye tracking data," 2020. [Online]. Available: https://arxiv.org/abs/2002.06806

[28] Ö. Sümer, P. Gerjets, U. Trautwein, and E. Kasneci, "Automated anonymisation of visual and audio data in classroom studies," in *The Workshops of the Thirty-Forth AAAI Conference on Artificial Intelligence*, Feb 2020.

[29] E. Bozkir, O. Günlü, W. Fuhl, R. F. Schaefer, and E. Kasneci, "Differential privacy for eye tracking with temporal correlations," 2020. [Online]. Available: https://arxiv.org/abs/2002.08972