SECURITY CONCERNS FOR BLOCKCHAIN BASED SHARING OF MOBILE STUDENT CREDENTIAL

Timothy Arndt

Department of Information Systems,
Cleveland State University, Cleveland, OH, USA

ABSTRACT

Blockchain has recently taken off as a disruptive technology, from its initial use in cryptocurrencies to wider applications in areas such as property registration and insurance due to its characteristic as a distributed ledger which can remove the need for a trusted third party to facilitate transaction. This spread of the technology to new application areas has been driven by the development of smart contracts – blockchain-based protocols which can automatically enforce a contract by executing code based on the logic expressed in the contract. One exciting area for blockchain is higher education. Students in higher education are ever more mobile, and in an ever more agile world, the friction and delays caused by multiple levels of administration in higher education can cause many anxieties and hardships for students as well as potential employers who need to examine and evaluate student credentials. Distance learning as a primary platform for higher education promises to open up higher education to a wider range of learners than ever before. Blockchain-based storage of academic credentials is being widely studied due to the advantages it can bring. As with any network-based system, blockchain comes with a number of security and privacy concerns. Blockchain needs to meet several security-related requirements in order to be widely accepted: decentralization; confidentiality; integrity; transparency; and immutability. Researchers have been busy devising schemes to ensure that such requirements can be met in blockchain-based systems. Several types of blockchain-specific attacks have been identified: 51% attacks; malicious contracts; spam attacks; mining pools; targeted DDoS attacks; and others. Real-world attacks on blockchain-based systems have been seen on cryptocurrency sites. In this paper, we will at look at the specific privacy and security concerns for blockchain-based systems used for academic credentials as well as suggested solutions. We also examine the issues for academic credentials which are stored "off-chain" in such systems (as is often the case).

KEYWORDS

Blockchain, Mobile Education, Higher Education, Privacy, Security.

1. INTRODUCTION

The blockchain idea was introduced in a paper published by Satoshi Nakamoto [1] and deployed in the bitcoin cryptocurrency the following year. Blockchain is an open, distributed ledger that can efficiently record transactions between two parties in a verifiable and immutable (permanent) fashion without the need for a trusted third party (disintermediation).

Bitcoin employs a peer-to-peer architecture and relies on proof-of-work, a piece of data which is time consuming and computationally complex to produce, but which is easy for others to verify (via "miners" who are rewarded with bitcoin for this computational work) and which satisfies

David C. Wyld et al. (Eds): DMML, SEAS, ADCO, NLPI, SP, BDBS, CMCA, CSITEC - 2022
pp. 139-145, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120712

certain requirements as a consensus mechanism. Consensus mechanisms allow for the correctness or "truth" of a transaction to be confirmed (depending on a set of rules) when multiple distributed actors perform transactions, and some of those actors may be untrustworthy. Subsequent developments have allowed blockchain to be programmed (via smart contracts) to trigger transactions automatically [2]. Transactions can cause code implementing rules which are part of the blockchain to be run, through these blockchain can lead to what have been called Distributed Autonomous Organisations (DAOs).

As a foundational technology, blockchain has been used or proposed in many application areas besides cryptocurrencies [3] including the banking sector [4], land registration (especially in developing countries) [5], the insurance sector [6], and electronic voting [7]. Alternative consensus mechanisms (such as proof of stake and mechanisms based on Byzantine Fault Tolerance) have been developed as well as alternative architectures (e.g. client-server).

In this paper, we will at look at the specific privacy and security concerns for blockchain-based systems used for academic credentials as well as suggested solutions. For further study on blockchain in higher education, [8], [9] (related works section of this work), and [10] will be helpful. We also examine the issues for academic credentials which are stored "off-chain" in such systems (as is often the case).

2. BLOCKCHAIN IN HIGHER EDUCATION

In this section we will take a brief look at a few representative projects in the application of blockchain technology in higher education.

A number of researchers have explored the use of blockchain to store university grades, i.e. university transcripts. A group at the University of Glasgow has developed a functional prototype for storage of student grades at the institution [11]. The platform chosen was Ethereum, hence it was built on a public blockchain. Based upon an exploratory, qualitative evaluation the authors found several tensions between the concepts of a university as an organization and of distributed autonomous organizations (DAOs) in Ethereum. Another project with a prototype implementation is [12], where a private BigChainDB blockchain is used for storage of student transcripts (not grades within a course as in the previously described research, though). Initial results were reported to be promising. Mahamatov et al.[13] describe a prototype implementation of a university transcript system using an Ethereum private blockchain and ERC-20 tokens (a standard for tokens, which are needed to carry out smart contracts, on Ethereum) on that blockchain. Students are able to read their grades, while professors and administrative personnel can record grades.

EduCTX [14] is an ambitious project for the development of a higher education credit platform based on the European Credit Transfer and Accumulation System (ECTS), a framework which has been approved by the EU. The decentralized higher education credit and grading system can offer a globally unified viewpoint for students, higher education institutions, and other potential stakeholders such as prospective employers. A prototype implementation has been built on the ARK blockchain platform [15]. ARK is a public blockchain, but the authors transformed it into a private (permissioned) one by taking advantage of the flexible nature of ARK to change the parameters of the DPoS (delegate proof of stake) consensus algorithm used. Logic to ensure the validity of transactions on the blockchain has been defined. ECTX tokens represent credits that students gain for completing courses (analogous to the way that ERC-20 tokens are used in [13]). The authors will use the prototype system firstly at their home institution, the University of Maribor, and then at a select set of institutions of higher education. They anticipate that this or a

similar system could potentially evolve into a unified, simplified, globally ubiquitous higher education credit and grading system.

A more theoretical investigation is given by [16] in which the architecture for the Disciplina platform for student records is described and an analysis of the main issues arising from storing student records in a blockchain is given. Their platform incorporates both private blockchains (maintained by individual institutions of higher learning) and public blockchains, managed by "Witnesses" who witness the fact that a private block was produced by a valid institution. A good, theoretical discussion of the problems of privacy, provability, and data disclosure in this context is given.

Besides traditional transcripts, blockchain is also being used or proposed for various alternative types of educational credentials. Blockchain enables permanent authentication and storage for a myriad of alternative credentials made up of diverse microcredentials, nanodegrees, MOOCs, and certificates/badges from various types of training programmes. These credentials can then be directly controlled and managed by users [17].

Among the most well-known of higher education blockchain projects was that at MIT's Media Lab which created blockcerts, a mobile app for educational credentialing built on Bitcoin [18]. At the Open University, researchers have developed the OpenLearn system built on the Ethereum public blockchain which awards OpenLearn badges for completing sections of a course and passing assessments [19]. The creators of that system have also developed a blockchain project to create a permanent distributed record of intellectual effort and associated reputational reward that instantiates and democratises educational reputation beyond the academic community. Blockchain for Education [20] is another prototype system supporting the storage, retrieval and verification of certificates via blockchain technology. Certificates are an important means of proving lifelong learning achievement in today's environment, however they are susceptible to forgery. Blockchain helps to solve this problem. The prototype system uses Ethereum and its smart contracts to manage identities of registered certificate authorities and the hashes of certificates which are stored in a separate, centralized document management system, while the profile information of certificate authorities is stored using the Interplanetary File System (IPFS) distributed file system. Storing data off the blockchain allows it to be be deleted as is required, for example, by the European General Data Protection Regulation (GDPR) for personal information.

Other uses of blockchain in higher education have also been contemplated, including motivation, assessment, advising, etc. [21]. A prototype system for a blockchain based learning analytics platform built on Ethereum has been proposed as well [22].

3. SECURITY AND PRIVACY ISSUES IN BLOCKCHAIN

A number of different types of security problems have been noted in blockchain. In this section, we survey a few of these and how they relate to blockchain in education.

3.1. 51% Attacks

Blockchain relies on a distributed consensus mechanism such as proof of work (PoW) in order to establish trust. Unfortunately, the consensus mechanism is itself vulnerable to a 51% attack. This occurs when a single malicious miner or mining pools controls more than 50% of the total hashing power of the entire blockchain [23]. The malicious miner who controls this much hashing power has basically unlimited power to manipulate and modify the blockchain

information including reversing transactions, changing the ordering of transactions and blocking transactions from being verified. A mining pool for the Bitcoin blockchain at one time reached 42% of hashing power before miners dropped out of the pool in order to stop a 51% attack from becoming possible [24].

51% attacks require a large investment in computing power and coordination in order to be carried out. While the effort might be worthwhile for the monetary gain associated with blockchains used for cryptocurrencies, for large public blockchains the effort will probably not be worthwhile for the advantages to be gained by manipulating educational credentials, unless some group wants to corrupt all of the credentials for an institution (for example), not just those of a single student. It is not to be discounted, though, that such corruption could occur as collateral damage from a 51% attack aimed at some other, more remunerative target.

3.2. Malicious Contracts

Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality [25]. Users of the Ethereum platform are 'pseudo-anonymous' and a single user can have multiple accounts under multiple cryptographic identities. It has been shown [26] how 'criminal smart contracts' can facilitate leakage of confidential information, theft of cryptographic keys, and various real-world crimes.Atzei et. al, [27], have presented a taxonomy of vulnerabilities of smart contracts in Ethereum including such vulnerabilities as stack overflow, exception disorder and unpredictable state. Various countermeasures to these malicious contracts have been proposed, including malicious contract detection using supervised learning [25].

For higher education blockchain, likely the most serious threat from this type of attack is the leaking of private credentials. However, it is also possible that a malicious contract exploiting the vulnerabilities identified above might falsely update a student's credentials, corrupting them.

3.3. Sybil Attacks

In a Sybil attack, a single adversary controls many nodes in a system by creating numerous fake identities in order to gain a disproportionately large influence [28]. A defense against Sybil attacks can rely on validated identities issued by a trusted authority. The requirements for agents to present a trusted identity conflicts with the need for permissionless open membership, though. An example of a blockchain development to defeat Sybil attacks is TrustChain [29] which includes a novel Sybil-resistant algorithm NetFlow to determine the trustworthiness of agents in an online community.

3.4. Eclipse attacks

An eclipse attack will allow the attacker to monopolize all of the victim's connections – both incoming and outgoing [30]. This will isolate the victim from other users on the network. The attacker is able to filter the victim's view of the blockchain or to cause the victim to waste computing power on obsolete views of the blockchain. The attacker is also able to use the victim's computing power to conduct its own malicious acts. In the context of education blockchain, a student might prevent a potential employer from having a complete view of all of the student's credentials.

4. CONCLUSIONS

Blockchain has been increasingly accepted in higher education as an alternative for the storage of academic records. A systematic literature review [10] shows that interest is continuing to grow, with the peak of interest occurring in the last complete year surveyed - 2020. The main advantage of blockchain in this context is that the records are not under the control of several institutions or of a centralized third party.

The current approach has each academic institution maintaining its own records, and students having to collect records from each institution they attended in order to present them to prospective employers. This system is both slow and costly (for students – institutions may make money by charging for the release of academic records). Blockchain solves the problem of speed (in addition to taking the records out of the hands of the institutions, as noted above). Some cost is associated with blockchain, however, much of that cost can be borne by prospective employers who carry out transactions on the blockchain in order to have access to academic records.

An alternative approach could be to have a trusted third party hold all of the academic records, but then we still have the problem of trust. Not all countries have an institution worthy of trust, and even in those that do, not all students may trust them (no universally trusted institution). Blockchain does not require a trusted third party, so it solves this problem.

As was seen in the descriptions of the types of attacks in the previous section, many of the attack strategies require obtaining large amounts of computing power in order to be effective. Such an attack may be considered worthwhile in the cryptocurrency application of blockchain, but in the education sector, no such financial incentive is apparent for attacks on a single student's credentials. Possibly the blackmailing of a large institution poses more of a threat, though given the higher payoffs available to criminals in other blockchain areas, that is still rather farfetched. The threats associated with malicious contracts seem to be more of concern in educational blockchain, since they may corrupt educational credentials.

Given the high cost of storing data on the blockchain, it is likely that educational transcripts themselves will be stored off the blockchain, with only the credentials needed to access and verify them being stored on the blockchain. One popular mode of storing data off the blockchain is to use the InterPlanetary File System (IPFS). IPFS is a peer-to-peer distributed file system, so its architecture and management style is a good match for blockchain-based architectures. For examples of the combination of blockchain and IPFS, see [31], [32] for the use in storage of electronic medical records, and [33] for the use in the automotive insurance sector.

In any case, it will be necessary for users of blockchain-based educational credential systems to keep up to date with the latest security issues in the blockchain area in order to guard against attacks, since those attacks, and the defences against them, are continuously evolving.

REFERENCES

[1] Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, [online] https://bitcoin.org/bitcoin.pdf.

[2] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X. & Wang, F. (2019) "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 49, No. 11, pp. 2266-2277.

[3] Iansiti, M. & Lakhani, K. R. (2017) "The Truth About Blockchain", *Harvard Business Review*, Vol. 95, No. 1, pp. 118-127.

[4] Peters, G. W. & Panayi, E. (2016) "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," in *Banking Beyond Banks and Money*, Springer, Cham, pp. 239-278.

[5] Underwood, S. (2016) "Blockchain Beyond Bitcoin," *Communications of the ACM*, Vol. 59, No. 11, pp. 15-17.

[6] Lamberti, F., Gatteschi, V., Demartini, C., Pranteda, C. & Santamaria, V. (2017) "Blockchain or Not Blockchain, That is the Question of the Insurance and Other Sectors," *IT Professional*.

[7] Ayed, A. B., (2017) "A Conceptual Secure Blockchain-Based Electronic Voting System," *International Journal of Network Security & Its Applications*, Vol. 93.

[8] Yumna, H. et al. (2019) "Use of Blockchain in Education: A Systematic Literature Review," in *Intelligent Information and Database Systems. ACIIDS 2019, Lecture Notes in Computer Science,* vol. 11432, N.Nguyen, F. Gaol, T.P. Hong, B. Trawiński Eds, Springer, Cham, pp. 191-202.

[9] Yokubov, B. (2018) "Blockchain Based Storage of Students Career," Master Degree Thesis, Politecnico di Torino, [online] https://webthesis.biblio.polito.it/9471/.

[10] Raimundo, R. & Rosário, A. (2021) "Blockchain System in the Higher Education", *European Journal of Investigation in Health, Psychology and Education*, Vol. 11, No. 1, pp. 276-293.

[11] Rooksby, J. & Dimitrov, K. (2019) "Trustless Education? A Blockchain System for University Grades", *Ubiquity: The Journal of Pervasive Media*, Vol. 6, No. 1, pp. 83-88.

[12] Arndt, T. (2018) "Empowering University Students with Blockchain-Based Transcripts," *Proceedings of CELDA 2018,* Budapest, Hungary, October 21-23.

[13] Mahamatov, N., Kuvnakov A. & Yokubov, B. (2020) "Application of Blockchain Technology in Higher Education," *2020 International Conference on Information Science and Communications Technologies (ICISCT),* pp. 1-6

[14] Turkanović, M. et al. (2019) "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access,* Vol. 6, pp. 5112-5127.

[15] Košič, K., Černec, R., Barnsley, A. & Thoorens, F., (2018) Building an open-source blockchain ecosystem with ARK, *OTS 2018 Sodobne informacijske tehnologije in storitve*, p. 45.

[16] Kuvshinov, K., Nikiforov, I., Mostovoy, J., Mukhutdinov, D., Andreev, K. & Podtelkin, V. (2018) Disciplina: Blockchain for education. *Yellow Paper. URL: https://disciplina. io/yellowpaper. pdf*.

[17] Selvaratnam, R.M. & Sankey, M. (2021) "An Integrative Literature Review of the Implementation of Micro-credentials in Higher Education: Implications for Practice in Australasia", *Journal of Teaching and Learning for Graduate Employability*, Vol. 12, No. 1, pp. 1-17.

[18] Blockcerts (2019) *The Open Standard for Blockchain Credentials,* [online] https://www.blockcerts.org

[19] Sharples, M. & Domingue, J. (2016) "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In *European conference on technology enhanced learning*. pp. 490-496, Springer, Cham.

[20] Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C. & Wendland, F. (2018) "Blockchain for Education: Lifelong Learning Passport", In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).

[21] Chen, G., Xu, B., Lu, M. & Chen, N.S. (2018) "Exploring Blockchain Technology and its Potential Applications for Education", *Smart Learning Environments*, Vol. 5, No. 1, pp. 1-10.

[22] Ocheja, P., Flanagan, B. & Ogata, H. (2018) "Connecting Decentralized Learning Records: A Blockchain Based Learning Analytics Platform", In *Proceedings of the 8th international conference on learning analytics and knowledge*, pp. 265-269.

[23] Shanaev, S., Shuraeva, A., Vasenin, M. and Kuznetsov, M. (2019) "Cryptocurrency Value and 51% Attacks: Evidence from Event Studies", *The Journal of Alternative Investments*, Vol. *22*, No. 3, pp.65-77.

[24] Hajdarbegovic, N. (2014) "Bitcoin Miners Ditch Ghash. io Pool Over Fears of 51% Attack", [online] http://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/.

[25] Kumar N., Singh A., Handa A., & Shukla S.K. (2020) "Detecting Malicious Accounts on the Ethereum Blockchain with Supervised Learning", In: Dolev S., Kolesnikov V., Lodha S., Weiss G. (eds) *Cyber Security Cryptography and Machine Learning*. CSCML 2020. Lecture Notes in Computer Science, vol 12161.

[26] Juels, A., Kosba, A. & Shi, E. (2016), "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts" In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 283-295.

[27] Atzei, N., Bartoletti, M. & Cimoli, T. (2017), "A Survey of Attacks On Ethereum Smart Contracts (sok)", In *International conference on principles of security and trust*, Springer, Berlin, Heidelberg, pp. 164-186.
[28] Douceur, J.R. (2002) "The Sybil Attack", In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.
[29] Otte, P., de Vos, M. & Pouwelse, J. (2020) "TrustChain: A Sybil-Resistant Scalable Blockchain", *Future Generation Computer Systems*, Vol. 107, pp. 770-780.
[30] Heilman, E., Kendler, A., Zohar, A. & Goldberg, S. (2015) "Eclipse Attacks on Bitcoin's Peer-to-Peer Network", In *24th USENIX Security Symposium (USENIX Security 15)*, pp. 129-144.
[31] Zheng, Q., Li, Y., Chen, P. & Dong, X. (2018) "An Innovative IPFS-Based Storage Model for Blockchain", In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, pp. 704-708.
[32] Sun, J., Yao, X., Wang, S. & Wu, Y. (2020) "Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS", *IEEE Access*, Vol. *8*, pp. 59389-59401.
[33] Nizamuddin, N. & Abugabah, A. (2021) "Blockchain for Automotive: An Insight Towards the IPFS Blockchain-Based Auto Insurance Sector", *International Journal of Electrical & Computer Engineering* pp. 2088-8708, Vol. 11, No. 3.

AUTHOR

Timothy Arndt is Chair and Professor of the Department of Information Systems, Cleveland State University. He received a Ph.D. in Computer Science from the University of Pittsburgh. He is editor of several journals and has been involved in the organization of several international conferences. His research interests include database systems, software engineering, e-learning, and blockchain.