Gallery Defender: Integration of Blockchain Technologies into a Serious Game for Assessment: A Guideline for Further Developments

André Thomas and Alexander Pfeiffer

Abstract Blockchain technologies are already being used in many different applications to secure specific data sets. For the same purpose, blockchain is also used in digital games. This technology is not only discussed, but also actively implemented in the educational sector, for example, in such projects as "Blockcerts". Typical applications are issuing certificates and their validation by using a one-way hash; more creative uses of blockchain beyond that are still uncharted territory. This article shows how blockchain (Ardor and its childchain Ignis) has been integrated into a serious game for assessment of students' knowledge. More specific details include encrypted meta-data in the respective transactions, and offer guidelines for future projects in education.

Keywords Blockchain · Blockchain games · Gamification · Serious games · Student assessment

1 Introduction

Blockchain offers significant opportunities, particularly from the socioeconomic perspective, that go beyond the current ways in which we deal with data storage. This includes such areas as art [17], museums [13] and learning. A summary of opportunities of blockchain for education can be found in the report by Grech and Camilleri [7]. Transfer of data sets into the blockchain and potentially rapid verification of their validity opens up new infrastructural and other possibilities that are related to the defining qualities of blockchain-based technical solutions [7, 11].

A. Thomas (✉)
Texas A&M University and Triseum LLC, College Station, TX, USA
e-mail: manink@arch.tamu.edu

A. Pfeiffer
Massachusetts Institute of Technology, Cambridge, MA, USA
e-mail: pfeiffer@alexpfeiffer.at

A. Dingli et al. (eds.), *Disruptive Technologies in Media, Arts and Design*, Lecture Notes in Networks and Systems 382, https://doi.org/10.1007/978-3-030-93780-5_4

– **Transparency** enables provenance of digital assets, i.e. artworks, so their buyers and sellers can conduct transactions and be sure that each party has the right to enter into that transaction;
– **Controllability** (self-sovereignty) allows individuals to identify themselves online while at the same time maintaining control over their personal data;
– **Trust**, in its algorithmically ensured form, provides enough confidence in payments and verified certificates;
– **Disintermediation** removes central controlling authority from the interactions between different blockchain users: the transactions are carried out in a peer to peer fashion, and the required records are made available to every participant;
– **Immutability** of a decentralized ledger of records enables permanent storage, without the possibility of modification unless designed otherwise;
– **Collaboration** can be carried out in a more democratic manner, as the parties can transact directly with each other without the need for mediating third parties.

Based on the information available in 2017, the report concludes that the use of blockchain applications in education is still in its infancy, although it is gaining fast momentum. A number of case studies have been conducted nevertheless, including the implementations at the Open University UK, the University of Nicosia, MIT and various educational institutions in Malta: each of these implementations were in a pilot phase at the time of the report [7]. The results of the pilot phase suggest that blockchain technologies might have a disruptive effect on current providers in the educational software market in the near future. As of recently, this disruption is becoming the reality, as many educational institutions and services has moved online due to the pandemic situation in 2020/21.

Based on [7], the following use cases for blockchain solutions can be named in relation to education.

– Creation of digital certificates and credentials, as well as designing digital proofs of authenticity for material certificates and printed credentials;
– Immutable storage of proofs of performance at examinations, including the related metadata;
– Recognition of examination results between and within educational institutions without the need for the central authority;
– Creating a personal "lifelong learning" record of achievements (a virtual CV) on blockchain;
– Verification of authenticity of the certificates issued by third parties;
– Management of intellectual property, e.g. results of research in the context of project implementation;
– Processing of payments, etc.

The demonstrator presented in this paper builds on Grech and Camilleri's vision of the rapidly approaching future regarding blockchain in education [7]. The aim of the team of authors was to develop a serious game [16], complete with the option for examination that transmits the results of the tests to all relevant persons (teachers as well as students). This solution is designed to include all relevant metadata, such as the curriculum stored in the database, the issuing institution, selected personal details of the examiner and examinee, etc. into transactions on blockchain.

The research that accompanies the demonstrator addresses the following research question:

> Which basic requirements are needed to use blockchain technologies not only for the verification of original documents by using a one-way hash, but to use blockchain directly with assessment instruments in real-time environments, taking technological, social and commercial factors into account?

2 Related Work

The last several years have brought considerable development in the area of blockchain research in the field of digital games, specifically in the field of education. However, there is hardly any or even no publication on serious games in connection with blockchain technologies. Below we look at the most notable working papers and articles that deal with the subject of distributed ledgers and games in the ways that can be applied to gamification of education.

A number of studies focuses on the design challenges of blockchain-based games. Kraft [10] explores the problem of generating fair randomness in a deterministic, multi-agent context (for instance, a decentralized game built on a blockchain). He states that the existing state-of-the art approaches are either susceptible to manipulation if the stakes are high enough or if they are not generally applicable. Therefore he introduces a new approach based on game theory. Min et al. [15] discuss the blockchain integration for games and then categorize existing blockchain games from the aspects of their genres and technical platforms. In practice, Cai et al. [4] develop two different prototypes to research the aspect of multi-chain as well as multi-game approaches with the aim to create an interoperable blockchain gaming framework. Lee et al. [12] examine the effects of speculative and enjoyable aspects of users' playing behavior in blockchain-based collectible games. As collectibles require dedicated marketplaces to circulate, Chen [5] observe blockchain technology as an innovative element of the virtual items trading platform. He concludes that the biggest impact of blockchain technology in the short term is the redistribution and integration of the game and trading platform market.

Gamification of education has a relatively small number of researched blockchain cases. In one of the earliest relevant studies, Jirgensons and Kapenieks [8] compare Blockcerts with Ethereum Smart Contracts developed by Open University, UK, while Baldi et al. [3] describe how to impersonate a legitimate issuer of Blockcerts certificates with the aim to produce certificates that cannot be distinguished from originals by the Blockcerts validation procedure. Setting the groundwork for the project presented in this paper, Pfeiffer and König [16] discuss the use of blockchain technologies in educational games for assessment from a humanities perspective. Komiya et al. [9] examine consensus algorithms as a reward system. They introduce their approach "Proof-of-Achievement (PoA)" which is an algorithm optimized for blockchain games, focusing on the number of tasks achieved in the game. The aim of using the PoA algorithm is to increase the motivation for playing blockchain-based games. Similar to Komiya, Yuen et al. [20] also perceive consensus algorithms like Proof of Work "PoW" as a bottleneck for games. Their proposal is called "Proof-of-Play" with a focus on Peer-to-peer (P2P) Games. Agustin et al. [1] describe application of blockchain technology in e-certificates in the open journal system. The study reports that issuance of e-certificates in an open journal system is a way to manage and verify, prevent duplication or even falsification of e-certificates and the reputation of the open journal system is already given. This project is based on Blockcerts by Learning Machine (originally developed at MIT). Finally, Aini et al. [2] explore different approaches to gamification that embed blockchain technologies in the educational sector.

3 The Context of the Demonstrator

To set up the demonstrator in the educational framework, we developed the educational game Gallery Defender on blockchain. This serious game replays the requirements of art history knowledge in the introductory college level Art History Curriculum Framework:

The learning goal equals the game goal [6] and is defined in the following way.

> All students, which equals the players of the game, will understand, analyze, and describe art styles in their historical, social, and cultural contexts.

Gallery Defender is inspired by the game ARTé: Lumiere [19] already available to students online. In our case, the new serious game introduces art concepts to the player/learner at the first stage and assesses the acquired knowledge of them at the following stage. The results are then transferred to the educational institution.

The game is a turn-based card game that consists of multiple levels. It develops a simple narrative, according to which the player/learner is invited to take the role of a gallery owner. Using their profound knowledge of art history, the player must defend the artworks of the gallery from a masterful thief (Fig. 1).

Each level provides the player/learner with a deck of cards that carry images of historical paintings on them. A small subset of the deck is dealt into the hands of players at the start of each turn. Each card corresponds to the action, which is denoted by a small icon; these actions include the attack icon, represented by a "race car" icon, and defense actions, represented by the "headphones", "helmet", and "building" icons. (These actions were chosen from existing icon assets that the authors already owned, and the icons themselves are not related to learning outcomes.)

The player/learner plays against a simple AI who declares an action at the start of each turn. There is exactly one painting in their hand that corresponds to the AI's declared action at any time, which must be correctly matched to the art movement that it belongs to by dragging the card into one of several labeled buckets near the bottom of the screen.

Fig. 1 Screenshot of gameplay in the first version of the game

After successfully matching some number of artworks (which vary by level), the player/learner can move on to the next level. Incorrectly matching too many artworks to art movements will result in failure of the level. Not all levels contain the same number or types of art movements. Additionally, certain levels may allow the player/learner to click on various buttons to gain more information about artworks, art movements, and their previous moves. The Simulation and Assessment Levels are based on the highest difficulty settings possible.

Following the classification of König [16], Gallery Defender is built on the Game Based Learning and Assessment framework. This means that the content and methods are identical in both learning and assessment mode. However, these areas are strictly separated from each other, and the user learns when they step from one sphere into the other.

Gallery Defender utilizes blockchain technologies in three different ways.

The player/learner receives a digital token at the end of the assessment, which contains the grade, points, and time that the assessment was finished as a message. This token and the attached message are stored forever and unchangeably on the blockchain in the player/learner's Ardor Blockchain Wallet. The certificate is encrypted and can only be decrypted by the sender and the original recipient. However, using a shared key enables the player/learner to share the results with third parties, such as their future boss, their family or another school/university (Fig. 2).

The tokens used in the token system of the demonstrator are defined as utility tokens, minted on the Ignis child chain of the Ardor Network. It is of utmost importance that the tokens cannot be traded or sent outside of the learning/assessment environment to prevent speculative behavior [12].

In addition, the player/learner with particularly good results receives an additional token. This token can be exchanged for digital rewards, e.g. a game poster, which

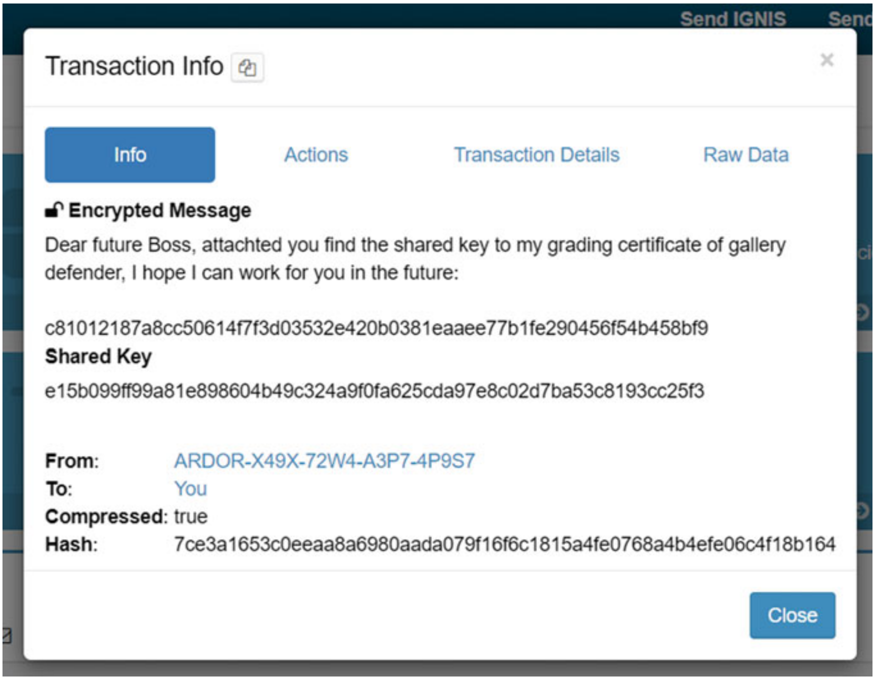

Fig. 2 Screenshot of a message on Ardor blockchain

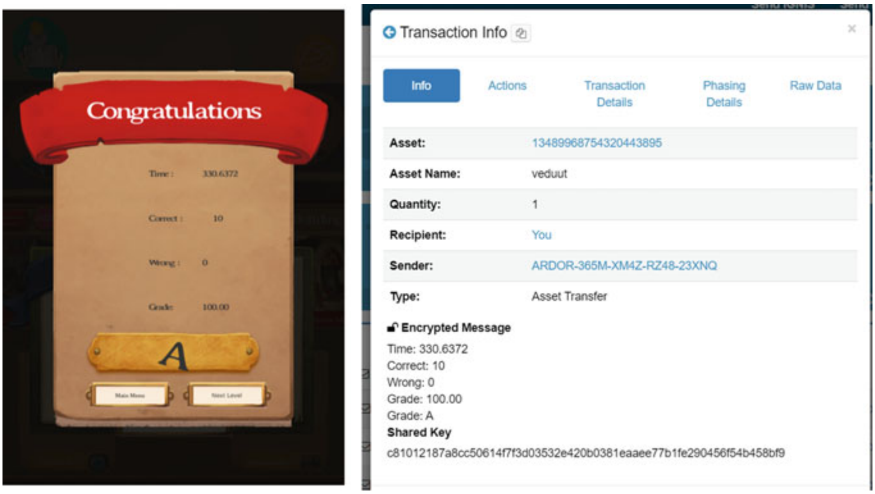

Fig. 3 The grade in the game (on the left) is translated into the exact amount in the blockchain tokens (on the right)

corresponds to the gamification principle realised on blockchain. This functionality can be used to build an entire ecosystem for rewards on blockchain within the context of education, as well as beyond this context.

Finally, the third type of a token is the verification token. Teachers can request this token with further information about the respective test result. After the assessment has been carried out, within a definable time the message is deleted, and only the proof that the token has been sent remains immutable on blockchain (Fig. 3).

4 Methodology

Gallery Defender was created in three iteration steps. The first two iterations took place on the testnet of the system, the third and last iteration was then implemented on the mainnet of the Ardor blockchain. These particular stages were evaluated by using online questionnaires. These questionnaires were filled out at live events such as the Connected Learning Summit, Irvine or the Future and Reality of Gaming Conference, Vienna. Additional participants were recruited, and they received a hyperlink via e-mail to test the demonstrator. The link could be requested using the contact address on the research website of the project. The total number of participants on this survey during the iterative design process was n = 105. The professional background of the survey participants ranges from education and technical professions to people with a background in sociology. This is the case due to the two specific events at which the tests were conducted. A more detailed report on testing has been published [18].

In the first place, testing helped find bugs in the solution. Secondly, new features were suggested by respondents, for example, on how to improve the gaming experience. The focus, however, was on the implementation of blockchain technologies to validate test results from both the socio-economic and technical perspective. For this purpose, open fields could be filled out and therefore both qualitative and quantitative feedback was collected. This was evaluated using the methodology of qualitative content analysis according to Mayring [14] and is discussed in the following section.

5 Results

The results of the content analysis as part of the iterative design process have led to the following guidelines and recommendations.

Either a public blockchain or a combination of private/consortium blockchains should be used in a setting that makes sense and does not limit the reasons why blockchain itself is being used. For instance, in one proposed architecture, personal data is stored using a private blockchain to ensure GDPR compliance. Other highly sensitive data remains in the private area of the respective institution, but the private blockchain sends the hash-value of each block-height to a public blockchain to reduce the possible attack vector for manipulation.

More attention should be paid on the performance of the used networks, regarding number of possible transactions per specified timeframe. In our project, “non freely tradeable utility tokens” are being used (as opposed to fungible and non-fungible freely tradeable tokens). More specifically, the tokens cannot be re-transferred to other users freely, but also, the issuer cannot withdraw them from the user either.

Transaction fees to the network are paid by the respective issuer(s) or operator(s) of the token(s). Therefore the users themselves do not need to hold any “tradeable network maintenance utility tokens”, or “cryptocurrencies”, nor do they need to know about blockchain. For users the experience should equate to simply using an app. More advanced users can always track their transactions using a public available blockchain tracker or their very own node.

It is possible to encrypt the message associated with the token, so only the transaction itself is publicly visible, while the private information remains private and only accessible to those parties who should have access to it (for the relevant period).

To achieve this shared-keys (or even sub-shared keys, making information available for a specific timeframe or for dedicated users) can be generated, and thus a sharing system for third parties who get access to the information attached to the token can be developed (but not the token itself as information bearer).

The message containing the core content, in certain cases where it makes sense, can be deleted from the blockchain after some time (with the knowledge of the partners involved). Only the proof of the transaction itself remains to reduce the blockchain bloat.

Users can, if they want, always operate a full node and this with existing devices such as their own modern smartphone, their own PC or with inexpensive hardware such as a Raspberry Pi.

The Full Node can be operated without holding network maintenance tokens or cryptocurrencies with the option to run a copy of the blockchain and look into it.

Holding “tradeable network maintenance utility tokens”, or “cryptocurrencies” is only necessary if the users want to be part of the active network and conduct mining/forging.

The availability of digital qualified signatures, or other secure forms of digital and forgery-proof identity verification, like an advanced Self-Sovereign Identity System.

A blockchain wallet needs to be created, similar to well-known solutions like the “Exodus Wallet”, which can hold different tokens, issued on various systems. However, instead of holding “cryptocurrencies” this time it is a utility token as information carrier.

Further education on the topic of blockchain is needed, if private individuals and companies operate directly with private keys, generated when they open a respective blockchain wallet.

Assuming that the time is not yet there in regards to trusting users to handle a unique key that cannot be restored if lost, it can be defined that the private key itself is only known to application utilizing blockchain to secure certain data, while setting up a classic user and password system which starts the blockchain operations.

Finally, we strongly encourage the designers and adopters of such systems to ‘think green’: opt-in for solutions that are safe but environmentally friendly. This is especially important for use cases like storing educational data from a game, which do not store monetary records. Therefore, we call for evaluation of a consensus algorithm that fits best for the purpose intended.

6 Conclusion

From these key findings, the following questions can be identified, which researchers, developers and users of systems and applications using blockchain technologies should ask themselves.

- Is a private or public blockchain used?
- Which Blockchain or combination of blockchains systems is used?
- Can the information-carrying tokens be sent from one account to another without this being originally intended?
- Is the private information of the token sufficiently encrypted? And if so, who has the keys to access the data?
- Can (temporary) shared-keys be created that give access to (specific) information for third parties?
- Is it possible for companies, universities and government institutions to operate their own nodes in the network and thus have data sovereignty? If so, how much effort and costs are involved?
- Is it even possible for users to run their own node? And if so, with what effort and costs?
- Do the partners involved have to purchase cryptocurrencies? If so, for what purposes and from which sources? And subsequently, do the users have to purchase cryptocurrencies?
- Who pays the transaction fees to the network? Can the solutions be used that do not charge transaction fees? If this is the case—which network was used and what are the effects of using a transaction fee-free solution?
- Who creates the required blockchain wallets—partners of the respective project or users themselves? Can this be done for them in an automated manner “through the app”? If the latter, who and in what form has control over the private keys?

Although blockchain technologies are constantly evolving from a technological perspective and a lot has been achieved since Grech and Camilleri’s report [7], blockchain technologies have not yet arrived at the mainstream areas of application. We could observe this during the content analysis stage of our research: those survey participants who linked blockchain to speculative hype expressed critical opinions on the topic. The second aspect that could be read out of the survey was that there are many blockchain developers and scientists who are fixated on a specific system and do not want to look at other systems or multi-chain solutions.

Therefore, there is still a lot of educational work to be done. One can hope that in the next few years a lot of applied research will be conducted, which will also reach the end users and thus communicate the topic hands-on. A very important finding of the project was also that the demonstrator and the testing together with the proponents, which had little contact with the matter, the active testing helped them to better understand blockchain, as they stated in the follow-up discussions.

7 Future Research

Three aspects will be addressed in the follow-up to the research project presented above.

- Ethical integration of the blockchain solution with digital identity systems.
- Solutions for management of private or shared keys, so that the system is secure but also understandable for its users.
- Further development of interfaces between different parts of the system, so that a wallet can read information from different tokens, and the learning or assessment software can transfer the results to different agents as it is appropriate for the user or the institution.

Acknowledgements The authors express gratitude to Michael Black, Lloyd Donelan and Nick Muniz for their work on the game, to Alexiei Dingli, Vince Vella and Thomas Wernbacher for their invaluable support and guidance, and to Alesha Serada for their editing work and support.

References

1. Agustin, F., Aini, Q., Khoirunisa, A., Nabila, E.A.: Utilization of blockchain technology for management E-certificate open journal system. APTISI Trans. Manag. (ATM) **4**(2), 134–139 (2020). https://doi.org/10.33050/atm.v4i2.1293
2. Aini, Q., Rahardja, U., Khoirunisa, A.: Blockchain technology into gamification on education. Indones. J. Comput. Cybern. Syst. (IJCCS) **14**(2), 147–158 (2020). https://doi.org/10.22146/ijccs.53221
3. Baldi, M., Chiaraluce, F., Kodra, M., Spalazzi, L.: Security analysis of a blockchain-based protocol for the certification of academic credentials. arXiv:1910.04622 (2019). http://arxiv.org/abs/1910.04622
4. Cai, W., Wu, X.: Demo abstract: an interoperable avatar framework across multiple games and blockchains. In: IEEE INFOCOM 2019—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 967–968 (2019). https://doi.org/10.1109/INFCOMW.2019.8845288
5. Chen, J.T.: Blockchain and the feature of game development. In: Frontier Computing: Theory, Technologies and Applications (FC 2019). Lecture Notes in Electrical Engineering, pp. 1797–1802. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3250-4. https://www.springer.com/gp/book/9789811532498
6. Gee, J.P.: What Video Games Have to Teach Us About Learning and Literacy, 2nd edn. Macmillan (2014). Google-Books-ID: v_XIBAAAQBAJ
7. Grech, A., Camilleri, A.F., Inamorato dos Santos, A.: Blockchain in education. Tech. Rep. Publications Office of the European Union (2017)

8. Jirgensons, M., Kapenieks, J.: Blockchain and the future of digital learning credential assessment and management. J. Teach. Educ. Sustain. **20**(1), 145–156 (2018). https://doi.org/10.2478/jtes-2018-0009
9. Komiya, K., Nakajima, T.: Increasing motivation for playing blockchain games using proof-of-achievement algorithm. In: Fang, X. (ed.) HCI in Games. Lecture Notes in Computer Science, pp. 125–140. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-22602-2_11
10. Kraft, D.: Game-theoretic randomness for blockchain games. arXiv: 1901.06285 (2019). http://arxiv.org/abs/1901.06285
11. Lapointe, C., Fishbane, L.: The blockchain ethical design framework. Innov. Technol. Gov. Glob. **12**(3–4), 50–71 (2019). https://doi.org/10.1162/inov_a_00275
12. Lee, J., Yoo, B., Jang, M.: Is a blockchain-based game a game for fun, or is it a tool for speculation? An empirical analysis of player behavior in crypokitties. In: The Ecosystem of e-Business: Technologies, Stakeholders, and Connections. Lecture Notes in Business Information Processing, vol. 357, pp. 141–148. Springer (2019)
13. Liddell, F.: Building shared guardianship through blockchain technology and digital museum objects. Mus. Soc. **19**(2), 220–236 (2021). https://doi.org/10.29311/mas.v19i2.3495
14. Mayring, P.: Qualitative Inhaltsanalyse. In: Handbuch Qualitative Forschung in der Psychologie: Band 2: Designs und Verfahren, pp. 495–511. Springer Fachmedien, Wiesbaden (2020). https://doi.org/10.1007/978-3-658-26887-9_52
15. Min, T., Wang, H., Guo, Y., Cai, W.: Blockchain games: a survey. In: 2019 IEEE Conference on Games (CoG), pp. 1–8 (2019). https://doi.org/10.1109/CIG.2019.8848111
16. Pfeiffer, A., Koenig, N.: Blockchain technologies and their impact on game-based education and learning assessment. In: Savegame. Perspektiven der Game Studies, pp. 55–67. Springer VS, Wiesbaden (2019). https://doi.org/10.1007/978-3-658-27395-8_5
17. Scherling, L.S.: Blockchain technologies in community-based arts: implications for fair use and changing practices in art education. Tech. Rep. Columbia University (2017)
18. Thomas, A., Koenig, N., Higgins, T., Black, M., Pfeiffer, A., Donelan, L., Lenzen, B., Muniz, N., Patel, K., Taylan, A., Wernbacher, T.: From learning to assessment, how to utilize Blockchain technologies in gaming environments to secure learning outcomes and test results. MCAST J. Appl. Res. Pract. **3**(2), 172 (2019)
19. Thomas, A., Ramadan, H., Campana, L., Leiderman, D., Sutherland, S., Zawadzki, M.: ARTé: Lumiere (2018). Available electronically at https://oaktrust.library.tamu.edu/handle/1969.1/188003
20. Yuen, H.Y., Wu, F., Cai, W., Chan, H.C., Yan, Q., Leung, V.C.: Proof-of-play: a novel consensus model for blockchain-based peer-to-peer gaming system. In: Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, BSCI '19, pp. 19–28. Association for Computing Machinery, New York, NY (2019). https://doi.org/10.1145/3327960.3332386