



Block the Chain: Software Weapons of Fighting Against COVID-19

Attila Kertesz, University of Szeged

This article proposes an architecture for vaccination information validation and tracking with a fog and cloud-based blockchain system, providing a privacy-aware and scalable approach for interoperable and effective data management. It evaluates the scalability of the underlying blockchain system by means of simulation.

Responding to the COVID-19 pandemic, smart applications¹ have begun to be developed for the prevention of virus spreading and the management of related societal problems, such as travel restrictions. The vast majority of these applications are centralized and nonsmart, which makes them carry single-point-of-failure, privacy, high-latency, and legal issues along with a lack of efficient handling of mobile devices.² Additionally, challenges in real-life

scenarios include different health-care institutions, various stakeholders within the supply chain, heterogeneous networks, and multicultural and highly distributed and dynamic system entities.³

There is a wide range of smart applications running in smart systems exploiting intelligent capabilities, relying on cloud, fog, and edge services.⁴ Those related to COVID include contact tracing (for example, VirusRadar, Stopp Corona, and StopCOVID) and social distancing applications⁵ to monitor and contribute to slowing the virus's spread and the number of infections. After the successful development and testing of COVID-19 vaccines, another

Digital Object Identifier 10.1109/MC.2022.3147368
Date of current version: 18 July 2022

This work is licensed under a
Creative Commons Attribution 4.0 License. For more information,
see <https://creativecommons.org/licenses/by/4.0/deed.ast>.

group of applications has arisen for managing immunity passports and vaccination certificates (for instance, International Air Travel Association Travel Pass and CommonPass). The adoption and mass acceptance of COVID-19-related applications are greatly hindered by a general lack of trust in the nature of tracing apps and the reluctance of people to share their personal data. To overcome this issue, we need to revise current solutions and design methods addressing privacy awareness and preservation, trust, explainability, and interoperability.⁷

Blockchain (BC)⁶ is a form of distributed ledger technology for applications such as digital cryptocurrencies and digital smart contracts. Solutions integrated with BCs provide high levels of security and trust and guarantee a fully immutable transactional history without the control of a central authority. BC applications have been proposed in various fields, from e-health to the Internet of Vehicles. The author believes that integrating BC technology with fog computing (FC) to serve smart applications to manage mobile device data can enhance the privacy and security of current systems.⁸ This article envisions a solution for gathering, storing, validating, and analyzing COVID-19-related data, including infections and vaccinations among citizens of a region. To realize such a system, emerging technologies are needed. This proposal builds on BC technology to provide trust and transparency and on FC to support local, private data management and low-latency access to the system.

The main contribution of this article is the general architecture for vaccination information validation and tracking with a fog- and cloud-based BC system (VACFOB). This approach merges FC and BC technologies to provide a

privacy-aware, scalable, and interoperable solution for effective vaccination information management. The article derives three scenarios from real-world vaccination reports and uses their requirements to evaluate the scalability of various BC systems with the Fog-Blockchain simulation environment (FoBSim) tool.¹⁵ The results can serve as recommendations for possible implementations of the proposal, which could contribute to a better and more efficient fight against COVID-19. The following sections gather and compare related works, then present a proposal for a unified, BC-based solution to fight COVID-19 and future pandemics.

RELATED WORK

Applying BC technology to health care has been studied by Kshetri.⁹ That work argues that such integration can improve accountability and data exchanges. Nevertheless, the management of detailed patient health records results in additional privacy issues. This article refrains from addressing management issues surrounding general health-care records and focuses on COVID-related information.

Concerning the state of the art for utilizing FC and BCs to address challenges related to the COVID-19 pandemic, there are some related approaches. A privacy-preserving mobile and fog computing framework¹⁰ is an e-government application framework for tracing COVID-19 community transmission by utilizing mobile computing and FC. The authors of this solution aimed to enhance privacy and trust by enabling user control with minimal data collection, data destruction at will, and transparency through open source codes. BeepTrace¹¹ is a solution for BC-enabled, privacy-preserving COVID-19 contact tracing. It stores user pseudonyms with

a coupled geodata cypher to track locations. Its authors argued that publicly sharing user pseudonyms generated by private keys are safe. They showed that BeepTrace overcomes earlier related solutions by using multiple positioning technologies with high security requirements. Dai et al.¹² proposed an approach for using a BC-enabled Internet of Medical Things (IoMT). They claimed that the IoMT can contribute to origin tracing and more efficient social distancing and quarantine management. In their work, they stated the requirements (smart hospitals, data provenance, and remote health care) for privacy-aware BC-based IoMT solutions. As open issues, they named BC scalability and trustworthy artificial intelligence.

Biometric and identity management companies, such as SCIPA, Mvine, and iProov, announced trials of their COVID-19 immunity and vaccination passports at the beginning of 2021. Meanwhile, European national efforts have been reported by the European Commission regarding mobile contact tracing apps,¹ and a European Union Digital COVID Certificate (EUDCC) initiative has been launched.¹³ A centralized EUDCC gateway will be used to verify certificate signatures, and both the issuer and the certificates will have digital signatures, and their data will be stored in the corresponding countries. The EUDCC seems to be a good approach, but it enables only COVID-19 vaccination information verification. It is also a good step toward standardization, but interoperability with non-EU countries has not been achieved.

The author believes that citizen trust and privacy could be further enhanced with fog and BC integration, although additional features would be needed to enable patient health tracking, pandemic monitoring, and increasing

prevention through data analysis. In summary, BeepTrace¹¹ represented a good step forward in exploiting BCs for fighting COVID-19, but it is specialized only for contact tracing. The current situation suggests that testing and vaccination information, as well as vaccination reliability, will be crucial pieces of information to handle. They could be used to predict virus spreading and trigger regional safety precautions. This article's proposal follows the latest trends in fog and BC utilization, but it shifts the focus from individual tracing to community-based verification.

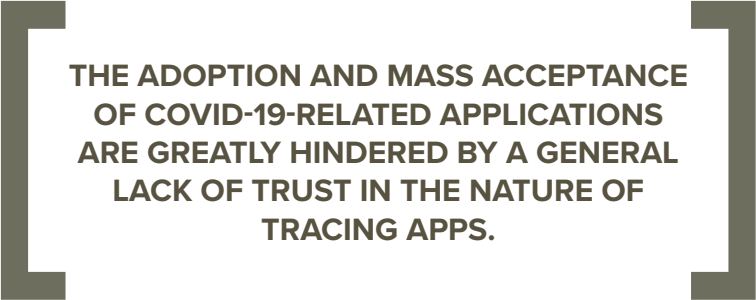
THE PROPOSED SOLUTION

Contact tracing seems to be less important since there are many vaccines available worldwide. To reestablish economic processes, going back to traditional work environments, ensuring safe business trips, and boosting tourism are the next steps. To this end, we need unified, privacy-aware, and scalable vaccination information and certificate management. Besides, what we still do not know and will be crucial is the effectiveness of the vaccines. This article's approach could provide means to support both of these directions by using BC and FC technologies.

The architecture of the VACFOB solution is provided in Figure 1. The utilized BC infrastructure is installed in the fog and possibly backed up at the cloud layer. Fog nodes can host one or more miners and serve several COVID-related information providers close to them. There are four different end user types (see the end user layer in Figure 1): 1) issuing bodies, which can provide vaccination certificates for citizens of a country; 2) hospitals and private testing centers that are allowed (certified) to perform testing and report the health status of citizens; 3) border control officers and other legal

parties that have to verify vaccinations; and 4) anyone who wishes to make public queries for analyzing the spread of a virus. Means for the fourth type may depend on the kind of BC infrastructure that is utilized. In the first three cases, citizens should identify themselves, and the corresponding issuing and reporting bodies need to retrieve the ID hash and append the status change for a BC transaction or query. In these processes, the required private data are stored in

In case we would like to restrict access to the system, we may close verification for the public and allow only specific bodies to perform queries, so the ID hash would not be shared with citizens and others through them. To this end, a trusted third party can be introduced and placed in a central cloud to govern BC participation. In this case, digitally signing a document is not necessary; any pseudonymized identifier in the form of a hash can be



**THE ADOPTION AND MASS ACCEPTANCE
OF COVID-19-RELATED APPLICATIONS
ARE GREATLY HINDERED BY A GENERAL
LACK OF TRUST IN THE NATURE OF
TRACING APPS.**

a secure, centralized government database (that is, off chain).

In case we consider vaccination verification as the sole role of the system, a public-permissioned BC would be suitable to enable anyone to validate the vaccination of a citizen. To guard privacy and comply with Europe's General Data Protection Regulation (GDPR), the issuing body should sign a vaccination or testing document with its digital certificate (stored off chain). In this way, any validator (who wishes to confirm a citizen vaccination) can perform a verification on the data queried from the BC. Border control agencies perform this action in Figure 1. An extracted citizen ID will be the ID hash stored in a block and considered personal data. Therefore, user consent and management need to be ensured by participating bodies (having permission to save new blocks).¹⁴

generated for all citizens (during their first registration) and stored within the local, private off-chain database together with other related personal and health data. From now on, the article considers this case and supposes that only a certified body (permissioned) can get a citizen ID hash from government and regional databases, so not everybody can verify vaccination. Nevertheless, by allowing public queries for pseudonymized information, the system can support the gathering of statistics and making of predictions, for example, about virus spreading and immunity rates.

To enable vaccination verification, every transaction should contain the following properties (as shown in Figure 1): 1) a digitally signed document extract or pseudonymized identifier of a citizen (ID hash), 2) an actual

status change (for example, getting vaccinated or recovering/receiving a negative test result), and 3) a time stamp and location information (the exact date and city). Note that this

solution does not restrict the system's use to COVID-19; VACFOB can be used to handle other types of viruses/vaccinations (such as Severe Acute Respiratory Syndrome, Middle East

Respiratory Syndrome, and flu variants). In the border control use case (as shown at the bottom right of Figure 1), an officer checks the personal ID of a citizen. He or she enters the ID into the

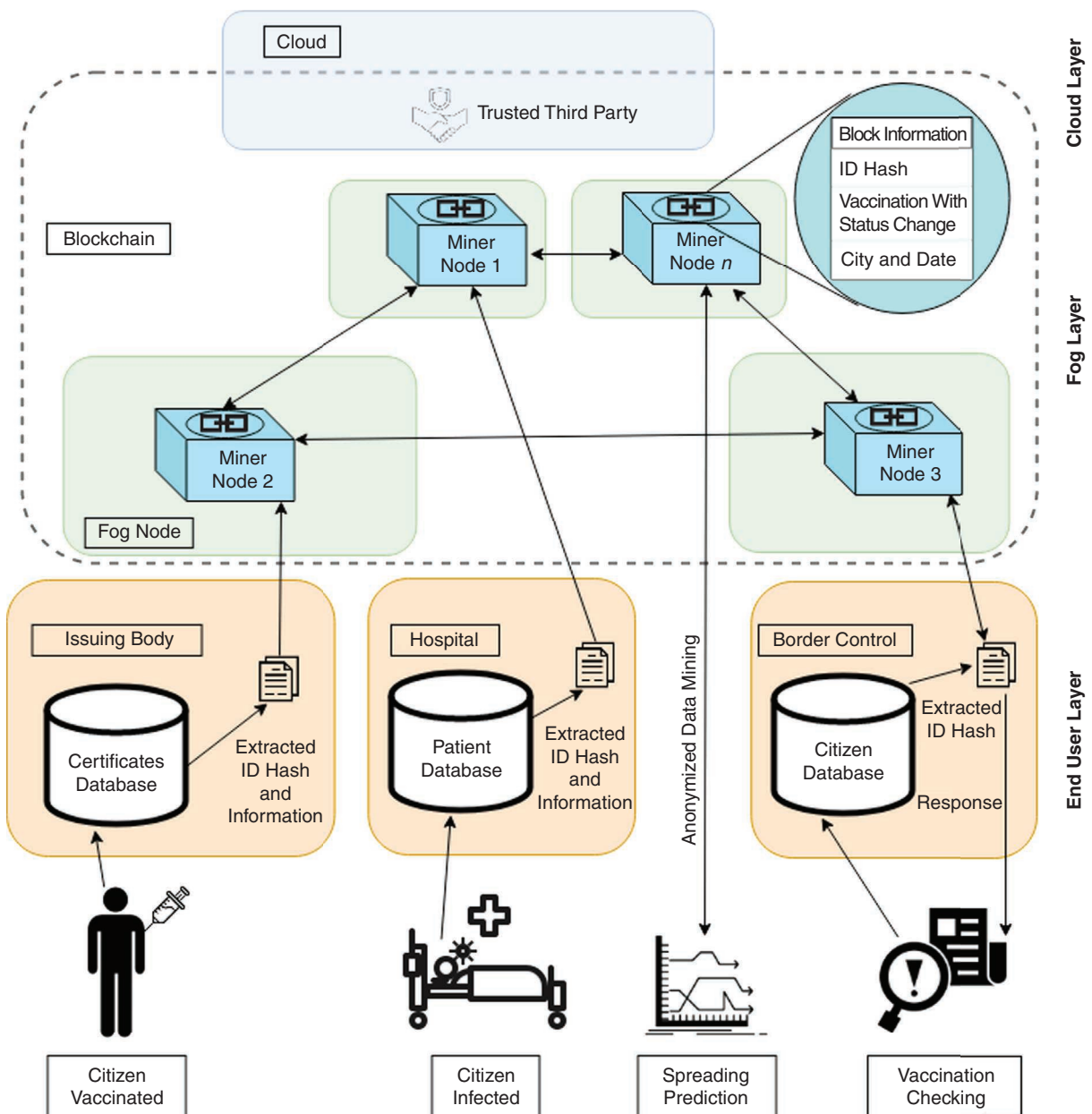


FIGURE 1. The proposed VACFOB architecture for COVID-19 vaccination verification and immunity analysis.

local government database to retrieve the corresponding hash ID, which should be used to make a query (look up a transaction) in the BC. If a transaction block is found with the ID hash containing vaccination information with a time stamp within the accepted range (for example, six months), the citizen can pass without having to quarantine.

With these system properties, the following types of queries could be performed:

- › vaccination validation
- › determining the number of active, infected people for a region (with a virus or disease type)
- › obtaining the infection, testing, and vaccination history of citizens; from these data, an end user can predict or estimate virus spreading, vaccine efficiency, and immunity levels for a region.

The VACFOB architecture and its operational methods bring novelty to applying BC and fog integration for vaccination verification, immunity success rate, and virus spreading analysis by enabling a high level of trust and privacy. The system is modular, extendable, and scalable: the number of fog nodes and the type and size of the BC infrastructure can be changed. In the end user layer, additional parties can be defined to enable optimized query management and specific mathematical models and algorithms for additional data analysis. As future work, possible integration options may be investigated (for example, with BeepTrace) to enable contact tracing, as well. Of note, the proposal can be used to handle future COVID variants, and it is able to store and manage different seasonal diseases, such as the ones caused by influenza. This contributes to the sustainability of the approach.

VALIDATION

A concrete implementation of the proposal could be analyzed and evaluated according to different metrics, such as security and privacy, scalability, and operation cost. Concerning privacy awareness, the proposal is GDPR compliant, and by utilizing the fog layer, its resources provide faster response times and better scalability compared to a purely cloud setup. This section demonstrates the scalability of the utilized BC infrastructure in the fog. Since VACFOB is a model in its current state, suitable BC settings that can serve its needs are sought. The exact performance values of a future implementation will depend on the actual BC implementation. Therefore, the article defines three scenarios based on real-world data with different scalability needs. An earlier work developed a BC simulation tool, FoBSim.¹⁵ It can be used to investigate the behavior of a BC system by employing different parameters and consensus algorithms; hence, it will be employed for this evaluation.

FoBSim facilitates investigating BC systems through three default consensus algorithms: proof of authority (PoA), proof of stake (PoS), and proof of work (PoW) (see Baniata and Kertesz¹⁵ for

definitions and implementation details). In a nationwide scenario, every BC miner in the fog can serve one or more end user nodes that handle requests from certain bodies (concerning vaccination certificate issuing, updates, health changes, and information requests). The experiments here rely on information shared by OurWorldInData.org,¹⁶ which provides statistics for the past year about the COVID pandemic for more than 200 countries. To estimate the number of daily transactions for a region for the proposed system, it is possible to gather information about daily performed vaccinations, new confirmed cases, and performed tests, as shown in Table 1 for two randomly selected dates. From these data, it is evident that for a small country, such as Hungary, there are around 10,000–200,000 daily transactions (status updates for citizens). For a large country, such as Germany, there are 1–3 million daily transactions, while for Europe and the United States, there may be up to 5 million.

Based on this information, we investigate BC systems that could be used for VACFOB implementations to serve different regions, employing the following scenarios with detailed parameter settings in FoBSim:

TABLE 1. The 2021 daily COVID-19 information (from Ritchie et al.¹⁶).

Date	Type	Hungary	Germany	EU	United States
1 February	Vaccinated	12,524	120,632	893,846	1.1 million
1 February	Cases	1,124	6,668	170,705	134,975
1 February	Tests	10,862	N/A	N/A	1.03 million
1 April	Vaccinated	166,720	324,913	3.21 million	3.36 million
1 April	Cases	9,288	22,679	251,149	79,115
1 April	Tests	40,444	N/A	N/A	1.44 million

- › **Scenario 1:** There are 100,000 daily transactions for COVID-19 status updates for citizens.
- › **Scenario 2:** There are 1 million daily transactions for COVID-19 status updates for citizens.
- › **Scenario 3:** There are 10 million daily transactions for COVID-19 status updates for citizens.

We assume that transactions are performed during working hours (for example, eight hours per day), so we can roughly estimate up to five transactions per second (TPS) for scenario 1, up to 50 TPS for scenario 2, and up to 500 TPS for scenario 3. A concrete BC infrastructure can be characterized by the number of fog nodes and miners in the system; the maintained block size, which is proportional to

a preset number of transactions per block (TPB); and the applied consensus algorithm. By investigating different parameter settings, we can analyze how to meet the required TPS values.

The FoBSim simulation experiments (see Table 2) using the PoA and PoS consensus algorithms were locally performed on an Intel i5-8265U CPU (eight cores, 3.8 GHz, and 12 GB of memory) running Windows 10. The PoW experiments were conducted on an HP Synergy 480 Gen10 server node with two Intel Xeon Gold 5118 CPUs (2.3 GHz and 12 cores each) and 384 GB of memory, running Ubuntu 20.10. The number of transactions to be processed in all simulation runs was fixed at 10,000. Each simulation was performed five times, taking the average TPS value, as the individual ones marginally fluctuated.

By determining the parameters to investigate certain BC infrastructures, we made the following restrictions. We varied the number of fog nodes and miners from 10 to 100 and the number of miner neighbors from two to 10. Concerning the block size in the BC system, Ethereum stores around 70 TPB, while Bitcoin stores roughly 2,000 TPB, on average; therefore, we decided to use 100- and 1,000-TPB values for the experiments. To set the delay between neighbors in the fog layer, we used the WonderNetwork (<https://wondernetwork.com/pings>) service. We counted network latency between big cities corresponding to the scenarios defined before [Hungary: Vienna, Austria–Budapest, Hungary (7.4 ms); Germany: Munich–Amsterdam, The Netherlands (15.2 ms); and Europe: Warsaw, Poland–Porto, Portugal (63.4 ms)].

TABLE 2. The selected performance results with FoBSim.

Simulation	Parameter settings						Results	
	Number of fog nodes	Number of miners	Neighbors per miner	Block size (TPB)	Delay between neighbors (ms)	Consensus algorithm	TPS	Target
9	10	10	2	100	15.2	PoA	238	✓
10	50	50	6	100	15.2	PoA	46	✗
17	10	10	2	100	63.4	PoA	129	✗
21	10	10	2	1,000	63.4	PoA	1,205	✓
1	10	10	2	100	15.2	PoS	206	✓
8	50	50	6	100	15.2	PoS	28	✗
16	10	10	2	1,000	63.4	PoS	860	✓
17	50	50	6	1,000	63.4	PoS	173	✗
1	100	100	10	100	63.4	PoW-10	263	✗
2	100	100	10	1,000	63.4	PoW-10	1,025	✓
3	100	100	10	100	63.4	PoW-15	246	✗
4	100	100	10	1,000	63.4	PoW-15	599	✓

TABLE 3. The BC system analysis performance results with FoBSim using the PoA consensus algorithm.

Simulation	Parameter settings						Results	
	Number of fog nodes	Number of miners	Neighbors per miner	Block size (TPB)	Delay between neighbors (ms)	Consensus algorithm	TPS	Target
1	10	10	2	100	7.4	PoA	333	✓
2	50	50	6	100	7.4	PoA	52	✓
3	50	100	10	100	7.4	PoA	19	✓
4	100	100	10	100	7.4	PoA	20	✓
5	10	10	2	1,000	7.4	PoA	2,976	✓
6	50	50	6	1,000	7.4	PoA	555	✓
7	50	100	10	1,000	7.4	PoA	263	✓
8	100	100	10	1,000	7.4	PoA	232	✓
9	10	10	2	100	15.2	PoA	238	✓
10	50	50	6	100	15.2	PoA	46	✗
11	50	100	10	100	15.2	PoA	19	✗
12	100	100	10	100	15.2	PoA	18	✗
13	10	10	2	1,000	15.2	PoA	1,957	✓
14	50	50	6	1,000	15.2	PoA	463	✓
15	50	100	10	1,000	15.2	PoA	202	✓
16	100	100	10	1,000	15.2	PoA	198	✓
17	10	10	2	100	63.4	PoA	129	✗
18	50	50	6	100	63.4	PoA	28	✗
19	50	100	10	100	63.4	PoA	13	✗
20	100	100	10	100	63.4	PoA	13	✗
21	10	10	2	1,000	63.4	PoA	1,205	✓
22	50	50	6	1,000	63.4	PoA	283	✗
23	50	100	10	1,000	63.4	PoA	131	✗
24	100	100	10	1,000	63.4	PoA	132	✗

TABLE 4. The BC system analysis performance results with FoBSim using the PoS consensus algorithm.

Simulation	Parameter settings						Results	
	Number of fog nodes	Number of miners	Neighbors per miner	Block size (TPB)	Delay between neighbors	Consensus algorithm	TPS	Target
1	10	10	2	100	7.4	PoS	206	✓
2	50	50	6	100	7.4	PoS	32	✓
3	100	100	10	100	7.4	PoS	12	✓
4	10	10	2	1,000	7.4	PoS	1,805	✓
5	50	50	6	1,000	7.4	PoS	340	✓
6	100	100	10	1,000	7.4	PoS	136	✓
7	10	10	2	100	15.2	PoS	206	✓
8	50	50	6	100	15.2	PoS	28	✗
9	100	100	10	100	15.2	PoS	11	✗
10	10	10	2	1,000	15.2	PoS	1,550	✓
11	50	50	6	1,000	15.2	PoS	298	✓
12	100	100	10	1,000	15.2	PoS	123	✓
13	10	10	2	100	63.4	PoS	98	✗
14	50	50	6	100	63.4	PoS	18	✗
15	100	100	10	100	63.4	PoS	7	✗
16	10	10	2	1,000	63.4	PoS	860	✓
17	50	50	6	1,000	63.4	PoS	173	✗
18	100	100	10	1,000	63.4	PoS	78	✗

TABLE 5. The BC system analysis performance results with FoBSim using the PoW consensus algorithm.

Simulation	Parameter settings						Results	
	Number of fog nodes	Number of miners	Neighbors per minute	Block size (TPB)	Delay between neighbors	Consensus algorithm	TPS	Target
1	100	100	10	100	63.4	PoW-10	263	✗
2	100	100	10	1,000	63.4	PoW-10	1,025	✓
3	100	100	10	100	63.4	PoW-15	246	✗
4	100	100	10	1,000	63.4	PoW-15	599	✓
5	100	100	10	100	63.4	PoW-20	24	✗
6	100	100	10	1,000	63.4	PoW-20	84	✗

For simplicity, we kept these numbers constant, even for a higher number of fog nodes.

Concerning the settings of the consensus algorithms, we varied the difficulty of the puzzle during the PoW-based BC simulation runs by changing the hardness level from 10 to 20. This value basically represents the number of zeros at the beginning of the hashes to be minted (see Baniata and Kertesz¹⁵ for details). During runs when the PoA was used, we fixed the number of authorized miners to 3/5 (three authorized out of a total of five miners). The measured TPS values are shown in the eighth column of the tables, while the ninth column indicates whether an experiment met the required target threshold.

First, we performed simulations with the PoA algorithm, then with the PoS algorithm, and finally, with the PoW algorithm. The detailed evaluation results are available in in Tables 3, 4, and 5, respectively. The scenarios were covered by simulation runs composed of three groups. For example, in Table 3, simulations 1–8 aimed to cover the needs of scenario 1 (with a 5-TPS target value), simulations 9–16 covered scenario 2 (with 50 TPS), and simulations 17–21 covered scenario 3 (with 500 TPS). Selected evaluation results are summarized in Table 2. From it, we can see that by using PoA, simulations 10 and 17 failed to provide the required TPS values, while simulations 9 and 21 succeeded. The experiments showed that varying the number of miners per fog node (one or two) did not make any difference. Therefore, this distinction was skipped in the remaining experiments. By using the PoS, simulations 1 and 16 managed to meet the target TPS, but simulations 8 and 17 resulted in failure. Compared to the PoA algorithm, it

is evident that a BC using the PoS can perform up to 50% fewer transactions within the same time frame.

Since simulations with the PoW are generally compute intensive, only the largest parameter settings of scenario 3 were selected for evaluation in the third set of experiments. To perform these, we used an HP Synergy 480 Gen10 server node with 24 CPU cores.

The results show that simulations 2 and 4 produced successful outcomes for the target TPS. Finally, we compare the performance of the utilized consensus algorithms. Figure 2 depicts the differences between the PoA and PoS for the same parameter settings in experiments for scenario 2. In these cases, the PoS provided 37% better results, on average. Figure 3 compares

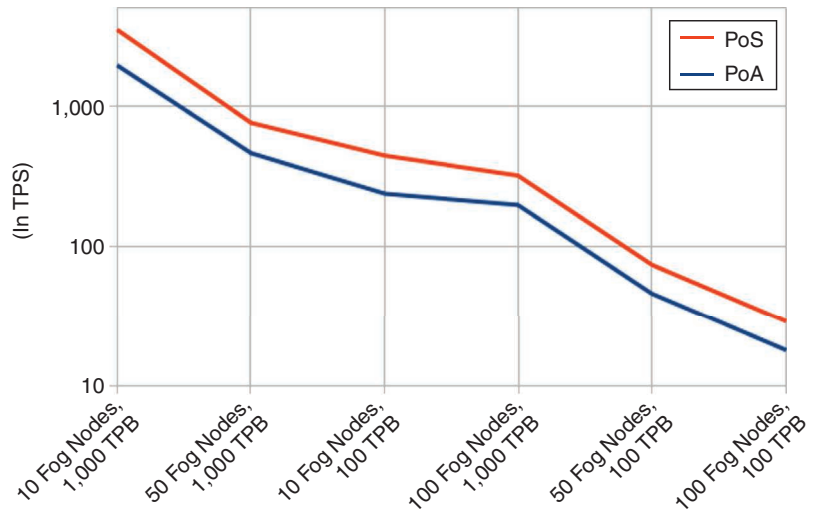


FIGURE 2. The comparison of different consensus algorithms for scenario 2.

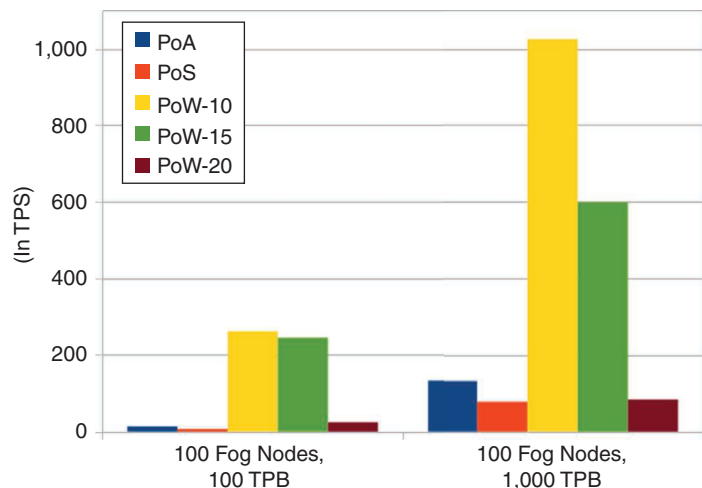


FIGURE 3. The comparison of different consensus algorithms for scenario 3.


ABOUT THE AUTHOR

ATTILA KERTESZ is an associate professor in the Department of Software Engineering, University of Szeged, Szeged, 6720, Hungary, where he leads the IoTCloud research group. His research interests include the federative management of Blockchain, the Internet of Things, fog and cloud systems, and interoperability issues of distributed systems in general. Kertesz received a Ph.D. from the Doctoral School of Computer Science, University of Szeged. Contact him at keratt@inf.u-szeged.hu.

the performance of BCs using different consensus algorithms for scenario 3. It is clear that the PoW with difficulty levels 10 and 15 can provide the best performance for the applied settings and requirements, but these variants can meet the target TPS only when 1,000 TPB are applied.

In summary, determining the number of fog nodes and TPB to be stored in the BC is crucial. For smaller-scale systems (for example, in scenario 1), it is possible to keep these numbers low, but to cover a larger region, the number of fog nodes must inevitably be scaled up, which implies that the TPB value needs to be raised, as well, to have the necessary performance. This systematic evaluation can provide a general overview of the behavior of BC-based systems, and in case of a possible implementation of the VACFOB proposal, it can serve as a guideline to ease parameter selection.

The COVID-19 pandemic has spread around the world, changing everybody's lives. Various smart applications have been developed in the past year for preventing virus spreading, but their widespread use is hindered by a lack of trust. This article proposed VACFOB, which utilizes FC and BC technologies to

provide privacy-aware, scalable, and interoperable vaccination information management. It analyzed real-world vaccination reports and derived three scenarios as requirements, for which the performance of various BC infrastructures was analyzed by means of simulation. The results can serve as recommendations for possible implementations of VACFOB in the near future. 

ACKNOWLEDGMENTS

The research leading to these results has received funding from the Trusted and reliable content on future blockchains (TruBlo) project of the European Union's Horizon 2020 research and innovation program, under grant 957228, and from the national project TKP2021-NVA-09, implemented with support provided by the Ministry of Innovation and Technology of Hungary, from the National Research, Development, and Innovation Fund, and from the University of Szeged Open Access Fund under grant 5612. We also thank Hamza Baniata for his support in discussions and performing simulations with FoBSim.

REFERENCES

1. "Mobile contact tracing apps in EU member states," European Commission, Brussels, Belgium. [Online].

Available: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (Accessed: May 22, 2021).

2. A. L. Phelan, "COVID-19 immunity passports and vaccination certificates: Scientific, equitable, and legal challenges," *Lancet*, vol. 395, no. 10237, pp. 1595–1598, 2020, doi: 10.1016/S0140-6736(20)31034-5.
3. P. K. Lahiri, R. Mandal, S. Banerjee, and U. Biswas, "An approach towards developments of smart COVID-19 patient's management and triaging using blockchain framework," *Res. Square*, pp. 1–18, Sep. 9, 2020, doi: 10.21203/rs.3.rs-70583/v1.
4. S. Varadi, G. Gultekin Varkonyi, and A. Kertesz, "Legal issues of social IoT services: The effects of using clouds, fogs and AI," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications. Studies in Computational Intelligence*, vol. 846, A. Hassanien, R. Bhatnagar, N. Khalifa, and M. Taha, Eds. Cham: Springer Nature Switzerland AG, 2020, pp. 123–138.
5. P. Barsocchi et al., "COVID-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing," *Array*, vol. 9, p. 100,051, Mar. 2021, doi: 10.1016/j.array.2020.100051.
6. K. Yue et al., "A survey of decentralizing applications via blockchain: The 5G and beyond perspective," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2191–2217, 2021, doi: 10.1109/COMST.2021.3115797.
7. "Good health pass: A safe path to global reopening," Good Health Pass Collaborative. <https://www.goodhealthpass.org/wp-content/uploads/2021/02/Good-Health-Pass-Collaborative-Principles-Paper.pdf> (Accessed: Jun. 10, 2021).

8. H. Baniata and A. Kertesz, "A survey on blockchain-fog integration approaches," *IEEE Access*, vol. 8, pp. 102,657–102,668, Jun. 2020, doi: 10.1109/ACCESS.2020.2999213.
9. N. Kshetri, "Blockchain and electronic healthcare records [Cybertrust]," *Computer*, vol. 51, no. 12, pp. 59–63, 2018, doi: 10.1109/MC.2018.2880021.
10. M. Whaiduzzaman *et al.*, "A privacy-preserving mobile and fog computing framework to trace and prevent COVID-19 community transmission," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 12, pp. 3564–3575, Dec. 2020, doi: 10.1109/JBHI.2020.3026060.
11. H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3915–3929, Mar. 1, 2021, doi: 10.1109/JIOT.2020.3025953.
12. H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled internet of medical things to combat COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 52–57, Sep. 2020, doi: 10.1109/IOTM.0001.2000087.
13. "EU digital COVID certificate," European Commission, Brussels, Belgium. [Online]. Available: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (Accessed: Jun. 1, 2021).
14. A. B. Haque, A. K. M. N. Islam, S. Hyrinsalmi, B. Naqvi, and K. Smolander, "GDPR compliant blockchains—A systematic literature review," *IEEE Access*, vol. 9, pp. 50,593–50,606, Mar. 2021, doi: 10.1109/ACCESS.2021.3069877.
15. H. Baniata and A. Kertesz, "FoBSim: An extensible open-source simulation tool for integrated fog-blockchain systems," *PeerJ Comput. Sci.*, vol. 7, p. e431, Apr. 2021, doi: 10.7717/peerj-cs.431.
16. H. Ritchie *et al.*, "Coronavirus pandemic (COVID-19)," Our World in Data. <https://ourworldindata.org/coronavirus> (Accessed: Jun. 1, 2021).



IEEE Security & Privacy magazine provides articles with both a practical and research bent by the top thinkers in the field.

- stay current on the latest security tools and theories and gain invaluable practical and research knowledge,
- learn more about the latest techniques and cutting-edge technology, and
- discover case studies, tutorials, columns, and in-depth interviews and podcasts for the information security industry.



computer.org/security

