Towards a Blockgraph-Based Trustless Authentication Scheme for Future 6G Technology

David Cordova Morales, Thi-Mai-Trang Nguyen, Guy Pujolle

▶ **To cite this version:**

David Cordova Morales, Thi-Mai-Trang Nguyen, Guy Pujolle. Towards a Blockgraph-Based Trustless Authentication Scheme for Future 6G Technology. 2023 2nd International Conference on 6G Networking (6GNet), Oct 2023, Paris, France. pp.1-4, 10.1109/6GNet58894.2023.10317665 . hal-04311911

HAL Id: hal-04311911
https://hal.science/hal-04311911

Submitted on 28 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Towards a Blockgraph-based Trustless Authentication Scheme for Future 6G Technology

David A. Cordova Morales*, Thi-Mai-Trang Nguyen*†, and Guy Pujolle*

* LIP6 - Sorbonne Université, CNRS, Paris, France
† L2TI - Université Sorbonne Paris Nord, Villetaneuse, France
david.cordova@lip6.fr, thi-mai-trang.nguyen@lip6.fr, guy.pujolle@lip6.fr

***Abstract*—One of the most important paradigm shifts nowadays regarding future 6G communication is related, from one side to the desire of bringing services and data as close as possible to the end users, and from another side, to empower the user with control over their data and personal information. In this vision, private 6G networks will shape trusted zones where data center services are placed at the edge of the network. The services will follow a Web3 approach, where decentralization and zero-trust mechanisms are predominant. In this environment, a decentralized authentication mechanism is needed. In this paper, we propose a 6G architecture and a blockchain-like authentication scheme based on Verifiable Credentials. Our model uses zero-trust technology for a better and more trusted Internet.**

***Index Terms*—6G architecture, Zero-trust model, Blockgraph, Verifiable Credentials**

I. Introduction

As 5G technology is being deployed around the world and new trends are emerging in the Web model, noble ideas are surging for the next generation of cellular networks. Web3 is a new Web paradigm that pushes towards a trustless and decentralized Internet, where users would rather interact with decentralized Applications (dApps), belong to collectively-owned Decentralized Autonomous Organizations (DAOs), and have control over their personal information than use the current Web model (i.e., Web2), where a few large corporations control most of the data traffic and users have no control over their personal information. These new features are all based on blockchain technology, which requires a distributed architecture [1]. In this regard, some work in the literature suggests that the future 6G technology should include a distributed network architecture composed of mobile trusted zones with nodes capable of maintaining a blockchain-like technology [2]–[6]. In our vision of a future 6G architecture, multiple private 6G networks (the trusted zones) might coexist and interact using blockchain, thus, removing the need for a trusted third party for authentication.

A Blockchain is a form of Distributed Ledger Technology (DLT) that can make all sorts of data immutable due to its properties. It is at the origin of Bitcoin [7] and is the underlayer technology for multiple services and applications [8]. Blockchain technology could easily be compatible with future 6G architecture [9], [10], not only for securing future 6G communication [11] but also to enable Web3 features and zero-knowledge inter-6G authentication. However, since our 6G nodes are mobile, a traditional blockchain cannot cope with network partitions due to the way it handles forks. Blockgraph, on the other hand, is a partition-tolerant blockchain-like data structure that inherits from blockchain properties, which was specially designed to function in dynamic networks with multiple network partitions and network aggregations.

Verifiable Credentials (VCs) are digital representations of information about an individual, an organization, or an entity that can easily be shared in the form of a Verifiable Presentation (VP) and easily verified by a verifier entity. They are usually used to prove claims of a subject issued by trusted entities (e.g., government, universities, and organizations). They use cryptographic primitives to ensure that the claim within the credential has not been tampered with and that it came from a trustworthy source. Decentralized Identifiers (DIDs) are a new type of globally unique identifier. They are designed to enable individuals and organizations to issue, hold, and control their own identifiers. DIDs enable entities to prove control over them by authenticating using cryptographic proofs such as digital signatures. DIDs are an integral part of the VC model and allow for a trustless identification of an entity.

The main objective of this paper is to propose a decentralized authentication scheme to enable the trusted zones to be connected to each other through Virtual Private Network (VPN) associated with zero-trust network access. This works without the need of a trusted third party. Our proposition uses blockgraph as a verifiable data registry where DIDs are stored in-chain. This makes DIDs unique, resolvable with high availability, and cryptographically verifiable. VCs are exchanged off-chain and contain the claims needed for authentication, where the verifier party only needs to cross-check the issuer's DID on the blockgraph to validate its identity.

The remainder of our paper is organized as follows. In section II, we describe the 6G architecture under development. Then, section III presents our distributed authentication scheme for inter-Edge communication between the trusted

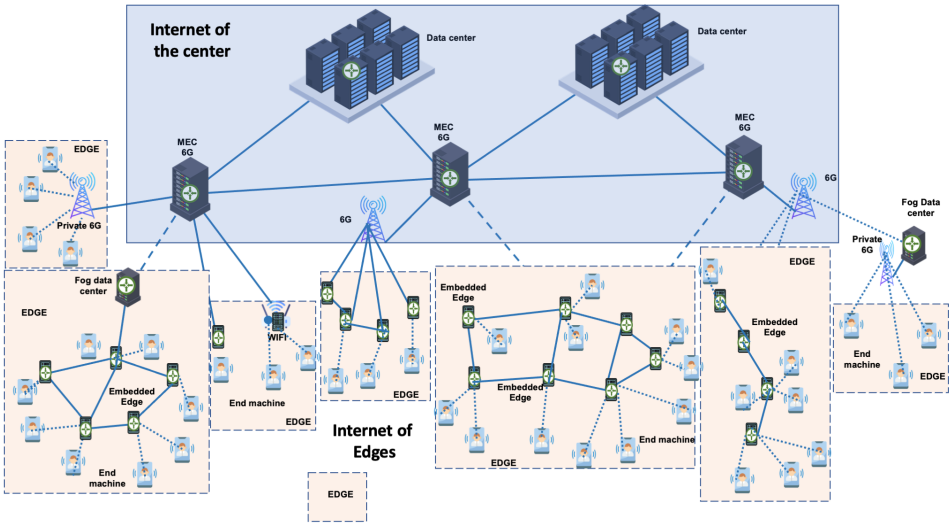

Fig. 1. The 6G architecture under study

zones. Section IV details the blockchain-like technology used for the authentication scheme and its resiliency to nodes' mobility. Finally, section V concludes this body of work.

II. The 6G network under study

In Figure 1, we describe the proposed 6G architecture, which is a service architecture incorporating a network that can be cut into two parts: the Internet of the Center and the Internet of Edges.

The Internet of the Center brings together large data centers and telecommunications operators' data centers placed at the edge, that is to say, mainly Multi-Access Edge Computing (MEC) data centers. These are the data centers going from relatively large to infinitely large size and are far from the end-users.

The Internet of Edges is formed from data centers that range from medium to infinitely small. Ideally, they should be tiny data centers embedded into the terminal equipment or very close to it. Fog data centers are also at a short distance from the terminal equipment. This network's architecture allows for vertical and horizontal traffic circulation. The vertical circulation climbs to the Internet of the Center or descends to the periphery, at the Internet of Edges, and the horizontal circulation moves at the same level. The horizontal displacement in the Internet of Edges provides short circuits, low energy consumption, and very strong security by cutting access to the Internet and working independently. On the contrary, vertical displacement gives long circuits, consumes more energy, and allows attacks from the Internet, but obviously, it has much higher computing power.

We recommend an architecture that integrates both horizontal and vertical networks, where the used services can move as close as possible to where they are requested, thus improving the energy consumption, quality of service, and data security of the requested service. The Edges are interconnected between them by secure channels generally crossing the Internet of the Center and are considered as horizontal links between Edges. Vertical networks are often linked through fixed antennas, while horizontal networks have the particularity of incorporating mobile antennas in addition to fixed antennas, especially when using embedded Edges.

As a result, and in contrast with current 5G architectures, our 6G architecture will be composed of multiple 6G private networks. Those networks should be able to remain hermetic to undesired connections and allow access when authorized. In this regard, we believe that the convergence between telecommunication networks and computer networks will be more anchored, and thus, multiple 6G private networks are likely to be deployed. To manage authorization access in this new architecture, a distributed authentication scheme among all trusted zones is needed. Today, blockchain technology is more mature and has proven to be resilient. Thus, we propose an authentication scheme based on blockchain-like technology to manage authorization access among trusted zones.

III. Authentification Scheme Proposal

The overall security of our 6G network architecture comes from trusted Edges, which are Edge networks including trusted zones endorsed by zero-trust policies. The confidentiality of an Edge network is ensured by the use of Decentralized Identities (DIDs), Verifiable Credentials (VCs), and Identity and Access Management (IAM) rules in a zero-trust authentication scheme. Moreover, it would be possible to use transparently, several techniques aiming for the protection of the network such as behavioral AI monitoring Edge software and securing code development by design. The security of inter-Edge communication will be enforced by the use of a partition-tolerant DLT, such as the

blockgraph, where zero-trust identifiers (i.e., DIDs) are stored in-chain and accessible to the whole network for verifiability.

A verification process between two entities will typically include a VP exchange between the VC holder and the VC verifier. The VP will include VCs containing claims of the VC holder to authenticate to a verifier entity. Claims are issued by well-known trusted issuers and contain the issuer's DID. Once the VP exchange is performed off-chain, the verifying entity will only have to cross-check the information relative to the issuer's DID in the VC with the information in the blockgraph.

Currently, several standards specifications are under revision to represent and request VCs claims [12], [13], to exchange them [14], [15], and to verify them [16]. This process creates a zero-trust environment that facilitates the secure authentication, authorization, and access control mechanisms that allow for granular control over the sharing and verification of identity attributes without relying on centralized identity providers. By following this process, certain data centers in the vertical network may be trusted areas by providing evidence for each request. Thus, it would not be possible of sending a message to a zone that cannot demonstrate the authenticity of its identity.

IV. Blockgraph

Blockgraph is a partition-tolerant DLT design for Mobile Ad Hoc Networks (MANETs). It brings blockchain properties and security while coping with network mobility and topologies changes. In the context of our proposed 6G architecture, MEC data centers in the Internet of Edge may be mobile and interact with each other through a mesh and ad hoc network. In this regard, the effect of mobility may cause links between nodes to break, causing potential network partitions. To cope with this issue, blockgraph can adapt the shape of its only-growing distributed ledger, accordingly to the partitions of the network. In that sense, the blockgraph will not form a traditional linear chain of blocks but a graph of blocks in the form of a Direct Acyclic Graph (DAG).

Cordova et. al. [17] introduced the concept of blockgraph where detailed characteristics of its architecture are provided. The blockgraph is composed of three primary modules that manage three different aspects of its functioning, naming, *the blockgraph protocol*, *the consensus module*, and *the group management module*. *The blockgraph protocol* takes care of the management of the DAG data structure and orchestrates the splits and merge functions. *The consensus module* hosts a compatible consensus algorithm such as C4M [18] capable of agreeing on the same state of the DLT while managing multiple node associations and dissociations. *The group management module* runs a topology discovery algorithm that gathers network topology information to alert on changes in the network topology. All modules use dedicated interfaces to exchange relevant information for the proper functioning of the blockgraph system.

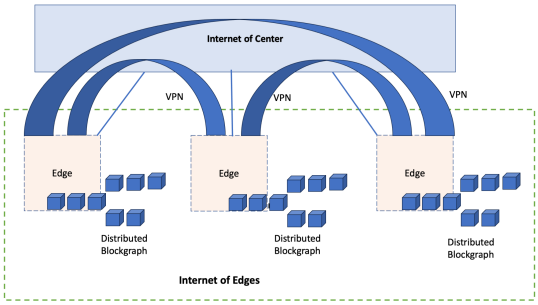

Fig. 2. Blockgraph deployment under study

The role of the blockgraph in our 6G architecture could be two folds: (i) as a means to securing future 6G communication as exposed in [11] and (ii) as a verifiable data registry for entity identity authentication. In the latter, the blockgraph will be distributed among multiple trusted zones as shown in figure 2, and each trusted zone will have multiple instances of the blockgraph, where identity identifier information (i.e., DIDs) from all trusted zones are stored. The blockgraph will guarantee the immutability and availability of all DIDs, while the distributivity property of the blockgraph will guarantee decentralization, which enhances the security and trust in the information that is being protected by the blockgraph. Moreover, DIDs are natively secure cryptographically and allow binding an identifier with an entity or subject. In our use case, the DIDs are identity information of well-known trusted VC issuers. Thus, a VC can be trusted by verifying that the issuer's DID is included in the VC, which is also cryptographically secured. The exchange of credentials is held off-chain through a standardized protocol that guarantees the authorized entities are allowed to interact. This blockgraph deployment aligns with the principle of zero-trust security since the distributivity of the blockgraph among the trusted zones will ensure decentralization and transparency of the DLT.

V. Conclusion

In this paper, we proposed a 6G architecture and an authentication scheme based on blockchain-like technology, called blockgraph, and Verifiable Credentials. We believe that our proposed architecture is an important stone to better achieve security for future 6G technology than its previous generations. However, there is still a lot of work to be done to achieve this goal, especially when moving from one trusted zone to another trusted zone. Using blockchain-like technology and Verifiable Credentials is a promising solution to enforce a decentralized and distributed zero-trust scheme for granular identity authentication and control access. Of course, attackers will always try to deceive any authentication scheme to become trusted before attacking. Thus, we must make sure that the entire system lies in a zero-trust model where resources are accurately verified, and requests are examined in detail to effectively limit the consequences of such attacks. The proposal made in this paper goes in that direction and will

be tested in depth by the authors within the framework of research projects. The main challenges of our proposal are on one hand to scale the blockgraph performance for massive use and on the other hand to prove that a zero-trust model for 6G technology is indeed feasible.

ACKNOWLEDGMENT

This work has been partially supported by the French AMI-5G ENE5AI project and the French DIM RFSI 5G-REISEP project

REFERENCES

[1] C. Guan, D. Ding, and J. Guo, "Web3.0: A review and research agenda," in *2022 RIVF International Conference on Computing and Communication Technologies (RIVF)*, 2022, pp. 653–658. DOI: 10.1109/RIVF55975.2022.10013794.

[2] K. Al Agha, P. Loygue, and G. Pujolle, *Edge Networking: Internet des Edges*. ISTE Group, 2022.

[3] K. Al Agha, P. Loygue, and G. Pujolle, "Horizontal network for a better cybersecurity," in *2022 6th Cyber Security in Networking Conference (CSNet)*, IEEE, 2022, pp. 1–4.

[4] K. Al Agha, P. Loygue, and G. Pujolle, "Horizontal 6g," in *2022 1st International Conference on 6G Networking (6GNet)*, IEEE, 2022, pp. 1–7.

[5] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6g networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[6] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6g: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21 260, 2008.

[8] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 99–114, 2020, ISSN: 0743-7315. DOI: https://doi.org/10.1016/j.jpdc.2019.12.019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0743731519308664.

[9] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[10] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6g: Challenges and opportunities," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[11] D. Cordova, T.-M.-T. Nguyen, P. B. Velloso, and G. Pujolle, "A preliminary assessment of blockgraph-a mobility-aware solution to secure 6g mesh networks," in *2022 1st International Conference on 6G Networking (6GNet)*, IEEE, 2022, pp. 1–4.

[12] W3C Working Draft, *Securing verifiable credentials using json web tokens*, https://www.w3.org/TR/vc-jwt/, May 2023.

[13] W3C Working Draft, *Verifiable credential data integrity 1.0*, https://www.w3.org/TR/vc-data-integrity/, Apr. 2023.

[14] K. N. Chadwick and J. Vercammen, "Openid for verifiable credentials," 2022.

[15] S. Curren, T. Looker, and O. Terbu, *Didcomm messaging v2.1 editor's draft*, https://identity.foundation/didcomm-messaging/spec/v2.1, 2022.

[16] M. Jones, J. Bradley, and N. Sakimura, "Json web signature (jws)," Tech. Rep., 2015.

[17] D. Cordova, A. Laube, G. Pujolle, *et al.*, "Blockgraph: A blockchain for mobile ad hoc networks," in *2020 4th cyber security in networking conference (CSNet)*, IEEE, 2020, pp. 1–8.

[18] D. C. Morales, P. B. Velloso, A. Laubé, T.-M.-T. Nguyen, and G. Pujolle, "A performance evaluation of c4m consensus algorithm," *Annals of Telecommunications*, vol. 78, no. 3-4, pp. 169–182, 2023.