Tradeoffs In Using Blockchain Technology For Security, Privacy, And Decentralization:theoretical And Empirical Perspectives

Aleksandar Tošić
Faculty of Mathematics, Natural Sciences and Information Technologies
University of Primorska
E-mail: aleksandar.tosic@upr.si

Thesis Summary

Keywords: Edge Computing, Blockchain, Container orchestration, Consensus mechanism

Received: June, 15, 2023

This paper is and extended abstract of the doctoral thesis [1]. It identifies four selected topics in which blockchain technology can have a positive or transformative effect on existing solutions. We propose new protocols, which change the current standards to add functionality, improve performance or overcome limitations of existing blockchain networks. Specifically, we focus on container orchestration on the edge using a unique blockchain protocol for security, verifiability, and trust.

Povzetek: Pričujoče delo je razširjen povzetek doktorske disertacije [1]. Delo predstavlja raziskavo, ki se osredotoča na uporabo tehnologije blockchain za izboljšanje obstoječih rešitev na štirih izbranih področjih. Poseben poudarek je na razvoju in implementaciji edinstvenega blockchain protokola za orkestracijo kontejnerjev na robu omrežja, ki zagotavlja varnost, preverljivost in zaupanje.

1 Introduction and problem statement

In recent years, cloud computing became a commonly used architecture for most applications. The shift of the geography of computation was incentivized by many factors ranging from ease of software maintenance [2], reliable quality of service(QoS), hardware flexibility, and cost (CapEx to OpEx) [3], etc However, with the expected growth of data generation and consumption and storage and service provisioning in cloud computing environments, the architecture is pushing network bandwidth requirements to the limit [4]. Edge computing in it's simplest form can be defined as an architecture in which computation is moved to the edge of the network in order to make use of the geographic proximity to decrease latency and improve bandwidth. This recent paradigm shift attempts to address the overly geographically-centralized cloud architecture. However, distributing services to the edge introduces new challenges such as resource allocation, service and application migration, trust, etc.. Blockchain technology may be used to address some of the issues. It can serve as a layer of trust between the system, and the end user by providing a verifiable and transparent ledger of the state of the system. To achieve this, a new protocol is required that would overcome the latency constraint, decentralized resource allocation, and real-time container migrations [5].

2 Methodology

We design, and develop a new blockchain protocol aimed at autonomous decentralized container orchestration suitable for edge devices. The proposed protocol uses verifiable delay functions(VDFs)[6] as the entropy source for secure randomness. Nodes participating in consensus compute a function $p = vdf(bh, bd)$ where p is the proof, bh is the SHA256 hash of the current block, and bd is the difficulty of the current block. We show that p is a sufficiently secure source of entropy for generating randomness. Moreover, given delay imposed on the nodes computing the VDF prevents malicious nodes to peek into the future. Using the shared seed, nodes are able to self-elect into consensus roles for each slot without communication overhead as shown in Figure 1.

3 Evaluation methodology and results

We performed extensive testing of our reference implementation simulating networks as large as 1000 nodes. The telemetry obtained from logging the state of all nodes shows that the protocol is scalable, and can efficiently converge towards average resource utilization of the entire network by performing real-time container migrations between nodes using Checkpoint/Restore In Userspace (CRIU). Moreover, our results show that using CRIU significantly improves the performance making our protocol viable in practice.

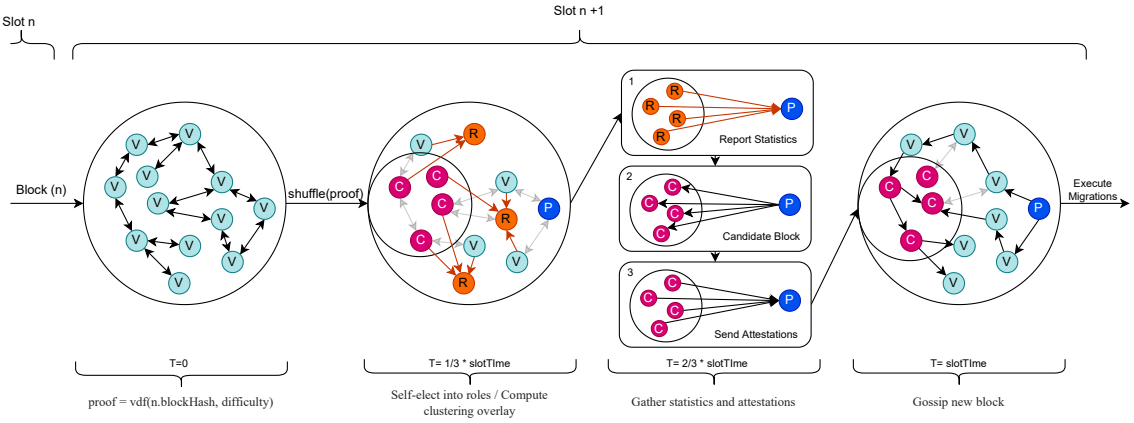

Figure 1: Role based consensus mechanism using VDFs as an entropy source

4 Discussion and further work

Our results showcase the feasibility of the proposed protocol for large networks of edge devices with limited compute resources. However, decentralized networks must address Byzantine behaviour of nodes. To secure the protocol against malicious actors the protocol must secure containerized application and guarantee the execution. Existing solutions such as Intel SGX are not generic and inherently impose hardware restrictions on the protocol. Research should focus overcoming specific hardware implementations of trusted computation.

References

[1] A. Tošić, "Empirična študija uporabe tehnologije veriženja blokov v obstoječih sistemih in arhitekturah: doktorska disertacija," Ph.D. dissertation, Univerza na Primorskem, Fakulteta za matematiko, naravoslovje in …, 2022.

[2] E. Bayrak, J. Conley, and S. Wilkie, "The economics of cloud computing," 2011.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[4] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[5] A. Tošić, J. Vičič, M. Burnard, and M. Mrissa, "A blockchain protocol for real-time application migration on the edge," *Sensors*, vol. 23, no. 9, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/9/4448

[6] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I*. Springer, 2018, pp. 757–788.