Foreword to the special issue on cryptocurrencies and blockchains for distributed systems

Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

SPECIAL ISSUE PAPER

Foreword to the Special Issue on Cryptocurrencies and Blockchains for Distributed Systems

Stefano Ferretti* | Gabriele D'Angelo

Department of Computer Science and Engineering, University of Bologna, Bologna, Italy

Correspondence
*Stefano Ferretti, Department of Computer Science and Engineering, University of Bologna,Via Zamboni, 33, 40126 Bologna, Italy. Email: s.ferretti@unibo.it

Summary

No summary.

1 | INTRODUCTION

The Internet is evolving into a new multi-factor paradigm based around smart systems, Internet of Things (IoT), distributed ledgers and blockchains, digital assets (e.g. cryptocurrencies). In the next years, these technologies will converge and interact, fostering novel services, business models and applications. For example, the blockchain can provide an automated and secure ledger infrastructure for the next generation IoT, mobile and smart systems. Moreover, distributed ledgers allow recording untamperable proofs that certain data have been produced, thus proving the validity of contained information. Blockchain and related cryptocurrencies also enable the development of micro-transactions schemes to foster data crowdsourcing and exchange for smart services.

This special issue collects important contributes focusing on the new challenges posed by the novel technologies and applications that are based on blockchain technologies. It collates representative research articles that were presented at the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2018), held in conjunction with the 16th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys 2018). Moreover, other completely original works have been included, for a total of 12 papers.

2 | THEMES OF THIS SPECIAL ISSUE

The set of accepted papers can be organized under the following key themes: "architecture and algorithms", "applications" and "IoT, smart cities and pervasive computing", "modeling and performance".

2.1 | Architecture and Algorithms

In [1], G. Vizier and V. Gramoli introduce a novel type of blockchain, called community blockchain. A community blockchain is in between the two opposite public and consortium blockchains. Community blockchains differ from public blockchains by constraining the set of deciders for a particular block and differ from consortium or private blockchains by letting all nodes decide upon some block. This allows to take the advantages of a private blockchain, without the need to restrict the block decision

to a small "elite". Thus, a periodic reconfiguration of the set of nodes in charge of validating and adding novel blocks to the blockchain. An experimentation demonstrates the feasibility of using Byzantine reconfiguration in a such a blockchain.

In [2], C. Pérez-Solà and J. Herrera-Joancomartí compare existing smart contract interactions and develop an architecture for asynchronous state consensus, a novel type of smart contract interaction required in applications but had rarely been addressed. The proposed architecture is composed of two types of smart contracts: Custodian and Client. Client smart contracts serve as network participants, reaching a particular consensus collectively by forming clusters and issuing votes towards a final state agreement. Custodian smart contracts serve as the arbiters that aggregate and calculate voting results as the finalized state consensus that is shared across the network. To test the feasibility of their proposal, the authors conduct experiments on the consensus reaching latency and the scalability under different network configurations.

In [3], N. Alzahrani and N. Bulusu address the problem of counterfeit goods. The authors propose a new system called Block-Supply that is a decentralized anti-counterfeiting supply chain that exploits NFC and blockchain technologies. Moreover, they propose a decentralized consensus protocol that, unlike most of the existing protocols, does not require Proof-of-Work. Rather, the scheme randomly employs a set of different size of validators each time a new block is proposed. More in detail, a decentralized, dynamic mapping between the nodes that participate in the consensus process is utilized. This mapping ensures that the interaction between these nodes is executed anonymously and blindly.

In [4], P. Ezhilchelvan, A. Aldweesh and van A. Moorsel propose a way to eliminate a well known vulnerability of the Two Phase Commit (2PC) protocol. The proposed solution uses a blockchain for coordinating 2PC execution. The authors present the impossibilities, the possibilities, the cost and the trade-offs of the blockchain-based approach to blocking-free management of distributed transactions. Moreover, they prove that a non-blocking and blockchain-coordinated 2PC protocol can exist only if both the blockchain and distributed database systems meet synchrony requirements. An implementation on the Ethereum Testnet demonstrates, through experiments, that the monetary cost of executing smart contracts is quite small.

2.2 | Applications

In [5], C. Pérez-Solà and J, Herrera-Joancomartí discuss some problems related to digital content authenticity. Since digital coins have solved a similar problem through cryptocurrencies, then the same techniques are applied to similar scenarios, where the ownership of digital assets needs to be preserved. In this paper, the authors propose BArt, a transparent and distributed mechanism for artists to commercialize their digital artwork, keeping control of the copies, monetizing its usage, and maintaining ownership. In fact, BArt allows artists to publicly register their work in the Bitcoin blockchain and sell usage rights in exchange for bitcoins. Buyers are allowed to exert the acquired rights. In the proposed system, proper behaviour from all parties is enforced by the system with cryptography and economic incentives.

In [6], L. Herskind, A. Giaretta, M. De Donno and N. Dragoni propose a new approach to disbursement registration. In this paper, they present BitFlow, a blockchain-based architecture that provides complete cash-flow transparency and diminishes the probability of undetected frauds through the BitKrone, a non-volatile cryptocurrency that maps to the Danish Krone (DKK). They show that confidentiality can be effectively achieved on a permissionless blockchain using ZeroKnowledge proofs, ensuring verifiable transfers and automatic evaluations.

2.3 | IoT, Smart Cities and Pervasive Computing

In [7], A. Durand, P. Gremaud and J. Pasquier propose a fully decentralized low-power wide-area network (LPWAN) infrastructure for the Internet of things (IoT) using the LoRa protocol. While global LPWANs typically require roaming agreements between network providers and a trusted third party for server resolution, a trustless model is presented in this paper, where the network servers are resolved using a blockchain application. Since LoRaWAN relies on symmetric cryptography, a new security model is proposed, that adds non-repudiation using digital signatures. This paves the way for linking devices to decentralized applications.

In [8], Z. Khan, A.G. Abbasi and Z. Pervez investigate the pivotal role of blockchain in providing privacy, self-verification, authentication, and authorisation of participatory transactions in open governance. They also investigate to what extent edge computing can contribute towards management of permissioned sharing at specific administrative levels, and enhances privacy and provides an economic approach for resource utilisation in a distributed environment. More specifically, the authors introduce a novel architecture that is based on distributed hybrid ledger and edge computing model. That architecture provides refined and secure management of data generated and processed in different geographical and administrative units of a city. To validate the

proposal, a proof of concept of the architecture has been implemented and it has been applied on a carefully designed use case: citizen participation in administrative decisions through consensus.

In 9, O.J.A. Pinno, A.R.A. Grégio and L.C.E. De Bona present ControlChain, that is an access control authorization architecture heavily based on the Blockchain technology. The authors demonstrate the viability of the ControlChain through the EControlChain, a proof-of-concept developed to run over the Ethereum network. The proposed architecture follows the IoT tendency requirements and are user-transparent, user-friendly, fully decentralized, scalable, fault tolerant and compatible with a wide range of today's access control models already used in the IoT.

In 10, A.R. Kabbinale, E. Dimogerontakis, M. Selimi, A. Anwaar, L. Navarro and A. Sathiaseelan deal with decentralization, in the form mesh networking and blockchain. They explore and evaluate two existing blockchain software stacks, Hyperledger Fabric (HLF) and Ethereum geth with Proof of Authority (PoA), deployed in a real citywide production mesh network, and in a centralized laboratory network. They aim to quantify the performance, bottlenecks and identify the current limitations and opportunities for improvement to serve the needs of wireless mesh networks.

2.4 | Modeling and Performance

In 11, S. Ferretti and G. D'Angelo analyze the Ethereum blockchain using the complex networks modeling framework. More specifically, accounts acting on the blockchain are represented as nodes, while the interactions among these accounts, recorded on the blockchain, are treated as links in the network. Using this representation, it is possible to derive interesting mathematical characteristics that improve the understanding of the actual interactions happening in the blockchain. Not only, by looking at the history of the blockchain, it is possible to verify if radical changes in the blockchain evolution happened.

In 12, S. Bergman, M. Asplund and S. Nadjm-Tehrani compare two popular frameworks, Hyperledger Fabric and Apache Cassandra as representatives of permissioned blockchains and distributed databases respectively. They compare their latency for varying workloads and network sizes. The results show that for small systems, blockchains can start to compete with traditional databases, but also that the difference in consistency models and differences in setup can have a large impact on the resulting performance.

3 | CONCLUSION

The articles presented in this special issue provides insights in fields related to Blockchains and Cryptocurrencies in distributed systems. We wish the readers can benefit from insights of these papers, and contribute to these rapidly growing areas.

4 | GUEST EDITORS

4.1 | Stefano Ferretti

Stefano Ferretti is an Associate Professor at the Department of Computer Science and Engineering of the University of Bologna. He received the Laurea degree (summa cum laude) and the Ph.D. in Computer Science from the University of Bologna respectively in 2001 and in 2005. His current research interests include distributed systems, computer networks, complex networks, wireless networks, mobile communications. He is in the editorial board of the Simulation Modelling Practice and Theory (SIMPAT) journal published by Elsevier.

4.2 | Gabriele D'Angelo

Gabriele D'Angelo received the Laurea degree (summa cum laude) in Computer Science in 2001, and a Ph.D. in Computer Science in 2005, both from the University of Bologna, Italy. He is an Assistant Professor at the Department of Computer Science and Engineering, University of Bologna. His research interests include parallel and distributed simulation, distributed systems, online gaming and computer security. Since 2011 he is in the editorial board of the Simulation Modelling Practice and Theory (SIMPAT) journal published by Elsevier.

ACKNOWLEDGEMENTS

We would like to thank all of the authors who provided valuable contributions to this special issue. We are also grateful to the Review Committee for the feedback provided to the authors, which are essential in further enhancing the papers. Finally we would like to express our sincere gratitude to Professor Geoffrey Fox, the Editor in Chief, for providing us with this unique opportunity to present our works in the international journal of Concurrency and Computation: Practice and Experience.

References

1. Vizier G, Gramoli V. ComChain: A Blockchain with Byzantine Fault Tolerant Reconfiguration. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

2. Hu YC, Lee TT, Chatzopoulos D, Hui P. Analyzing Smart Contract Interactions and Contract Level State Consensus. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

3. Alzahrani N, Bulusu N. A New Product Anti-Counterfeiting Blockchain Using a Truly Decentralized, Dynamic Consensus Protocol. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

4. Ezhilchelvan P, Aldweesh A, Moorsel vA. Non-Blocking Two Phase Commit Using Blockchain. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

5. Pérez-Solà C, Herrera-Joancomartí J. BArt: Trading digital contents through digital assets. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

6. Herskind L, Giaretta A, De Donno M, Dragoni N. BitFlow: Enabling Real-Time Cash-Flow Evaluations through Blockchain. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

7. Durand A, Gremaud P, Pasquier J. Decentralized LPWAN infrastructure using blockchain and digital signatures. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

8. Khan Z, Abbasi AG, Pervez Z. Blockchain and Edge Computing based Architecture for Participatory Smart City Applications. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

9. Pinno OJA, Grégio ARA, De Bona LCE. ControlChain: a New Stage on the IoT Access Control Authorization. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

10. Kabbinale AR, Dimogerontakis E, Selimi M, Anwaar A, Navarro L, Arjuna S. Blockchain for Economically Sustainable Wireless Mesh Networks. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

11. Ferretti S, D'Angelo G. On the Ethereum blockchain structure: a complex networks theory perspective. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.

12. Bergman S, Asplund M, Nadjm-Tehrani S. Permissioned Blockchains and Distributed Databases: A Performance Study. *Concurrency and Computation: Practice and Experience [this issue]*; Note to Publisher: Please put full reference here in proofs.