Blockchain Ecosystems

Goals: Define, study, and develop efficient composition of blockchain-like systems

Tools: Logic, algorithmic reasoning, programming

Prerequisites: The positions are offered to both foreign and French students who hold a Master degree in computer science. Solid mathematical background, basic knowledge of distributed algorithms, basic concurrent programming skills, curiosity, persistence and taste for challenging problems are expected.

The prominent *blockchain* technology aims at implementing a public "ledger": a decentralized consistent history of transactions proposed by an *open* set of participating processes, with no static membership. This problem can be seen as an instance of fault-tolerant *state-machine replication* [17], examples of which are the *crash-tolerant* Paxos protocol by Lamport [14] and the PBFT (*Byzantine* fault-tolerance) by Castro and Liskov [2]. These systems use instances of *consensus* protocols in order to ensure that users get consistent views of the system evolution.

Principal downside of classical consensus protocols are lack of scalability and the need for a fixed or properly reconfigurable set of participants out of which only a bounded fraction (up to one third) can be faulty. This can be hard to ensure in an open (permissionless) system, where an arbitrary fraction of participants can be controlled by the adversary [4].

The crucial innovation of the Bitcoin protocol [16] was achieving (nondeterministic) consistency in an open system by assuming that the adversary can control at most a minority (in practice, a minor fraction) of computing power. Consistency of the protocol relies on the *proof of work* (PoW) mechanism, requiring a participant to solve a time-consuming cryptographic puzzle before updating the ledger, assuming that communication is synchronous. The resulting protocols are notoriously slow and energy-demanding and an immediate question is whether these costs and assumptions are unavoidable.

Multiple alternative "proof-based" mechanisms have been proposed: *proof-of-stake* [1,13], *proof-of-space* [5], or *proof of space-time* [15]. However, the proposals still resort to synchronous networks and/or impose restrictions on the fraction of honest players to ensure proper security levels.

An alternative approach is to focus on the very problem that blockchains originally intended to solve: exchanging assets between users' accounts [16]. It turns out that this problem *per se* does not require consensus [8, 9]. In many practical scenarios, when every account is exclusively *owned* by a dedicated user, an asset transfer system can be implemented via standard broadcast mechanisms, and inherent complexity bounds of these mechanisms can be efficiently circumvented using randomization [10].

Of course, the scope of blockchain application goes way beyond asset transfers. In this proposal, we intend to adress the very question of the optimal consistency level for a specific application that An intriguing example of such an application of this study is a "blockchain ecosystem": a collection

of blockchains or storage systems interacting with each other. In the simplest form, we might want to bound strong consistency demands to individual systems and limit cross-system request to simple *read* operations. But what if we also need complex *cross-chain* transactions, not limited to swaps or deals [11, 12]? Which model assumptions efficient implementation of such transaction might require?

The goals of this project are twofold. On the one hand, we intend to characterize the model assumptions that enable generic blockchain interactions in an consortium or an open system. This will involve determining precise bounds on the amount of synchrony [3, 6] and energy/space/time consumption for implementing a generic distributed transaction ledger. This might lead to improving the conventional "proof" mechanisms, used, e.g., in Tezos [7] and Cardano [13] platforms.

On the other hand, we plan to explore the space of consistency definitions that enable generalizations of *cross-chain* transactions in the ecosystem. Maintaining a consensus-based total order on *all* transactions across blockchain systems may not be necessary: intuitively, nonconflicting transactions may be accepted in parallel without requiring consensus. In the permissionless context, this may allow us to completely get rid of costly and slow "proofs". In conventional ("permissioned") models, we expect this to bring considerable performance gains.

Theoretical in nature, the project is motivated by important practical concerns. Besides establishing provable complexity and computability bounds, it intends to develop system prototypes that are not only formally proved correct but also studied experimentally.

Location

Located in the Paris area, Télécom Paris (formerly known as ENST or École nationale supérieure des télécommunications) is one of the top French public institutions of higher education and research (Grandes Écoles), a founding member of Institut Polytechnique Paris. In collaboration with httph://epfl.ch, it has established Institut Eurécom at Sophia-Antipolis.

Contact

Prof. Petr Kuznetsov
`https://perso.telecom-paristech.fr/kuznetso/`
`petr.kuznetsov@telecom-paris.fr`
INFRES, Télécom Paris, Institut Polytechnique Paris

References

[1] I. Bentov, A. Gabizon, and A. Mizrahi. Cryptocurrencies without proof of work. In *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*, pages 142–157, 2016.

[2] M. Castro and B. Liskov. Practical byzantine fault tolerance. In *OSDI: Symposium on Operating Systems Design and Implementation*. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, Feb. 1999.

[3] T. D. Chandra, V. Hadzilacos, and S. Toueg. The weakest failure detector for solving consensus. *J. ACM*, 43(4):685–722, July 1996.

[4] J. R. Douceur. The sybil attack. In *Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*, pages 251–260, 2002.

[5] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak. Proofs of space. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, pages 585–605, 2015.

[6] F. C. Freiling, R. Guerraoui, and P. Kuznetsov. The failure detector abstraction. *ACM Comput. Surv.*, 43(2):9:1–9:40, 2011.

[7] L. Goodman. Tezos: A self-amending crypto-ledger: Position paper, August 2014. `https://tezos.com/static/papers/position_paper.pdf`.

[8] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D. Seredinschi. AT2: asynchronous trustworthy transfers. *CoRR*, abs/1812.10844, 2018.

[9] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D. Seredinschi. The consensus number of a cryptocurrency. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC 2019, Toronto, ON, Canada, July 29 - August 2, 2019.*, pages 307–316, 2019.

[10] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D. Seredinschi. Scalable byzantine reliable broadcast. In *DISC 2019*, 2019. To appear, TR: https://arxiv.org/abs/1908.01738.

[11] M. Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, PODC 2018, Egham, United Kingdom, July 23-27, 2018*, pages 245–254, 2018.

[12] M. Herlihy, B. Liskov, and L. Shrira. Cross-chain deals and adversarial commerce. *CoRR*, abs/1905.09743, 2019.

[13] A. Kiayias, A. Russell, B. David, and R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 357–388, 2017.

[14] L. Lamport. The Part-Time parliament. *ACM Transactions on Computer Systems*, 16(2):133–169, May 1998.

[15] T. Moran and I. Orlov. Proofs of space-time and rational proofs of storage. *IACR Cryptology ePrint Archive*, 2016:35, 2016.

[16] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, May 2009. `https://bitcoin.org/bitcoin.pdf`.

[17] F. B. Schneider. Implementing fault-tolerant services using the state machine approach: A tutorial. *ACM Computing Surveys*, 22(4):299–319, Dec. 1990.