Secure and scalable algorithms for DAG-based blockchains

PhD Director : Maria Potop-Butucaru
Team : NPA, LIP6
maria.potop-butucaru@lip6.fr

Abstract
Blockchain and distributed ledger technologies have emerged as one of the most revolutionary developments in recent years, with the goal of eliminating centralised intermediaries and installing distributed trusted services. They facilitate trustworthy trades and exchanges over the Internet, power cryptocurrencies, ensure transparency for documents, and much more. Traditionally, blockchain systems maintain a continuously-growing list of ordered blocks that include one or more transactions that have been verified by the members of the system, called miners. Blocks are linked using cryptography and the order of blocks in the blockchain is the result of a form of agreement among the system participants. After the releasing of the most popular blockchains (e.g., Bitcoin or Ethereum) with a specific focus on economical transactions their huge potential for various other applications became evident. However, quickly after their release blockchains reached their limits in terms of throughput, blocksize and unforeseen behaviors. Therefore, non academic research further concentrate in proposing alternatives by improving some performance aspects but with non zero costs either on security or throughput. One of these solutions extends the blockchain to a DAG overlay. The objective of the thesis is to analyze the algorithmic building blocks of existing DAG-based blockchains and to push further the state of the art in terms of security , privacy, consistency guaranties, algorithms, performance evaluation (energy).

Detailed description
Blockchain and distributed ledger technologies have emerged as one of the most revolutionary developments in recent years, with the goal of eliminating centralised intermediaries and installing distributed trusted services. They facilitate trustworthy trades and exchanges over the Internet, power cryptocurrencies, ensure transparency for documents, and much more. Traditionally, blockchain systems maintain a continuously-growing list of ordered blocks that include one or more transactions that have been verified by the members of the system, called miners. Blocks are linked using cryptography and the order of blocks in the blockchain is the result of a form of agreement among the system participants. After the releasing of the most popular blockchains (e.g., Bitcoin or Ethereum) with a specific focus on economical transactions their huge potential for various other applications became evident. However, quickly after their release blockchains reached their limits in terms of throughput, blocksize and unforeseen behaviors. Therefore, non academic research further concentrate in proposing alternatives by improving some performance aspects but with non zero costs either on security or throughput. One of these solutions extends the blockchain to a DAG overlay and provide an ordering over all blocks and transactions, and outputs a consistent set of accepted transactions. In the research along this line transactions are still organized on blocks. All these DAG-based systems structure blocks in a Directed Acyclic Graph. Each block can include several references to predecessors. More recently, IOTA has been defined as an alternative dedicated to IoT area where micro-transactions are submitted at a very high rate. Transactions define a DAG overlay a.k.a. tangle. Strategies to maintain an IOTA-tagle have been proposed and analyzed in [6]. IOTA-tangle properties have been formalized and analyzed in [2], [7] and [4]. More recently, [10] and [1] analyze in detail the stability and the attack resilience of IOTA-tangle. One of

the first works addressing the fairness of the selection mechanism in the IOTA tangle is [3]. Recently in [12] is defined a new notion of fairness: confidence fairness for tips selection algorithms to guarantee the first approval for all honest tips. A new tangle is proposed, G-IOTA, that aims at increasing the overall fairness in IOTA tangle by protecting tips who have been left behind, incentivizes users to respect the algorithm and punishes the conflicting transactions. G-IOTA provides also a mutual supervision mechanism that reduces the benefits of speculative and lazy behaviours. IOTA is one of the many examples of DAG-based blockchains and the curent state of the art analyses only few aspects of the DAG-based blockchains (e.g stability and security).

Objectives of the thesis

The objective of the thesis is to analyze the algorithmic building blocks of existing DAG-based blockchains (IOTA, Ghost, Phantom, Phantomette, Sycomore, etc) into a unified framework and to push further the state of the art in terms of security , privacy, consistency guaranties, fairness, energy consumption performances.

Bibliography

[1] Quentin Bramas. La Stabilité de l'Enchevêtrement dans la Cryptomonnaie IOTA. In ALGOTEL 2018 - 20èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, Roscoff, France, May 2018.

[2] B Kusmierz. The first glance at the simulation of the tangle: discrete model.

https://assets.ctfassets.net/r1dr6vzfxhev/2ZO5XxwehymSMsgusUE6YG

/f15f4571500a64b7741963df5312c7e7/The First Glance of the Simulation Tangle - Discrete Model v0.1.pdf, 2017. Accessed 14 Feb 2018.

[3] Bartosz Kusmierz and Alon Gal. Probability of being left behind and probability of becoming permanent tip in the tangle v0. 2.
https://assets.ctfassets.net/r1dr6vzfxhev/6FMwUH0b4WIyi6mm8oWWgY

/8f1d7b30f7b652098a5e68b6634c63df/POLB-02.pdf, 2018. Accessed 16

APR 2018.

[4] Bartosz Kusmierz, Philip Staupe, and Alon Gal. Extracting tangle properties in continuous time via large-scale simulations. Technical report, working paper, 2018.

[5] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008.

[6] Serguei Popov. The tangle. http://www.descryptions.com/Iota.pdf, 2018. Accessed 30 APR 2018.

[7] Serguei Popov, Olivia Saa, and Paulo Finardi. Equilibria in the tangle. arXiv preprint arXiv:1712.05385, 2017.

[8] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. SPECTRE: A fast and scalable cryptocurrency protocol. IACR Cryptology ePrint Archive, 2016:1159, 2016.

[9] Yonatan Sompolinsky and Aviv Zohar. PHANTOM: A scalable blockdag protocol. IACR Cryptology ePrint Archive, 2018:104, 2018.

[10] Philip Staupe. Quasi-analytic parasite chain absorption probabilities in the tangle.

https://assets.ctfassets.net/r1dr6vzfxhev/1qm4qixNPSqOWIAImMYMaG

/5cc32a3c4d6f54dbe85c9321dc25a01b/QuasiAnalytic Parasite Chain

Absorption Probability - v2.pdf, 2017. Accessed 31 Dec 2017.

[11] G. Wood. Ethereum: A secure decentralised generalised transaction ledger. http://gavwood.com/Paper.pdf.

[12] Gewu Bu, Onder Gurcan, Maria Potop-Butucaru, G-IOTA: Fairness and confidence aware Tangle, preprint 2019 (Cryblock@Infocom 2019).