Verifiable Delay Functions for Permissionless Replicated Systems

**Goals:** Design a permissionless agreement protocol based on verifiable delay functions.

**Tools:** Logic, algorithmic reasoning, programming

**Prerequisites:** basic knowledge of distributed algorithms and cryptographic tools, basic concurrent programming skills, curiosity and persistence

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 [19], prominent examples of which are the crash-tolerant Paxos protocol by Lamport [16] and the BFT (Byzantine fault-tolerant) system by Castro and Liskov [5]. 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 (also called permissionless) system, where an arbitrary fraction of participants can be controlled by the adversary [9]. Prominent blockchain protocols [18,20] achieve (nondeterministic) consistency by assuming that (1) the system is synchronous, (2) participants can use asymmetric cryptography, and (3) the adversary can control at most a minority (in practice, a minor fraction) of computing power.

Intuitively, these assumptions are used to overcome the folklore CAP theorem [3,10] stating that no system can combine Consistency, Availability, and Partition-Tolerance. In particular, these protocols avoid partitioning by enforcing the proof of work (PoW) mechanism requiring that a participant must solve a time-consuming cryptographic puzzle before updating the ledger. The resulting protocols are notoriously slow and energy-demanding. More recent blockchain prototypes propose to obviate the energy demands via using proof-of-stake [1,13]. However, these solutions are subject to multiple attacks enabling forks, such as the "nothing-at-stake attack", where many miners are incentivized to extend every branch in a potential fork, and the "long range attack", where a long alternative branch is held privately by the adversary in order to overtake the longest chain. More recent proposals [7] resort to synchronous networks, rely on expensive cryptographic assumptions, and/or impose restrictions on honest players. An immediate question is whether these costs and assumptions are unavoidable.

To mitigate these attacks and, possibly, improve performance, one may invest into verifiable delay functions (VDFs) [2], a recently proposed cryptographic mechanism based on puzzles that can only be solved sequentially, but without wasting energy on meaningless intensive computations. There is evidence that VDFs can be used to replace PoW in Nakamoto consensus [17], however we still do not understand how this mechanism can be used in more general contexts.
This project intends to explore the potential of using VDFs in permissionless implementations of replicated services, not only consensus-based [6,16], but also weaker abstractions: reliable broadcast [12], lattice agreement [14,15] and cryptocurrencies [8,11].

Milestones

1. Study the literature on permissionless computing [4,7,18] and modern cryptographic tools [2].
2. Define a range of permissionless system model that allows the use of VDFs for consistent data replication: synchrony assumptions, failure patterns, the use of trusted cryptographic setup.
3. Implement a replicated state machine and weaker abstractions in the resulting models and study their performance.

Contact

Duong Hieu Phan
https://www.di.ens.fr/users/phan/
hieu.phan@telecom-paris.fr
INFRES, Télécom ParisTech, Institut Polytechnique Paris

Petr Kuznetsov
http://www.infres.enst.fr/~kuznetso/
petr.kuznetsov@telecom-paristech.fr
INFRES, Télécom ParisTech, Institut Polytechnique Paris

References


