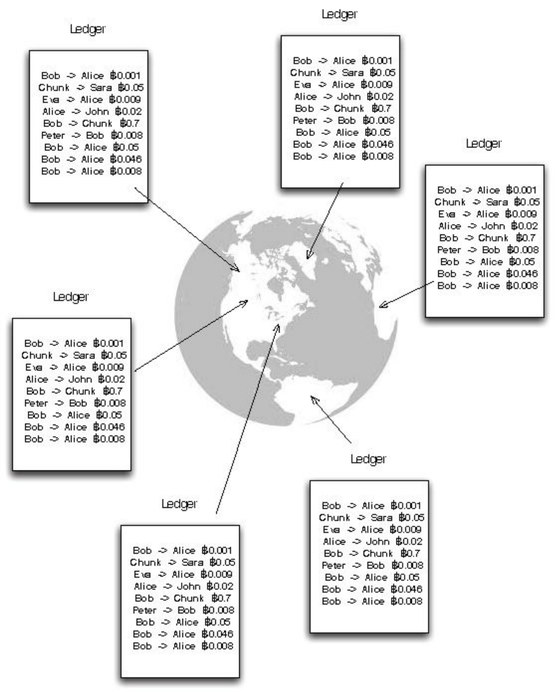
Blockchain FM
Formal Methods

IRISA Adopnet
IRISA/Inria Celtique
IRISA/Inria Cidre

Context and Objectives

Project started january 2019, related to the distributed algorithms for the blockchain technology, and its formal verification.

A blockchain is commonly presented as “an immutable distributed ledger with decentralized control”, i.e., a continuously growing list of records that mimics the functionning of a traditional ledger, namely transparency and falsification-proof of documentation.

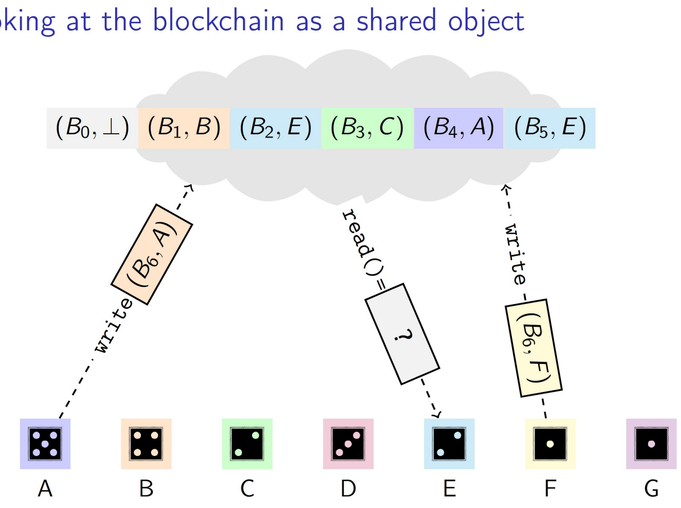


There are several fundamental aspects that require to be understood and studied to safely incorporate the blockchain as the backbone of distributed applications:

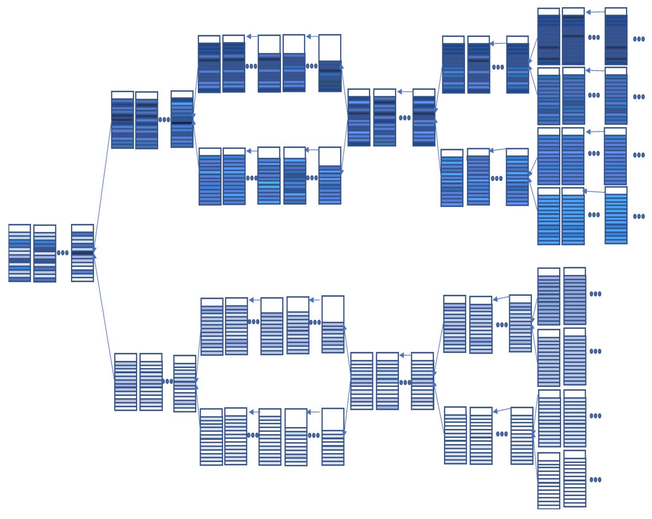
- Formalisation of consistency properties:
  A variety of consistency properties have been attributed to blockchains, ranging from eventual consistency to strong one. These properties need to be formalized and proved so that one can build safe higher-level protocols.
- Scalability issues :
  Blockchain is at heart a consensus algorithm. The presence of reconciliation between nodes due to forks has a direct impact on the speed/security tradeoff on which the regulation of block generation rate is based. Looking in the depth of the blockchain, novel algorithms are needed to noticeably improve transaction throughput, and thus scalability of the blockchain.
- Formalizing the Ethereum Virtual Machine
  As with other virtual machines (notably the Java VM), a mechanised formalization is capable to pinpointing safety and security issues that went unnoticed when designing the language. We will also analyze resource consumption and control flow properties of smart contracts as these are two properties that are essential for guaranteeing that contracts can complete their transactions and that their behaviour cannot be altered by an attacker.

Approaches and results

Looking at the blockchain as a shared object



Sycomore : from a chain of blocks to a DAG of blocks



Partnership

Three teams with complementary expertise are involved in the project: (1) distributed algorithms, (2) formal methods, and (3) distributed systems

Distributed Algorithms

CIDRE/IRISA-INRIA is a team working on distributed algorithms in large-scale distributed systems prone to Byzantine failures. The team has brought its expertise in two aspects of this project: consistency properties and scalability issues of the blockchain technology.

Key persons: Emmanuelle Anceaume, Pierre Wilke, Frédéric Tronel

Formal Methods

CELTIQUE/IRISA-INRIA is a team working on formal methods and their application to the verification of realistic softwares. The team has worked on the formalisation of gas consumption in the Ethereum blockchain framework. Starting from the formal semantics of Ethereum, Celtique has built a mechanized proof that the gas mechanism of Ethereum guarantees that contracts terminates. This property is necessary to ensure that the Ethereum system is free of denial of service.

Key persons: Thomas Genet, Thomas Jensen

students hired within the project: Justine Sauvage

Distributed Systems

Adoptnet/IRISA: is a team dedicated to architectures, protocols and monitoring of networks. The team has brought its expertise with respect to throughput of blockchains protocols. Throughput was studied through to complementary approaches. The first one is related to a alternative ledger internal structure called Sycomore while the second ont is related to lightning, a layer-2 approach, which is similar to BGP.

Key persons: Romaric Ludinard, Géraldine Texier