Modèle formel pour la blockchain

Mots clés : Blockchain, méthodes formelles, assistants à la preuve, algorithmes de consensus distribué, sémantique de langages de programmation, sécurité.

Lieu : Laboratoire IRISA à Rennes, co-encadrement entre les équipes CIDRE (sécurité, blockchain, algorithmes de consensus) et CELTIQUE (méthodes formelles, sémantique des langages de programmation)

Résumé : La blockchain, au coeur de la cryptomonnaie Bitcoin, est une technique permettant de construire un registre d'informations partagé et infalsifiable. Contrairement à ce qui était pratiqué avant Bitcoin, le contrôle de ce registre n'est pas confié à une entité de confiance mais distribué entre à tous ses usagers. Dans Bitcoin, les informations stockées dans ce registre sont simplement des transferts d'argent d'un compte virtuel à un autre. La sécurité de l'ensemble repose sur l'utilisation de signatures cryptographiques et d'algorithmes de consensus distribué garantissant que les pages de ce registre de transferts ne peuvent être falsifiées par un agent malveillant.

Par dessus la blockchain, de nouveaux protocoles ont vu le jour et vont au delà des simples transferts monétaires prévus dans Bitcoin. Dans ces protocoles spécifiques, une large part de la logique du protocole est programmable par l'utilisateur lui-même. On parle alors de protocoles de "smart contracts" (comme Ethereum et Tezos) et de langage de programmation de contrats (Solidity pour Ethereum et Liquidity pour Tezos). Le fait que ces protocoles soient programmables par les utilisateurs multiplie les vecteurs d'attaques et rend leur preuve de sécurité encore plus complexe que dans le cas de Bitcoin.

Avec les équipes CIDRE et CELTIQUE, nous souhaitons construire un modèle formel simple et concis du noyau d'un protocole de smart contract afin d'étudier et de prouver des propriétés de sécurité sur celui-ci.

Objectifs du stage : l'objectif est de comprendre comment interagissent les composants clés des protocoles de smart contracts (les algorithmes de consensus, les primitives cryptographiques, les langages de contrats, etc.) et à quel niveau se placer pour les formaliser de façon pertinente par rapport aux propriétés ciblées : propriétés de consensus, propriétés de sûreté, propriétés de sécurité. Le modèle formel devra être aisément manipulable dans un assistant à la preuve. Un des objectifs est donc de produire une formalisation (Coq ou Isabelle/HOL) du coeur d'un protocole de smart contracts comme Ethereum ou Tezos. Cette formalisation devra être suffisamment fine pour permettre de raisonner sur les propriétés de consensus, de sûreté et de sécurité des contrats et suffisamment générale pour pouvoir être étendue à d'autres protocoles de smart contracts.

Contacts

— `emmanuelle.anceaume@irisa.fr`
— `thomas.genet@irisa.fr`
— `thomas.jensen@irisa.fr`