High-Assurance Blockchains: Applications and Verification

Submitted by Katie Dey on Sat, 03/10/2018 - 1:59pm. Contributors: Joe Hendrix, Dave Archer

BIO
Dr. Joe Hendrix is a Principal Researcher at Galois. His research interests are in the application of automated reasoning techniques to hard computer science and engineering problems. While at Galois, he has contributed to Galois' SAW Verification tools, the Crucible symbolic simulator, and the Macaw binary analysis library.

ABSTRACT
In this presentation, we will describe work at Galois aimed at providing and maintaining data integrity guarantees via blockchains even when systems are compromised, and verifying a blockchain implementation satisfies security and functionality requirements. Blockchain developers have shown an interest in extending blockchains to be useful in context outside crypto-currencies. Making this transition requires both finding suitable use cases that address needs, and in ensuring the proposed blockchain technology can actually deliver on its promises.

In the talk, we will focus on two use cases that we can demonstrate: (1) A user-level filesystem that used a blockchain and Intel SGX to provide tamper resistant event logging; (2) a secure messaging application that records and allows verification of each step of a high throughput message delivery protocol. The latter demonstration takes as input telemetry from a UAV flight simulator and distributes that data through a decentralized messaging middleware to multiple analytic packages that graphically display flight data. Those analytics packages then verify each transport protocol step as the data is displayed.

In our verification efforts, we have focused on an existing blockchain system, namely GuardTime KSI blockchain system, which maintains a hash-based ledger to provide secure timestamping and providence guarantees with a fast transaction time. We used the applications above to derive security requirements on the system, and then used automated reasoning tools to show selected aspects of those requirements.

In particular, we formalized a model of the core Guardtime signing service in the Lean interactive theorem prover. We then proved the temporal property that under specific configuration limits and assumptions of network delivery the system would respond to each signature request with a certificate. From a formal methods standpoint, the work made heavy use of Lean's reflection capabilities to automate proofs within an interactive theorem proving environment even though the proofs were fundamentally about model-checking of infinite state systems.

The main goals of this talk are to provide an overview of the main components in a blockchain system, the guarantees they should provide, and how different techniques and tools developed by the formal methods community can ensure a given system satisfies its requirements. In addition to our work, we would also like to discuss areas where we feel there are gaps in FM tools and cryptographic proofs, and propose ways in which the two communities can work together to address those gaps. In particular, we think there is additional work to be done in model-code correspondence so that proofs about the model can be shown to be true about the implementation, and in developing tools to extend cryptographic proofs, as found in an academic cryptographic paper, to proofs about the underlying distributed network semantics of an implementation.

Additional contributors to our efforts include Ledah Casburn, Joey Dodds, Tom DuBuisson, Simon Hudon, Ben Jones, Alex Malozemoff, and Ben Sherman