Verification of Bitcoin Smart Contracts using the Interactive Theorem Prover Agda

Fahad Alhabardi[1], Anton Setzer, and Bogdan Lazer
Department of Computer Science
Swansea University

August 31, 2021

Smart Contracts

- What are smart contracts?
  Smart contracts are transactions that are defined through software and executed automatically when conditions in the blockchains are met.
- Smart contracts in the crypto currency Bitcoin are written in the language Script .

Bitcoin Script Language

- The scripting language for Bitcoin is stack-based, and similar to Forth.
- The script in Bitcoin has a set of commands called Operation Codes such as OP_HASH160, OP_ ADD, OP_ EQUAL and OP_VERIFY.
- Several standards scripts are used in Bitcoin such as the pay-to-public-key-hash (P2PKH) script.

P2PKH

P2PKH has a locking script (scriptPubKey) and an unlocking script (scriptSig) [1].
For clarity:

- The OP_Codes for scriptPubKey are as follows:

OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- The OP_Codes for scriptSig are as follows:
  <sig> <pubKey>

Hoare triple

We define for $\Phi, \Psi \subseteq \mathrm{State1}$ and p a Bitcoin Script the Hoare triple with weakest pre condition

For the unlocking script of P2PKH we show:

Therefore in order to unlock one needs to provide a script which computes the pubkey hashing to the pbkh and a signature.

Hoare triple

We define for $\Phi, \Psi \subseteq \mathrm{State1}$ and p a Bitcoin Script the Hoare triple with weakest pre condition

$$\begin{aligned}\langle\ \Phi\ \rangle^{\leftrightarrow}\ p\ \langle\ \Psi\ \rangle :\Leftrightarrow \\ (\forall s \in \mathrm{State1}.\Phi(s) \rightarrow \Psi([\![\, p \,]\!]s)) \\ \wedge(\forall s \in \mathrm{State1}.\Psi([\![\, p \,]\!]s) \rightarrow \Phi(s))\end{aligned}$$

For the unlocking script of P2PKH we show:

Therefore in order to unlock one needs to provide a script which computes the pubkey hashing to the pbkh and a signature.

Hoare triple

We define for $\Phi, \Psi \subseteq \mathrm{State1}$ and p a Bitcoin Script the Hoare triple with weakest pre condition

$$\begin{aligned}\langle\ \Phi\ \rangle^{\leftrightarrow}\ p\ \langle\ \Psi\ \rangle :\Leftrightarrow\\ &(\forall s \in \mathrm{State1}.\Phi(s) \rightarrow \Psi([\![\, p \,]\!]s))\\ &\wedge(\forall s \in \mathrm{State1}.\Psi([\![\, p \,]\!]s) \rightarrow \Phi(s))\end{aligned}$$

For the unlocking script of P2PKH we show:

$(\langle\Phi\rangle^{\leftrightarrow}\ \mathrm{scriptSig}\ \langle\mathrm{accept}\rangle)$
$\Longleftrightarrow$ the two top elements of the stack consist of a pubkey hashing to the pbkh and a corresponding signature.

Therefore in order to unlock one needs to provide a script which computes the pubkey hashing to the pbkh and a signature.

Thank you for listening.


Bitcoin Community.
Welcome to the Bitcoin Wiki.
Availabe from https://en.bitcoin.it/wiki/Bitcoin, 2010.