Hash Time Lock Contract Analysis

Using Tamarin

Shuang Wu

NTNU

Abstract

1. What Blockchain is?
2. Cross-chain Trading
3. Hash time lock contract
4. Tamarin

What is Blockchain?

Blockchain is a growing list of records, called blocks. Each block contains the hash value of the previous block, a timestamp, transactions information and some other parameters.

- Decentralised
- Immutable

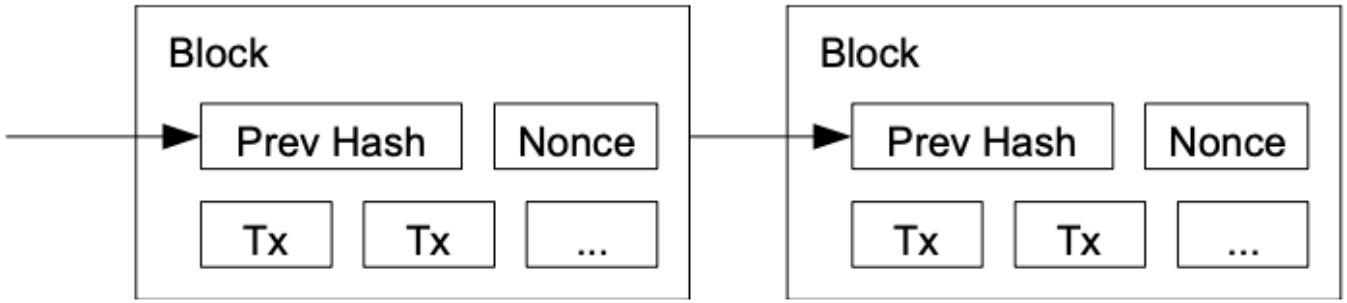
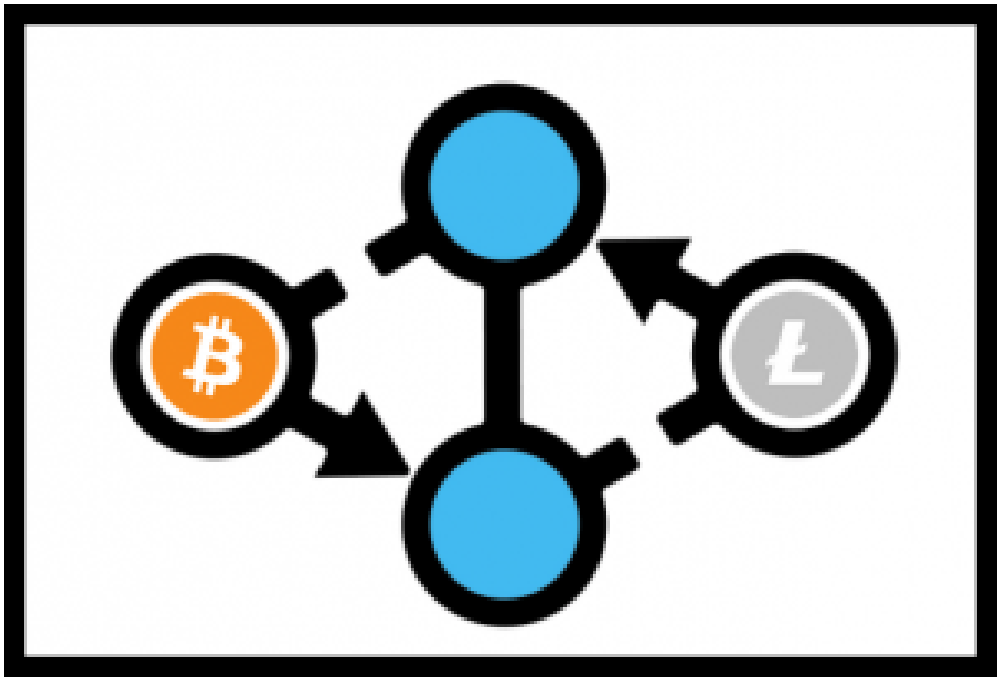


Figure: Blockchain

Cryptocurrencies

Cross-chain trading



Cross-chain trading

Exchanging different cryptocurrencies

- Decentralise : without trusting anyone.
- Atomic swap: no one will lose money if he follows the protocol honestly.

The Hash time lock contract is a protocol to achieve atomic swap in a decentralised way.

Cross-chain trading

Existing projects:

- Interledger
- Lightning network
- ...

Figure: Lightning networking

Figure: Interledger

Hash Time Lock Contract

Key point: add two obstacles to the normal transactions.

- Hash Lock: Restrict an output of a transaction can only be spent when the pre-image of the hash value is revealed.
- Time Lock: Restrict a transaction which can only be appended on the blockchain after a specific time period.

Hash Time Lock Contract

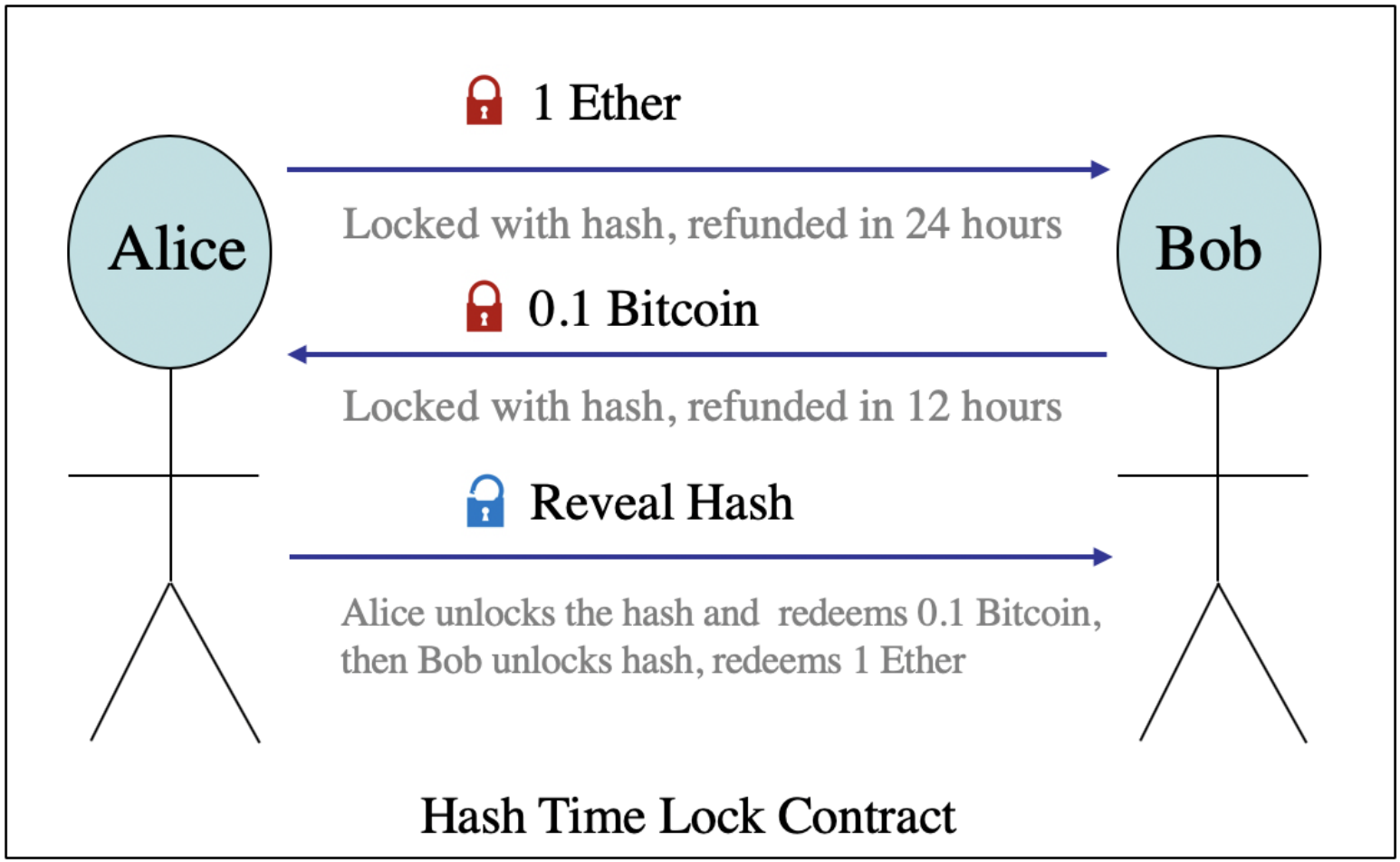


Figure: HTLC

Hash Time Lock Contract

Alice:

1. Transaction 1:
   Alice sends 1 Ether to Bob, lock with h.

Hash Time Lock Contract

Alice:

1. Transaction 1:
   Alice sends 1 Ether to Bob, lock with h.
2. Transaction 2:
   Alice redeems the Transaction 1 after 2 days
   $< SigAlice >< SigBob >$

Hash Time Lock Contract

Alice:

1. Transaction 1:
   Alice sends 1 Ether to Bob, lock with h.
2. Transaction 2:
   Alice redeems the Transaction 1 after 2 days
   $< SigAlice >< SigBob >$
3. Alice broadcast the first transaction on Ehereum blockchain.

Bob:

1. Transaction 3: send 0.1 Bitcoin to Alice, lock with h

Hash Time Lock Contract

Alice:

1. Transaction 1:
   Alice sends 1 Ether to Bob, lock with h.
2. Transaction 2:
   Alice redeems the Transaction 1 after 2 days
   $< SigAlice >< SigBob >$
3. Alice broadcast the first transaction on Ehereum blockchain.

Bob:

1. Transaction 3: send 0.1 Bitcoin to Alice, lock with h
2. Transaction 4: Bob redeems TX3 after 1 day
   $< SigAlice >< SigBob >$

Hash Time Lock Contract

Alice:

1. Transaction 1:
   Alice sends 1 Ether to Bob, lock with h.
2. Transaction 2:
   Alice redeems the Transaction 1 after 2 days
   $< SigAlice >< SigBob >$
3. Alice broadcast the first transaction on Ehereum blockchain.

Bob:

1. Transaction 3: send 0.1 Bitcoin to Alice, lock with h
2. Transaction 4: Bob redeems TX3 after 1 day
   $< SigAlice >< SigBob >$
3. Bob broadcasts the third transaction to Bitcoin blockchain.

Tamarin

The Tamarin prover is a security protocol verification tool that supports both falsification and unbounded verification in the symbolic model.

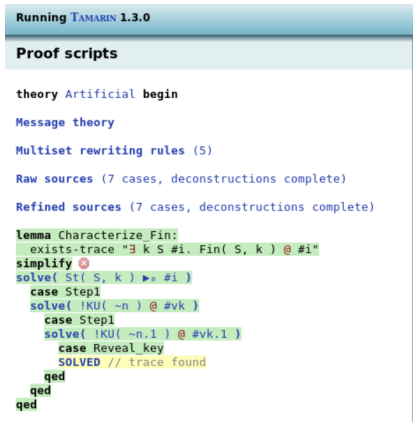


Figure: Tamarin user interface

How to use it?

1. Rewrite your protocol using the Tamarin language.
2. Specify your security properties.
3. Let Tamarin prove it!

Tamarin

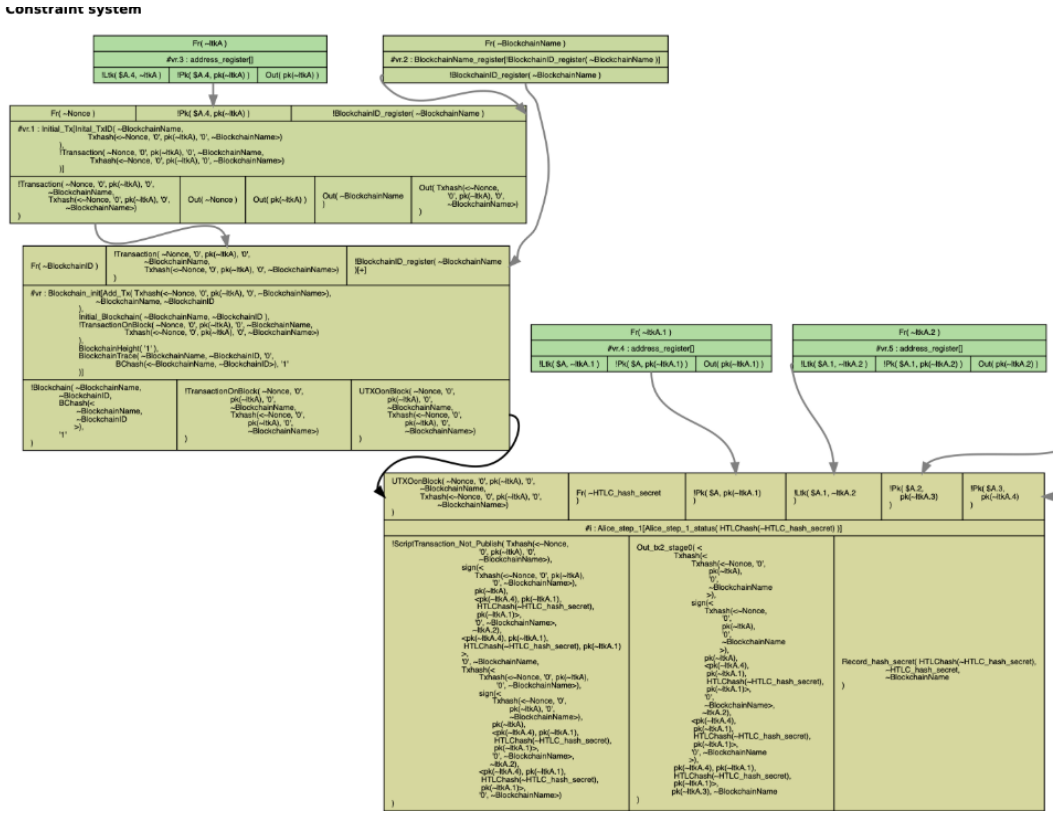


Figure: Tamarin graphic analysis

1

Thank You!