Monero

Parser

PA193 Term Project

Adam Janovský
Kristián Kozák

Intro: Monero Principles

Privacy
Hide source with ring signatures
Hide destination with one-time transaction keys

Smooth payments and emission
Lower inertia, regular block rate
Smoother block rewards

Intro: Transactions

Input

Foreign (fake) inputs

Ring signature over the inputs

Key image — to prevent double spending

Output

Unique transaction key(s)

1st part of receiver's key: Recognize his transactions

2nd part of receiver’s key: Access the funds

Resources & Challenges

Whitepaper + Reviews
CryptoNote standard

Monero code
Not many comments or docs
Not very readable

Tools on top of Monero
Usually do not compile with current Monero version

Resources & Challenges

```
/* I have no clue what these lines mean */
```

```
// This one just fails when you call it.... Okay
```

— Authors of Monero, 2017

Blochain DB

Blocks
Block header
Miner transaction (emission of Monero)
Hashes of other transactions

Transactions
Inputs & Outputs
Amounts
Spent keys

Block Structure

Block header
Version(s)
Timestamp
Previous ID
Nonce

Miner Tx
Version 1 or 2
Unlock time
Input: Gen
Ouput(s)
Extra

Tx hashes
Hash vector

Block validation

1. Hash miner transaction (txn version 1 or 2?)
2. Hash all transaction hashes in Merkle tree
3. Concatenate block header with the root hash and hash it

Implementation

De/serialization
Skip / deserialize variable length integers

Hashing
Miner transaction hash
Merkle tree hash
Block hashing structure

Block & Parser classes
Load, recognize & check block structure

Implementation cont.

Time
Understanding Monero: 65 %
Actually coding and testing: 35 %

Priorities
Simple and understandable code
Good documentation
Standard constructs & containers / avoid dynamic alloc

Tools

Static analysis: **cppcheck**

Dynamic analysis: **Valgrind**

Testing: **GoogleTest** + **Run all blocks from blockchain**

(200k validations / min)

Fuzzing: **Radamsa**

Summary

Outcomes
Fast and reliable validator
Block hashes validated, transactions not

Lessons
Privacy is complicated
Comments and docs are important