Practical Guide of Smart Contracts

Smart Contract Japan

Published with GitBook

Table of Contents

Purpose of the book

The book intends to provide practical guide with a lot of images and diagrams about Smart Contract. Smart Contract itself evolving ideas, and there are seldom to see real-smart contract implementation. The reason is from Bitcoin's transaction malleability, and Ethereum is now alpha release status.

So on the book, the details will be changed more or less in each protocols in the future. However general landscape of Smart contracts won't change so much, it allows us to build reliable online apps and infrastructure on decentralized technologies.
From 2009, the disruptive innovation of Bitcoin, we can see the real implementation even if it's not secure. The idea is started from the Nick Szabo's http://szabo.best.vwh.net/smart_contracts_idea.html and populated by Vitalik Buterin's Ethereum whitepaper https://github.com/ethereum/wiki/wiki/White-Paper

The book's main purpose is to provide information about smart contracts with real-use-cases.

Coverage of smart contracts on platforms (On 31th August 2015)

1. Bitcoin
2. Ethereum

Coverage of smart contracts

1. Bitcoin (Lighthouse, Crowdfunding contract)
By using Lighthouse from GUI and read the source code, then guide how the crowdfunding contract works. Mainly about SIGHASH_ANYONECANPAY.

2. Bitcoin (Reality Keys, contract with centralized oracle)
With RealityKeys Example. we will see how the Smart contract with Oracle information works.

3. Bitcoin (OpenBazaar, Trade protocol using Ricardian Contracts)
There are 2 types of smart contracts on Bitcoin. one is the Escrow contracts and the other is Ricardian contracts, which records an agreement between multiple parties which proves what you want contracts as a digital document. https://github.com/OpenBazaar/OpenBazaar/wiki/03.-OpenBazaar-Protocol#32-trade-protocol We will show both of the contracts usage and the source code notation with diagram and screenshots.

4. Bitcoin (Coinprism, Ricardian contracts)
By using Coinprism's smart contracts, user can atomically swap the Bitcoin and coloredcoins by Openassets protocol. We do the crowdsale, buy it, and exchange atomically between Bitcoin and coloredcoin.

5. Bitcoin (Streamium, Micro payment channel contract for online video subscription)
In Streamium, user can pay as you go style video streaming service.The mechanism using Micropayments system, called Micropayment channel. Once the channel opened between viewer and host, don't have to propagate every micro-payment to Bitcoin network. We describe the system with diagrams and images.

6. Bitcoin (LightningNetwork, Micro payment channel, HashLock and TimeLock contract)
Coupling Micro payment channel idea with HashLock, and TimeLock contract, then every transaction can be done by offchain. http://lightning.network/lightning-network.pdf We will see the source code and explain what's happening in source code level.

7. Bitcoin (Darkwallet, Stealth address, CoinJoin)
Darkwallet enables you to receive payments unlinked, hidden total receive balance way, and send Bitcoin by probabilistically unlinkable way. We see how it works.

8. Bitcoin (CrytpoNote, Ring Signature)
Crytponote's ring signature hides the sender by hiding signer as one of many signers in the transaction. Ring transaction can be signed by anybody in the ring, therefore it's impossible to say a person is 100% sender of the transaction.

9. Ethereum (Etherex, decentralized exchange)

10. Ethereum (Augur, prediction market, serpent logrithmatic market scoring rules.)

11. Ethereum (Atomic_cross_chain_trading,)
Ether-Bitcoin atomic swapping. And also covering the Bitcoin smart contract Ethereum: https://github.com/zack-bitcoin/ethereum-atomic-swap.git
Bitcoin(and original idea): https://en.bitcoin.it/wiki/Atomic_cross-chain_trading These protocols we will use and report.It can be also used for coloredcoin transactions with many implementations, (counterparty, coinprism, coloredcoins.org)

Landscape applications

First Chapter

GitBook allows you to organize your book into chapters, each chapter is stored in a separate file like this one.

Chapter 2. Bitcoin (Reality Keys)

// Updated 2015.09.19 by Edmund Edgar

Abstract

Using Bitcoin's scripting language and an oracle service like Reality Keys for external data sources, you lock up funds in a multi-signature contract so that the person who can spend it depends on an external event.

Multi-signature transactions

The simplest form of bitcoin payment specifies a public key, and locks up funds such that they can only be spent if you can sign with the private key corresponding to that public key.

In the bitcoin scripting language, this is expressed as follows:

Bitcoin allows us to lock up funds such that they require multiple keys to spend them. To require `Alice`'s signature to spend funds this is expressed as follows:

```
A-pub OP_CHECKSIG
```

This is spent by providing a signature, resulting in:

```
A-sig A-pub OP_CHECKSIG
```

The above returns true if `A-sig` is a correct signature for `A-pub`.

Bitcoin can also require signatures for multiple keys before funds can be spent. To require signatures from both `Alice` and `Bob`:

```
2 A-pub B-pub 2 OP_CHECKMULTISIG
```

This is spent by providing two valid signatures, preceded (for obscure legacy reasons) by a null value.

```
0 A-sig B-sig 2 A-pub B-pub 2 OP_CHECKMULTISIG
```

Using keys to represent facts

Usually both of the signatures are signatures representing people. But they can also represent facts.

Reality Keys issue keys representing things happening in the world. Suppose Alice wants to lock up funds that can only be spent if she runs 1000 meters. She hits the Reality Keys API to request a public key representing "Yes, Alice ran 1000 meters". Reality Keys can track this information using RunKeeper, who get the data based on the GPS on Alice's phone.

The transaction will look like the previous example, but instead of Bob's key, we will use the "Yes, she ran" key from Reality Keys.

```
2 A-pub RK-yes-pub 2 OP_CHECKMULTISIG
```

Since Reality Keys will only release private key corresponding to `RK-yes-pub` if Alice successfully completes her run, this has the effect of locking up her money so that it will be unspendable unless she completes the run successfully.

She may want someone else - say Bob - to be able to get the funds if she does not complete the run. Reality Keys also releases a key representing, "No, Alice did not run".

`2 B-pub RK-no-pub 2 OP_CHECKMULTISIG`

The above two options can be combined into a single script:

```
OP_IF
2 A-pub RK-yes-pub 2 OP_CHECKMULTISIG
OP_ELSE
2 B-pub RK-no-pub 2 OP_CHECKMULTISIG
OP_ENDIF
```

The above is spent in the same way as a either of the branches on its own would be spent, except that you add an extra `1` or `0` after the signatures to direct the script interpreter to one or the other of the branches. If Alice is trying to claim her funds after a successful run, she would supply `1` and the first branch would be evaluated. If Bob is trying to claim funds after Alice failed to complete her run, he would supply `0` and the second branch would be evaluated.

Putting it into practice

Chapter 3. Bitcoin (OpenBazaar)

// Updated 2015.10.03 by Tomoaki Sato

Abstract

Bitcoin smart contract enables you to get

About Open Bazaar

Open Bazaar contract template by

```
{
   "vendor_offer" : {
      "listing" : {
         "metadata" : {
            "version" : "",
            "expiry" : "",
            "category" : "",
            "category_sub" : "fixed price"
         },
         "id" : {
            "guid" : "",
            "pubkeys" : {
               "guid" : "",
               "bitcoin" : ""
            },
            "blockchain_id" : ""
         },
         "listing" : {
            "title" : "",
            "description" : "",
            "condition" : "",
            "price_per_unit" : {
               "bitcoin" : "",
               "fiat" : {
                  "price" : "",
                  "currency_code" : ""
               }
            },
            "item_properties" : "",
            "quantity" : {
               "metric" : "",
               "units" : 1
            },
            "category" : [ "" ],
            "image_hashes" : [ "" ],
            "keywords" : [ "" ],
            "process_time" : {
               "metric": "",
               "units" : 1
            },
            "sku" : ""
         },
         "shipping" : {
            "free" : false,
            "flat_fee" : {
               "bitcoin" : {
                  "domestic" : "",
                  "international" : ""
               },
               "fiat" : {
                  "price" : {
                     "domestic" : "",
                     "international" : ""
                  },
                  "currency_code" : ""
                  }
               },
               "shipping_region" : {
                  "domestic" : {
                        "country" : "",
                        "city_state" : [ "" ]
                     },
                  "international" : [ "" ]
               },
               "est_delivery" : {
                  "domestic" : "",
                  "international" : ""
               },
               "shipping_origin" : "",
               "api" : {
                  "api_src" : "",
                  "carriers" : [ "", "" ],
                  "package" : {
                     "length" : "",
                     "width" : "",
                     "height" : "",
                     "distance_unit" : "",
                     "weight" : "",
                     "mass_unit" : ""
                  }
               }
            },
            "policy": {
               "terms_conditions": "",
               "returns": "",
               "custom": []
            },
            "moderators" : [
               {
                  "guid" : "",
                  "pubkeys" : {
                     "guid" : {
                        "key" : "",
                        "signature" : ""
                        },
                     "escrow" : {
                        "key" : "",
                        "signature" : ""
                        }
                  },
                  "blockchain_id" : ""
               }
            ]
         },
         "signatures" : {
            "guid" : "sig(vendor_listing.listing)"
         }
      },
      "buyer_order" : {
         "order" : {
            "ref" : {
               "algorithm" : "base58(RIPEMD-160[vendor_listing])",
               "ref_hash" : ""
            },
            "id" : {
               "guid" : "",
               "pubkeys" : {
                  "bitcoin" : "",
                  "guid" : ""
               },
               "passcard" : ""
            },
            "order" : {
               "item_properties" : {},
               "shipping_address" : {
                  "encrypted_address" : "guid(nonce XOR shipping address)",
                  "sha256_nonce" : "sha256(nonce)",
                  "nonce_enc" : "vendor_guid(nonce)",
                  "api_shipping_cost" : {
                     "bitcoin" : "",
                     "fiat" : {
                        "price" : "",
                        "currency_code" : ""
                     }
                  }
               },
               "service_address" : {
                  "encrypted_address" : "guid(nonce XOR service address)",
                  "sha256_nonce" : "sha256(nonce)",
                  "nonce_enc" : "vendor_guid(nonce)"
               }
            },
            "multisignature" : {
               "chaincode" : "",
               "vendor_sig" : "",
               "redemption_script" : "",
               "txid" : ""
            }
         },
         "signatures" : {
            "guid" : "sig(buyer.order)"
         }
      },
      "vendor_order_confirmation" : {
         "invoice" : {
            "ref" : {
               "algorithm" : "base58(RIPEMD-160[buyer_order])",
               "ref_hash" : ""
            },
            "shipping" : {
               "tracking_id" : "",
               "shipper" : "",
               "payout" : {
                  "payout_address" : "",
                  "signed_tx" : ""
               },
               "rev_est_delivery" : ""
            },
            "pickup_address" : {
               "encrypted_address" : "bitcoin_ecc(nonce XOR pickup address)",
               "sha256_nonce" : "sha256(nonce)",
               "enc_nonce" : "buyer_bitcoin_ecc(nonce)"
            },
            "content_source" : {
               "enc_url" : "bitcoin_ecc(nonce XOR URL)",
               "enc_password" : "bitcoin_ecc(nonce XOR password)",
               "nonce_url_sha256" : "sha256(nonce_url)",
               "nonce_password_sha256" : "sha256(nonce_password)",
               "nonce_url_enc" : "buyer_bitcoin_ecc(nonce_url)",
               "nonce_password_enc" : "buyer_bitcoin_ecc(nonce_password)"
            },
            "comments" : ""
         },
         "signatures" : {
            "guid" : "sig(vendor_invoice.invoice)"
         }
      },
      "buyer_receipt" : {
         "receipt" : {
            "ref" : {
               "algorithm" : "base58(RIPEMD-160[vendor_invoice])",
               "ref_hash" : ""
            },
            "listing" : {
               "received" : true
            },
            "payout" : {
               "signed_tx" : "",
               "txid" : ""
            },
            "rating" : {
               "feedback" : 0,
               "quality" : 0,
               "description" : 0,
               "delivery_time" : 0,
               "customer_service" : 0,
               "review" : ""
            },
            "dispute" : {
               "dispute" : false,
               "claim" : ""
         }
      },
      "signatures" : {
         "guid" : "sig(buyer_receipt.receipt)"
      }
   }
}
```