Elements Deep Dive

Day 1: Federated Pegs, Command-line Usage

Gregory Sanders

Blockstream Tech Engineer

Confidential Assets Team Lead

Elements Blockchain Platform maintainer

Core Contributor

サイドチェーン
Sidechains

サイドチェーンのホワイトペーパーは2014に公開した

主に「マージ・マインされた」のサイドチェーンであり、マイナーはペグインされたコインの管理人とサイドチェーンの履歴を確定する役割を持つ。”DMMS” : ダイナミックなメンバーの複数当事者の署名のこと。サイドチェーン上のコインの所有権はBitcoin上の完全に検証しているクライアントによって追跡されない。

Sidechains whitepaper published 2014

Dealt primarily with “Merge-mined” sidechains, where miners are in essence custodians of the pegged-in funds and determine sidechain history. “DMMS”: Dynamic Membership Multiparty Signature. Chain of custody of coins in sidechain not tracked by fully-validating clients in Bitcoin.

付録A (Federatedペグ)
Appendix A (Federated Pegs)

Bitcoinのフルノードクライアントはサイドチェーンのコイン履歴を検証しない（前で説明した事と同じ）

置き換えると:

DMMS ➔ OP_CHECKMULTISIGVERIFY
チェーン履歴:マイナー ➔ ブロック・サイナー（blocksigners）
コインの管理:マイナー ➔ ウォッチメン（watchmen）

Bitcoin full node clients do not validate coin history of the sidechain(just like before)
Replace:
DMMS -> OP_CHECKMULTISIGVERIFY
Chain history: Miners -> “blocksigners”
Coin Custody: Miners -> “watchmen”

ブロック・サイン
Blocksigning

nBitsは無くなった

「チャレンジ」: scriptPubKey

「ソリューション」: scriptSig

nBits gone

“Challenge”: scriptPubKey

“Solution”: scriptSig

ペグ・イン
Peg In

1) サイドチェーンのアドレスを作成する
2) それぞれのpubkeyに対してfedRedeemScript(マルチ・シグ scriptPubKey)を使う:
    a) pubkeyをハッシュする
    b) サイドチェーンのアドレスのpubkeyをハッシュする
    c) 古いpubkeyは新しい変更されたpubkeyに置き換える
3) Bitcoinのp2shのアドレスを出力する（自分しか分からない）
4) アドレスにbitcoinを送金する
5) claimpegin: 先の「変更」をウォッチ・メンを含むサイドチェーンのユーザに公開する
6) ウォッチ・メンはその資金を管理する

1) Create sidechain address
2) Take fedRedeemScript(multisig scriptPubKey), for each pubkey:
    a) Hash pubkey
    b) Hash sidechain address pubkey
    c) replace old pubkey with new tweaked pubkey
3) Output Bitcoin p2sh address (unknown to anyone but yourself)
4) Send bitcoin to address
5) claimpegin: Reveals “tweak” to sidechain users, including watchmen
6) Watchmen then manage those funds

ペグ・アウト
Peg Out

1) Bitcoinのアドレスを作成する
2) サイドチェーンのコインをロックして、Bitcoinのアドレスに送金を依頼する
3) ウォッチ・メンはそのペグ・アウトの依頼を見て、送金する

1) Create Bitcoin address
2) Lock sidechain coin, requesting money to go to Bitcoin address
3) Watchmen see the pegout request, sends

elements.conf

contrib/assets_tutorials/elements1.conf

fedpegscript=5121<pubkey>51ae

signblockscript=5121<pubkey>51ae

validatepegin=1

mainchainrpcport=<port>

mainchainrpcuser=<user>

mainchainrpcpassword=<password>

Questions?

質問？

Let’s Dive In

早速やって見ましょう！