Blockchain Core Camp

最新の課題

@ DG Lab - Anditto Heristyo

Agenda

1. ここまでの話
2. 最新の情報

ここまでの話

BC2のテーマ

1日目：基礎の理解

2日目：現在の改善（Layer 2 Technology）

3日目：将来について

最新の情報

最新情報の収集

カンファレンス: https://scalingbitcoin.org/

メーリングリスト:
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/

Github: https://github.com/bitcoin/bitcoin

または IRC と Slack。

最新の課題

色々課題がありますが、少しだけ紹介します。

Scalability

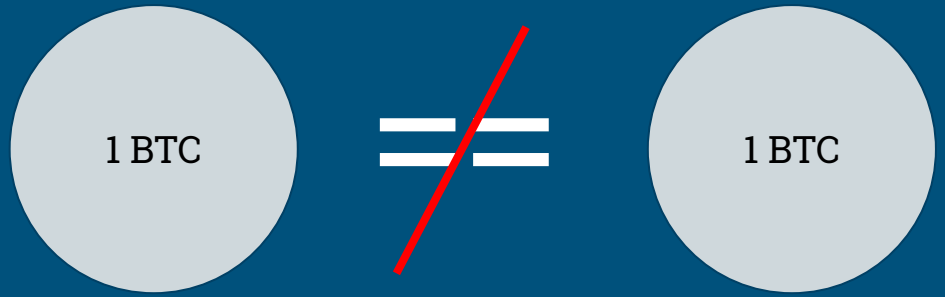
- 現在は 7 Tx / s
  - Visa 平均 2000 tps、ピークは 4000 tps

最近の解決方法 :

SegWit, Lightning Network

Fungibility

“Fungibility”とは何ですか？



1abcde....　　1zyxwv....

Fungibility

https://scalingbitcoin.org/milan2016/presentations/D1%20-%201%20-%20Adam%20and%20Matt.pdf

なぜ必要？

1. Bitcoin == 現金　は目標
2. 皆が繋がっている→他人の行動が自分に影響する
3. 使えないBTCは価値が無い→システムが崩れる

Fungibility

1. BTCの解析会社
   a. Tx Flow Graph 解析（4-hopまで出来るそう）
   b. Tx の送信元の解析
   c. Address Re-use / 再利用（**注意！**）
   d. ウォレットの特徴の解析
2. エクスチェンジのKYC (Know Your Customer)
   a. 自分のウォレットとして使っている（**注意！**）

最近の解決方法

Address 再利用問題:

- HD Wallet (BIP 32)

最近の解決方法

Tx グラフの解析（TxInとTxOutのプライバシー）問題：

- CoinJoin
- TumbleBit
- Lightning Network

最近の解決方法

ウォレットの特徴の解析問題：

- コインの選び方
- Scriptの使い方

→ ウォレットによってアルゴリズムに特徴がある

それ以外もまだ問題がある

Simple Payment Verification (SPV) Wallet

全てのブロックデータを持たずに、ブロックヘッダーしか依頼しない。

- 100ギガ以上じゃなくて、約50メガ
- bitcoin-qt 以外のワレットは大体SPV、又はSPVより　セキュリティが低い
- SPVはリスクがあります

フルウォレット(フルノード)の動き

- ブロックをダウンロードと保存
- 全ての取引を確かめる
- 自分のアドレスを探します
- 自分のアドレス見つけたら、UTXOのDBに入れる
- UTXOが消えたら、DBから消える

SPV ウォレットの動き

- 80バイトのheaderだけダウンロードする
- Bloom filterをフールノードに送って

https://ja.wikipedia.org/wiki/ブルームフィルタ

- 自分のアドレスが入ってる取引だけをダウンロードする
- 数メガだけかかる

SPV ウォレット

- ネットワークのルール守れない
  - 例えば、ルール以上のコインを作る
- 署名をverifyするのは出来ない
  - 前の取引持ってない;署名と前の鍵が合ってる？
- 繋がてるフルノードが色々分かっちゃう
  - 特に自分のアドレス
- 未確認の取引は全く意味ない

まとめ

- Layer 2 の技術(Lightning, TumbleBit, など)はFungibilityの実現とScalabilityの向上にすごく良いこと
- 技術は色々出てきていますので「実施」と「利用」を増やしましょう
- まだ色々課題がありますので、皆の協力も期待している！

anditto@dglab.com
github.com/anditto