Bitcoin as a Platform

@ DG Lab - Anditto Heristyo

Agenda

1. Bitcoin の拡張
2. 実例
    a. Open Assets
    b. Altcoins
    c. Sidechains
    d. TumbleBit

Bitcoin の拡張

Bitcoin上で何を作る？

- Smart Contract (MultiSig アドレス)
- Altcoin (Namecoin)
- Digital Asset (Open Assets/Colored Coin)
- …

Bitcoin上で何を作る？

今日までみたのは:

- Script
- RPCのAPI

Scriptの場合

OP_RETURN の後に任意のデータを入れられる。

課題：

- そもそもBitcoinの目的はそういうことじゃ無い
- 普通のデータだったら、他のDBの方が安い

Bitcoinの現状

1. ScalabilityとdecentralizationのトレードオフⅠ
2. 新しい技術を統合するには、ほぼ全員の賛成が必要
3. セキュリティのため、Scriptの機能は少ない

実例

Open Assets, Altcoins, Sidechains, TumbleBit

Open Assets

https://github.com/OpenAssets/open-assets-protocol

Bitcoin上で仮想通貨以外のアセット作成と送信

Bitcoin上での追加情報:

- Asset ID
- Asset Quantity (正数)

https://www.coinprism.info/assets

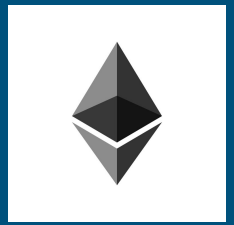
Altcoins

1. Bitcoinとともに動く

   Namecoin, Rootstock, ...

2. 完全に別のネットワーク

   Litecoin, Dogecoin, Ethereum, ...



Altcoinの問題点

1. 参加者とマイナーにとって、リスクが高い
2. Bitcoin の fork だとしたら、バグもコピーされるかも
3. 別の技術を使うと作業が重なったり無駄になったりする

解決方法：

- Merge-mining
- Sidechain

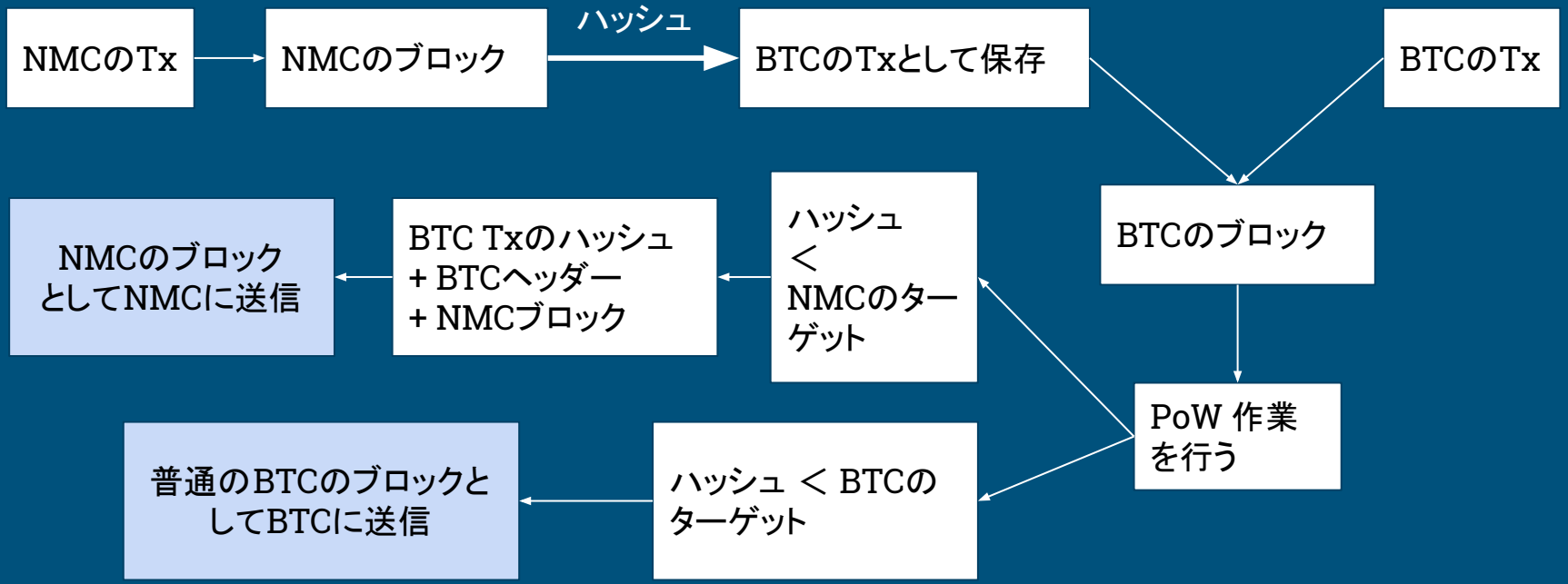
Merge-mining

Bitcoinのブロックをマイニングすると同時に
Altcoinをマイニングする。

→

同じPoWを使う。

Merge mining 例（Namecoin/NMC）



http://bitcoin.stackexchange.com/questions/273/how-does-merged-mining-work

Merge mining のメリット

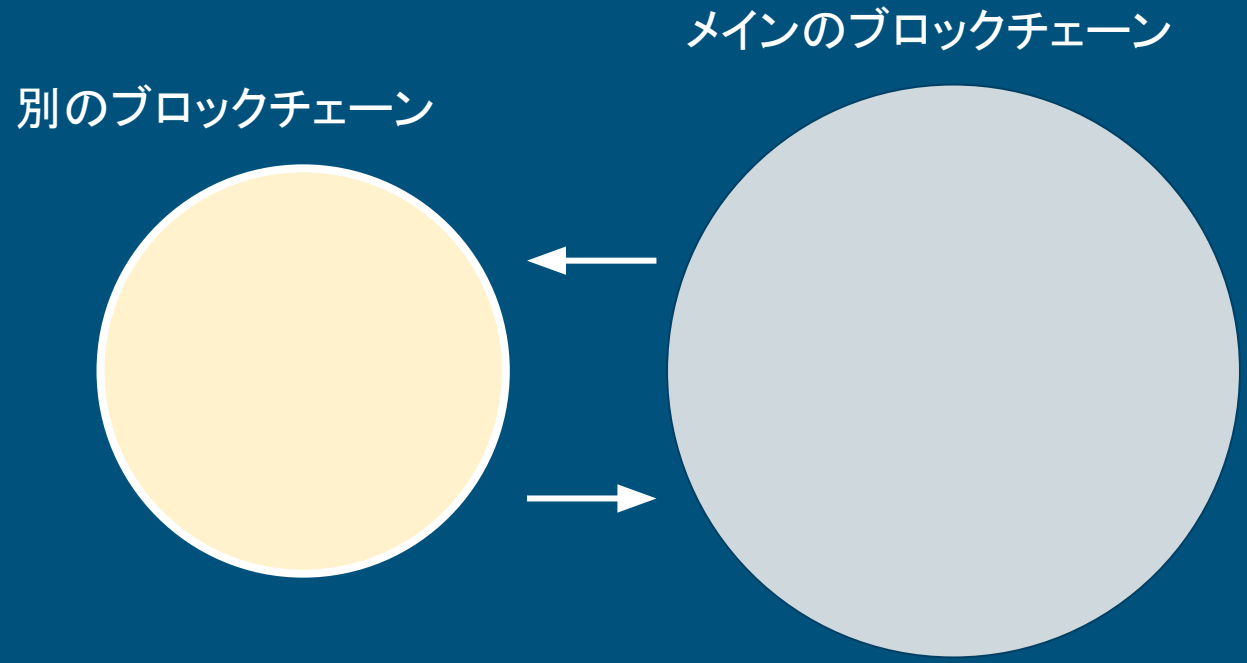
- マイナーの作業のコストはあまり上がらない
- AltcoinはBitcoinのPoWで完全性を守れる
- BitCoinのブロックに影響がほとんど無い

Sidechains

https://blockstream.com/technology/sidechains.pdf

https://elementsproject.org/sidechains/

Sidechains



Sidechainのメリット

先ほどの現状のBitcoinの問題を解決出来る:

- Bitcoinは今のままで、技術的なイノベーションが可能になる
- Bitcoinのセキュリティィに基づいてAltcoinを作れる

TumbleBit

https://github.com/BUSEC/TumbleBit

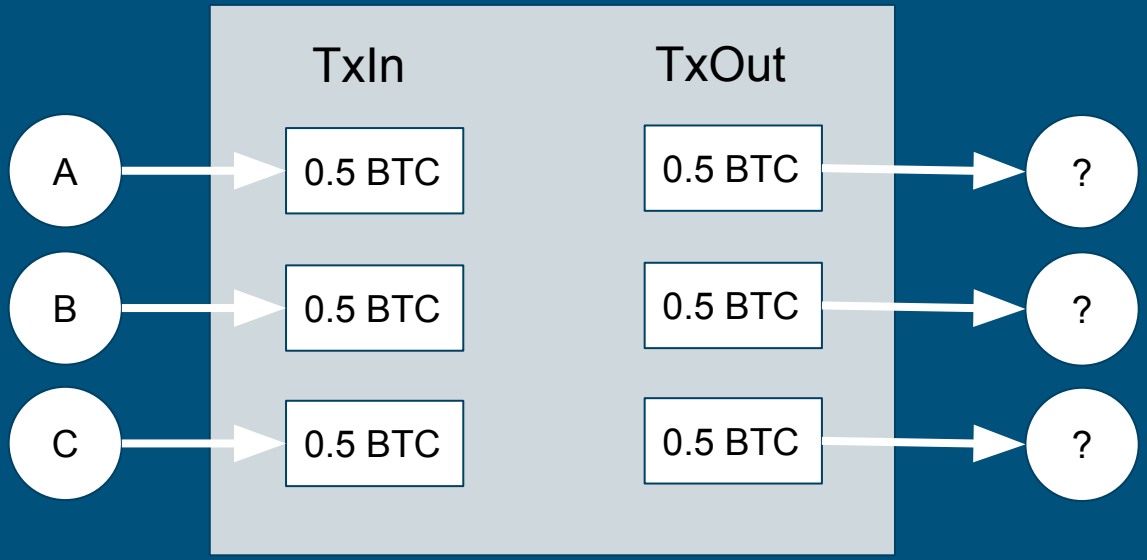
問題点 :

Bitcoinの匿名性 (Fungibility)

解決方法 :

Tumbler

TumbleBit



「Mixingをする人の信頼性と匿名性」を解決

後ほど説明がある

- Segregated Witness (SegWit)
- Lightning Network

anditto@dglab.com
github.com/anditto