コンセンサスと Orphan Block

@ DG Lab - Anditto Heristyo

Agenda

1. コンセンサス
2. Orphan Block
3. デモ

コンセンサス

目的

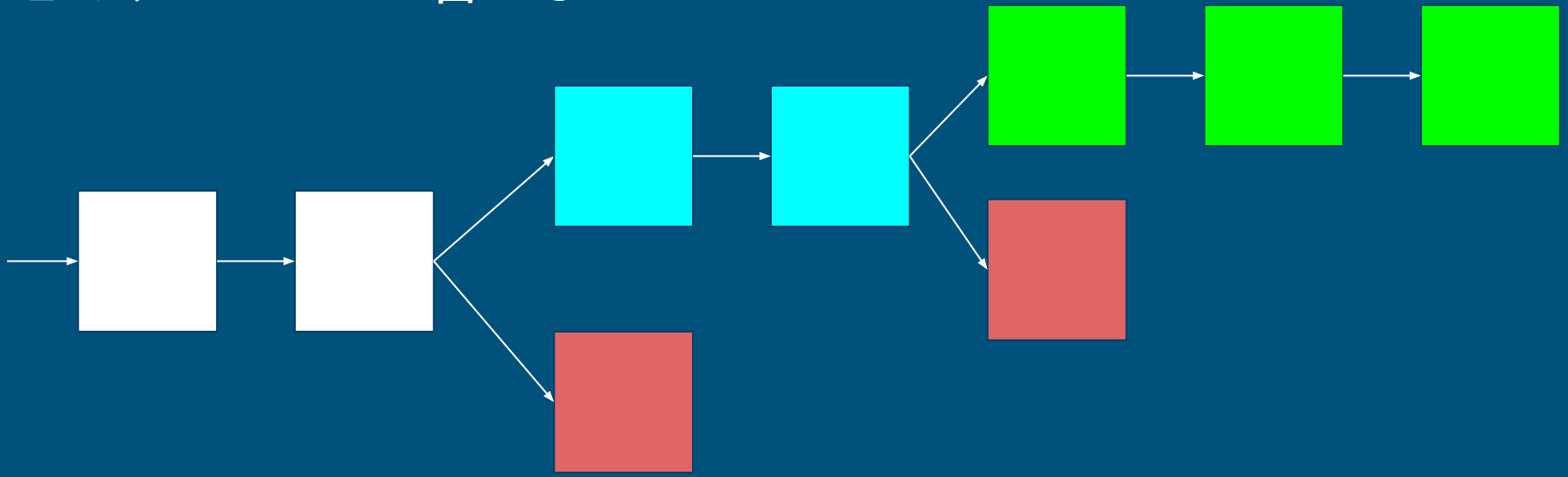
皆が同じブロックを持つこと。

問題点：

1. ビザンチン将軍問題
2. ネットワークの遅延
3. 悪意

コンセンサス

どのチェーンが一番正しい？



基本的に：**一番作業された**チェーン（一番長いとは限らない）

Orphan Block

Orphan Blockとは？

実は少し複雑：

1. 無効になったブロックを親としてマイニングした。
   （Stale Blockとも言われる）
2. 親が見当たらないブロックをもらった。
   （最近あまり無い）

http://bitcoin.stackexchange.com/questions/5859/what-are-orphaned-and-stale-blocks
(Peter Wuille)

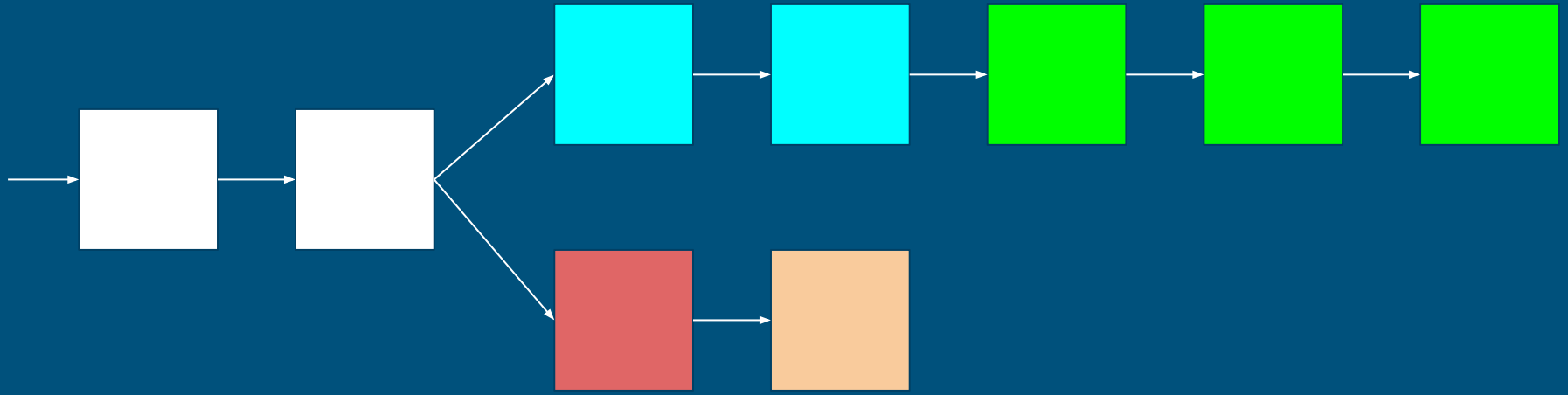
Stale Block

実例：https://blockchain.info/orphaned-blocks

前は有効だったブロックを親として作業している間に、そのブロックが無効になってしまった。

Fork

ブロックチェーンの状態が分岐し不一致となる状況



Soft Fork vs. Hard Fork

Soft Forkの場合 :

もっと厳しいルールを適応する。

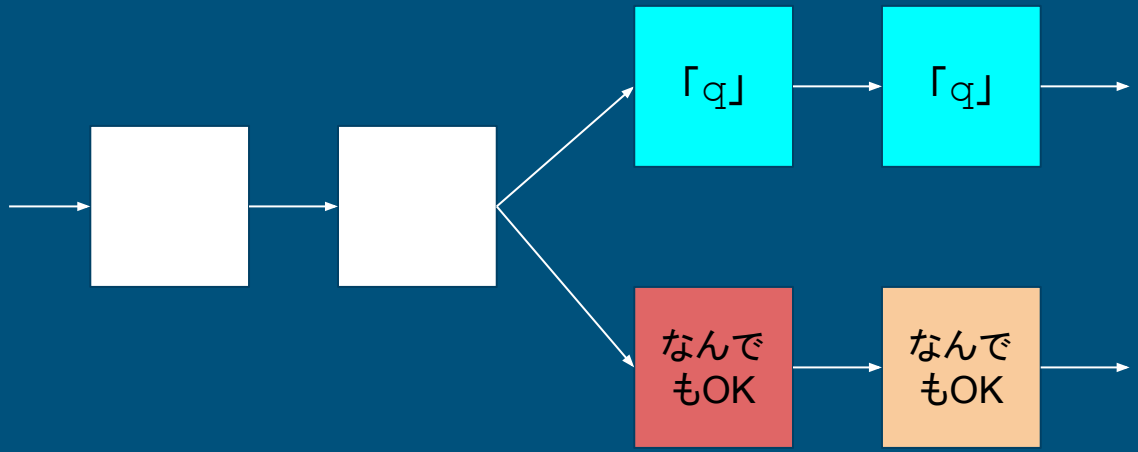
Hard Forkの場合 :

前のルールを消す。

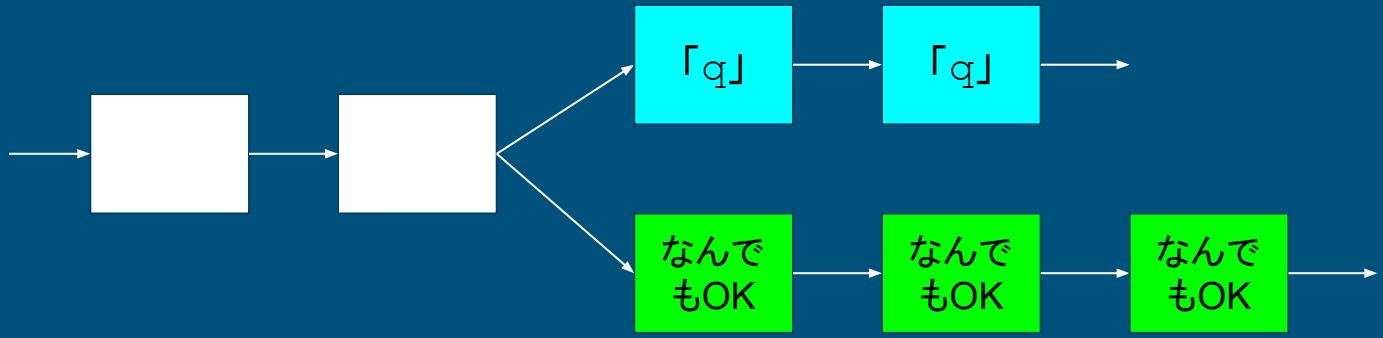
Soft Forkの例

例えば:

アドレスは全部「q」で終わらないと有効じゃない。

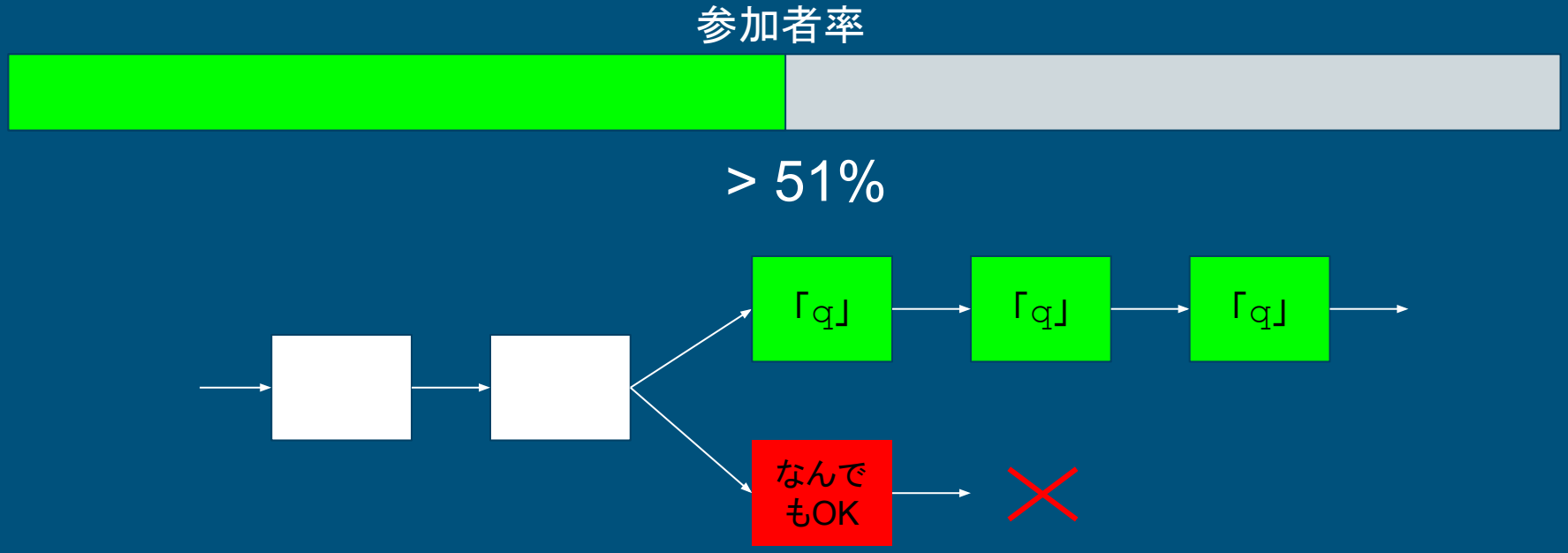


Soft Fork



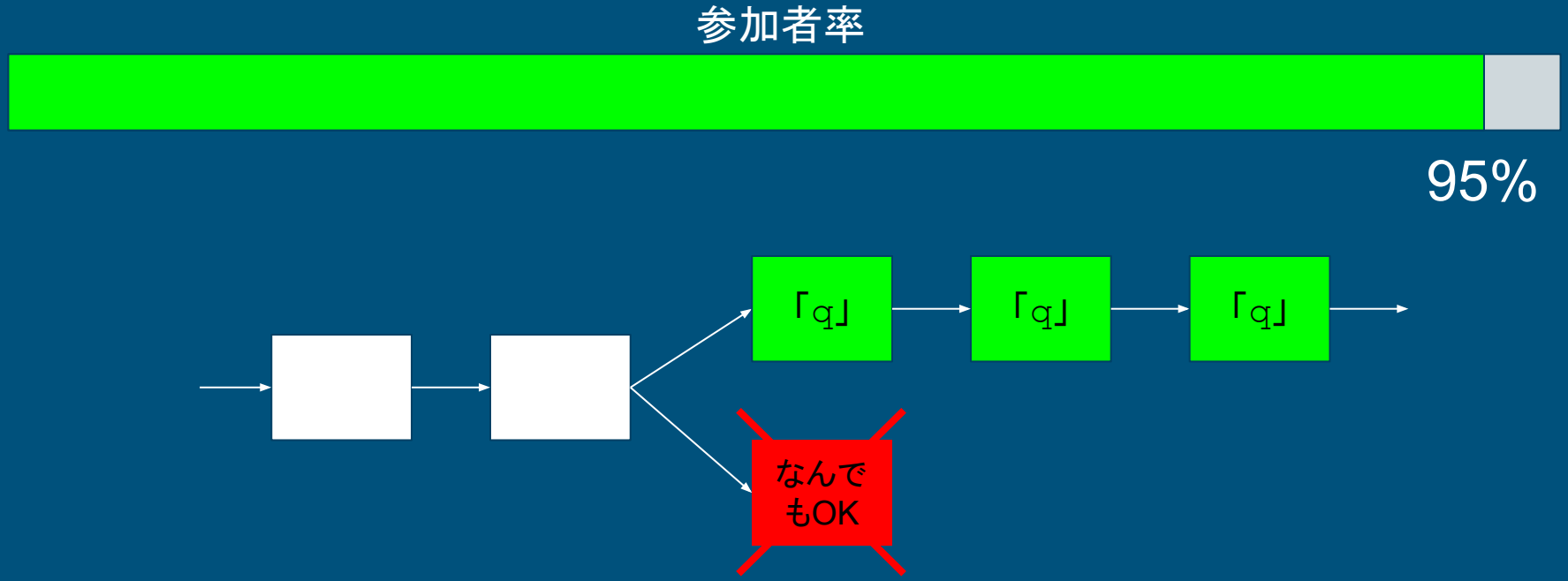
2つのネットワークになる。

Soft Fork



1つのネットワークになる。

Soft Fork

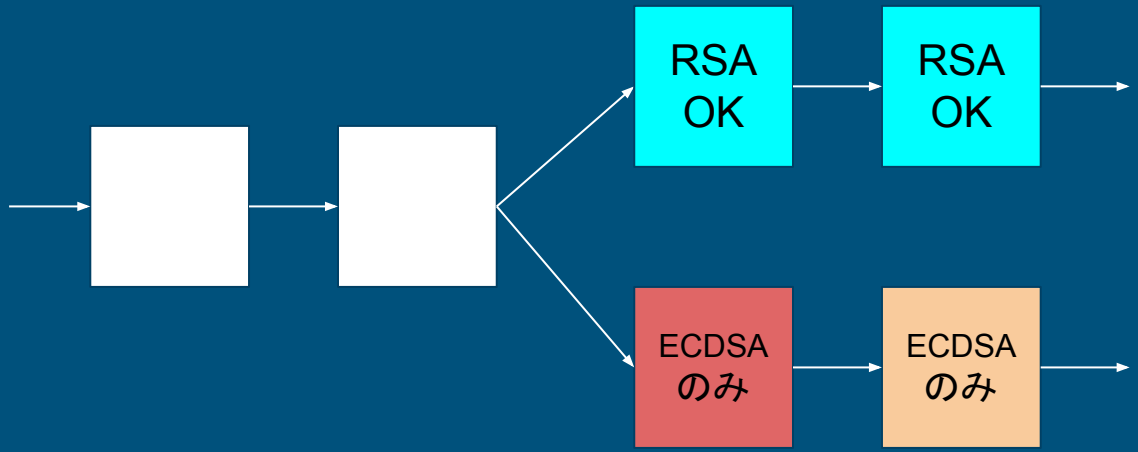


1つのネットワークになって、新しいルールは標準になる。

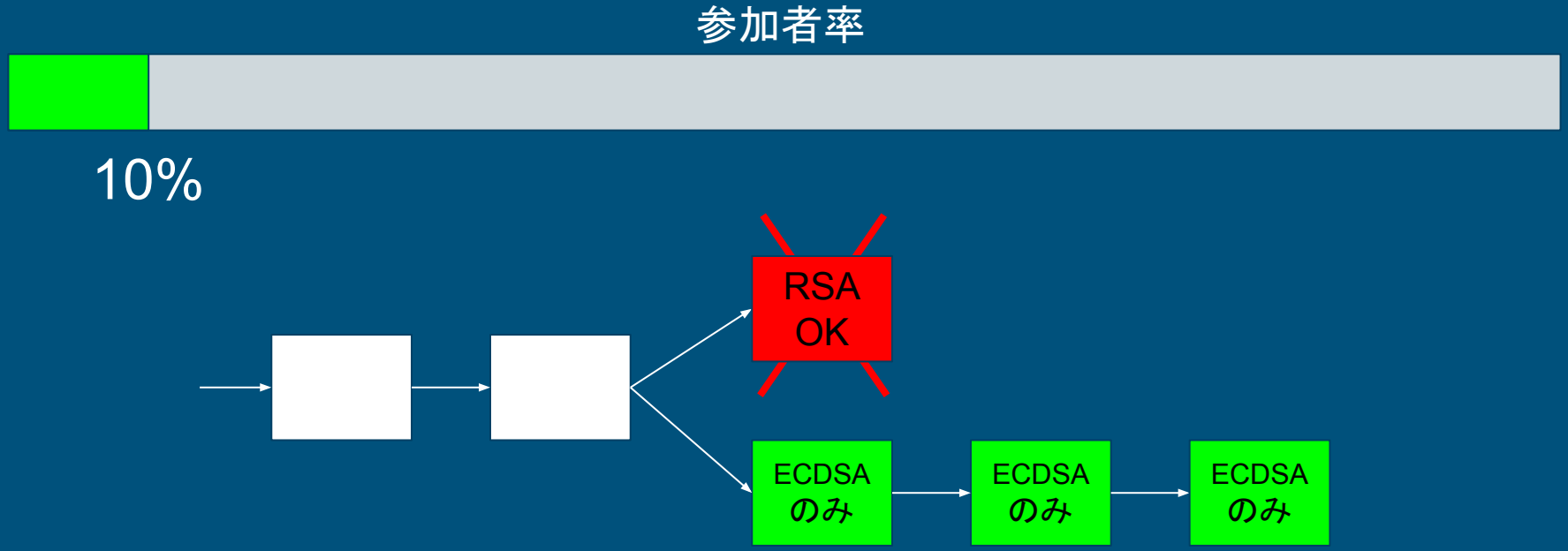
Hard Forkの例

例えば:

ECDSAだけじゃなくてRSAの署名も可能。

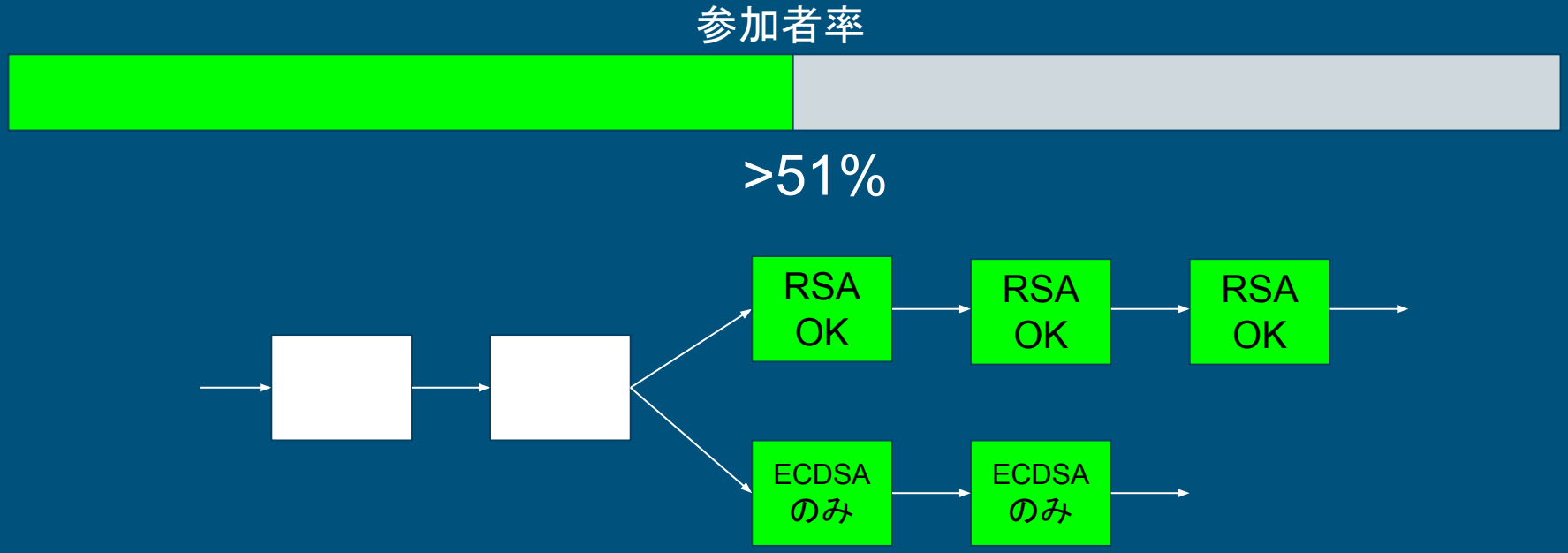


Hard Fork



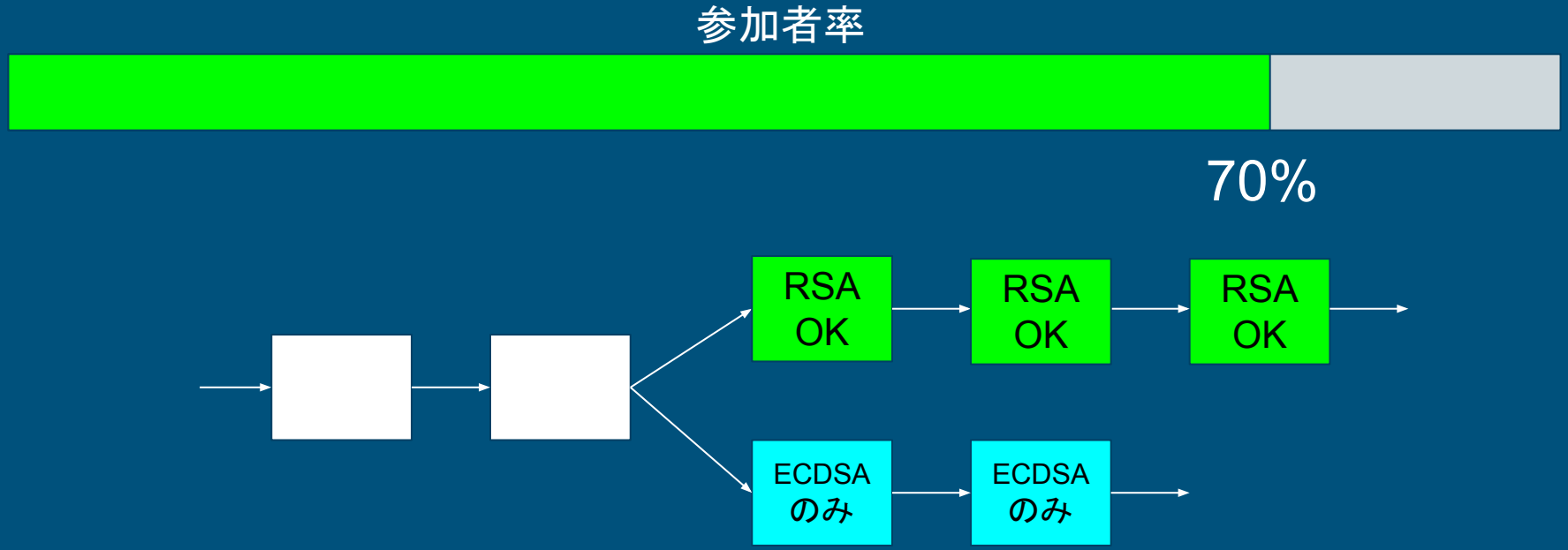
1つのネットワークのまま。

Hard Fork



2つのネットワークになる。

Hard Fork



2つのネットワークのまま。

まとめ

- トランザクションが最新のブロックに取り込まれても完璧では無い（かもしれない）
- 段々とブロックを重ねるにつれ、信頼性が高くなる

新しいTxを作ってみよう

隣の人とアドレスを交換して、BTCを送ってください。

```
$ ./bitcoin-cli getnewaddress

$ ./bitcoin-cli sendtoaddress <ADDRESS> 0.5
```

出力された TxId に注目してください。

デモ

anditto@dglab.com
github.com/anditto