

Fintech 特許紹介(8)

マルチフォークブロックチェーン生成方法

2017年2月6日

河野特許事務所

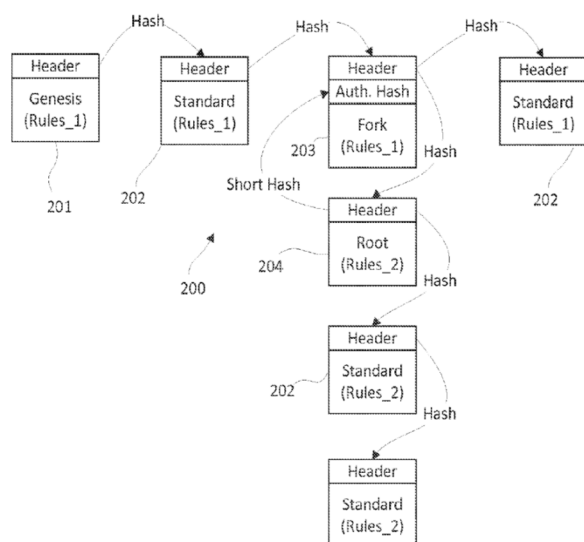
所長 弁理士 河野 英仁

マルチフォークブロックチェーン生成方法

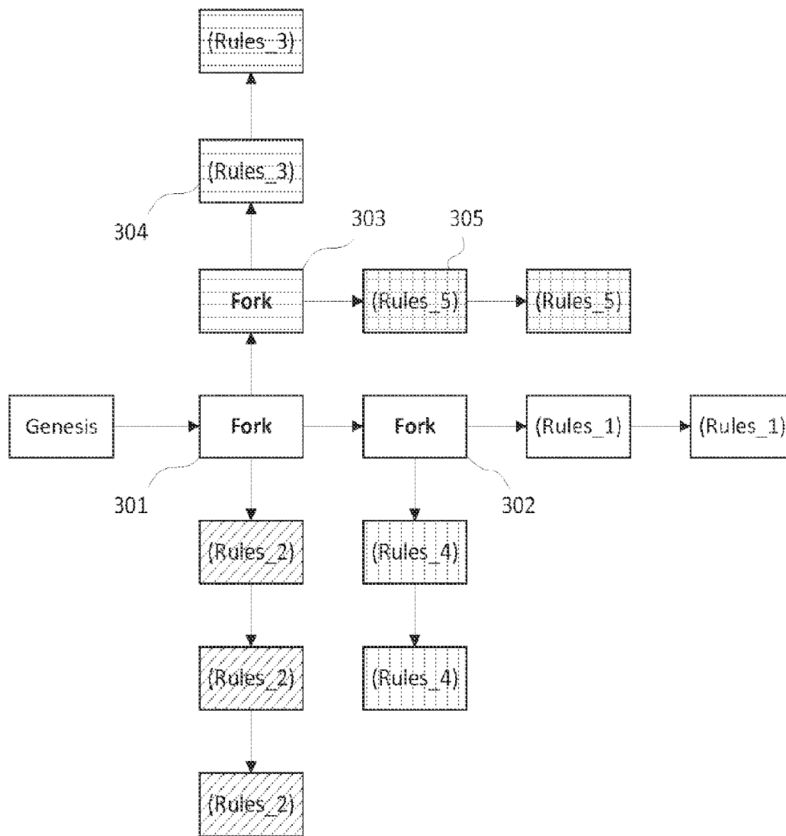
米国公開番号 US2016/28552 出願人 BLOCKCHAIN TECHNOLOGIES CORPORATION

本特許は2015年7月24日に出願された。本発明はブロックチェーンにおいて生じるフォークを有効活用する方法である。

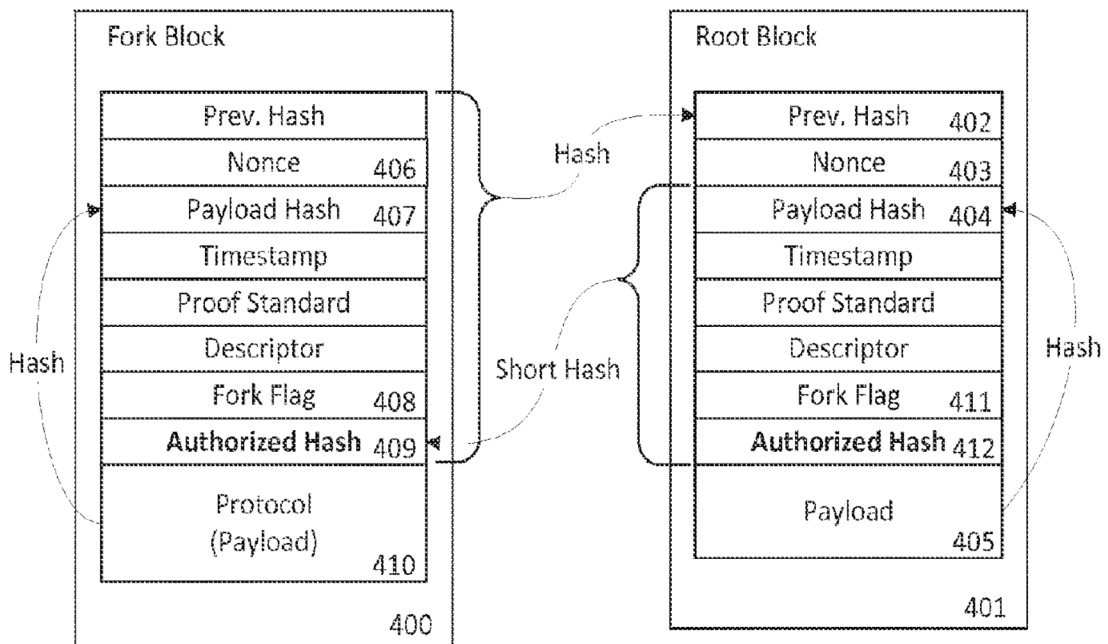
ブロックチェーンでは同じタイミングでマイニングに成功した場合、ブロックチェーンのフォークが発生することがある。この場合、ビットコインにおいて用いられているブロックチェーンでは、フォークの短いチェーンは破棄されることとなる。本発明は、フォークチェーンを破棄せずに有効活用しようとするアイデアである。



ブロックチェーンの各ブロックは前ブロックのハッシュ値をヘッダに記憶している。本発明では分岐するルートブロックを活用すべく、ルートブロックの前のフォークブロックに、ルートブロックの認証ハッシュ値を記憶させ、相互認証を行う。これにより、2分岐だけではなく、下記図のように数多くの分岐ブロックチェーンを生成するものである。



Root BlockはヘッダとPayload(データ部分)を有するヘッダには、前ブロック(Fork Block)のハッシュ、暗号法のNonce(ノンス)、Payload Hash、タイムスタンプなどを含む。前ブロックハッシュ及びノンス以外のヘッダデータでショートハッシュを生成する。

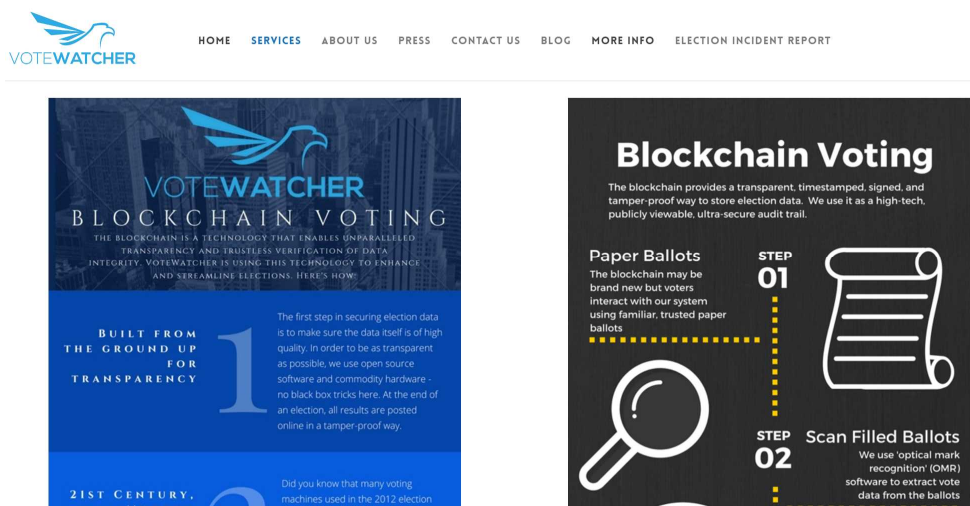


ショートハッシュはFork Blockのヘッダに書き込まれる。Fork BlockのPayloadハッシュ、タイムスタンプ等からRoot Block用のハッシュを生成する。これにより、相互認証を経て複数の有効な分岐・フォークを有するスライドチェーンが増殖される。

ブロックチェーンテクノロジー社はニューヨークに本社をおき、主にブロックチェーンに関するコンサルティング及びビットコインATMの提供などを行っている¹。



ブロックチェーンはビットコイン等の仮想通貨だけではなく、契約、証券等様々なデータを認証、トランザクション対象とすることができ、各社での開発競争が始まっている。ブロックチェーンテクノロジー社では、投票システムにブロックチェーン技術を用いる“Vote Watcher”サービスの開発を進めている。



以上

¹ 2017年2月3日ブロックチェーンテクノロジー社HPより
<http://blockchaintechcorp.com/>
<http://votewatcher.com/>