推論攻撃を考慮したアクセス制御へのコンセンサスアルゴリズムの適用の検討

神奈川大学　電気電子情報工学科
201503923　武藤寛弥

研究背景

- 近年、推論攻撃による情報漏えいが問題になっている。
- 一つ一つは重要でない情報も、複数集めることで重要な情報を特定することが出来うるため、防御が難しい。

推論攻撃の例

先行研究

- 『推論による情報漏えい防止のためのブロックチェーンの応用』
  神奈川大学(2017)小野洋介

権限の強いユーザーがアクセス履歴を改ざんするなどの不正を行う可能性があるという問題があった。

目的

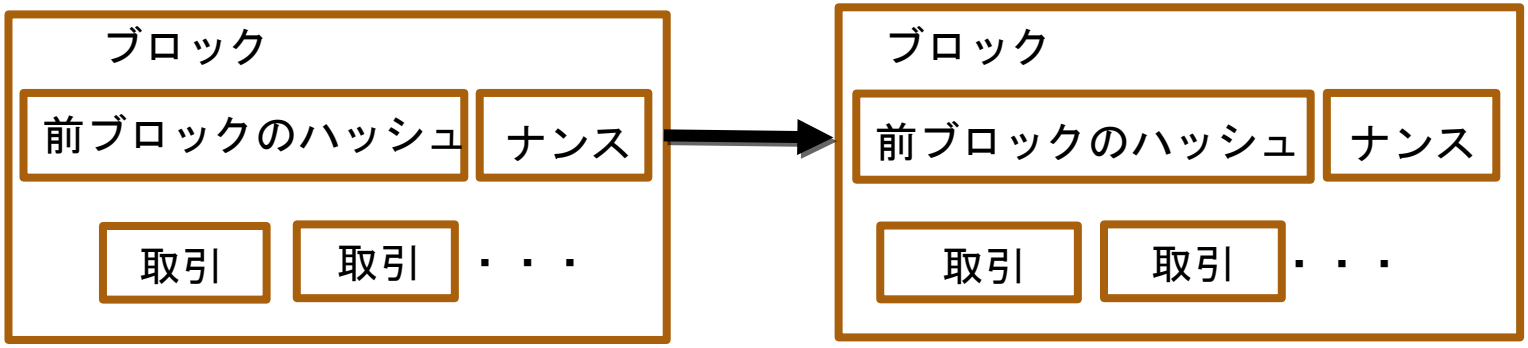
- まず、4つのコンセンサスアルゴリズムを分析する。
- 次に、複数のブロックチェーンのシステムにおけるコンセンサスをとるという概念について検討する。

ブロックチェーン

取引などの時系列を持った出来事を参加者全員が
監視することにより、不正や改ざんを防止する分散型の台帳。

要素技術としては公開鍵暗号、一方向性ハッシュ関数、
P2Pネットワークなどが用いられている。

ブロックチェーンのイメージ図



提案

(1)コンセンサスアルゴリズムがある。

(2)そこには、ブロックチェーンが使用されているとされる。

(3)まず、世の中にあるコンセンサスアルゴリズムを調べ、分析する。

(4)次に、コンセンサスをとる新しい方式を考案する。

各コンセンサスアルゴリズムの比較

	特徴	メリット	デメリット
Proof of Stake	コインを多く、長く保有しているほどブロックを生成しやすい。	時間、コストがかからない。51%攻撃のリスクがない。	通貨の流動性が損なわれる。貧富の差が生じる。
Proof of Importance	コインを多く保有し、かつ取引量が多いほど、ブロックを生成しやすい。	Proof of Stakeと比べて貧富の差が生じにくい。	取引の承認には一定量以上の通貨を保有する必要がある。
Proof of Consensus	特定の企業たちによる合意によって取引を承認し、ブロックに記録していく。	取引を承認する時間が非常に速い。改ざんがされにくい。	企業たちが共謀すると改ざんが起こる可能性があり。
Proof of Work	膨大な計算量を解いてナンスを見つけた人がブロックを生成できる。	改ざんがされにくい。	時間、コストがかかる。51%問題のリスクがある。

批判

- ブロックチェーンは取引アルゴリズムの健全性(改ざんをされていないことの証明)を目的としている。この方式は、1つのブロックチェーンのシステムにおける健全性において、システム内の取引のコンセンサスをとる、というモデルである。しかし、複数のコミュニティが同じブロックチェーンのシステムを使用していないという現実がある。

コンセンサスアルゴリズムから見えてくるもの

分析

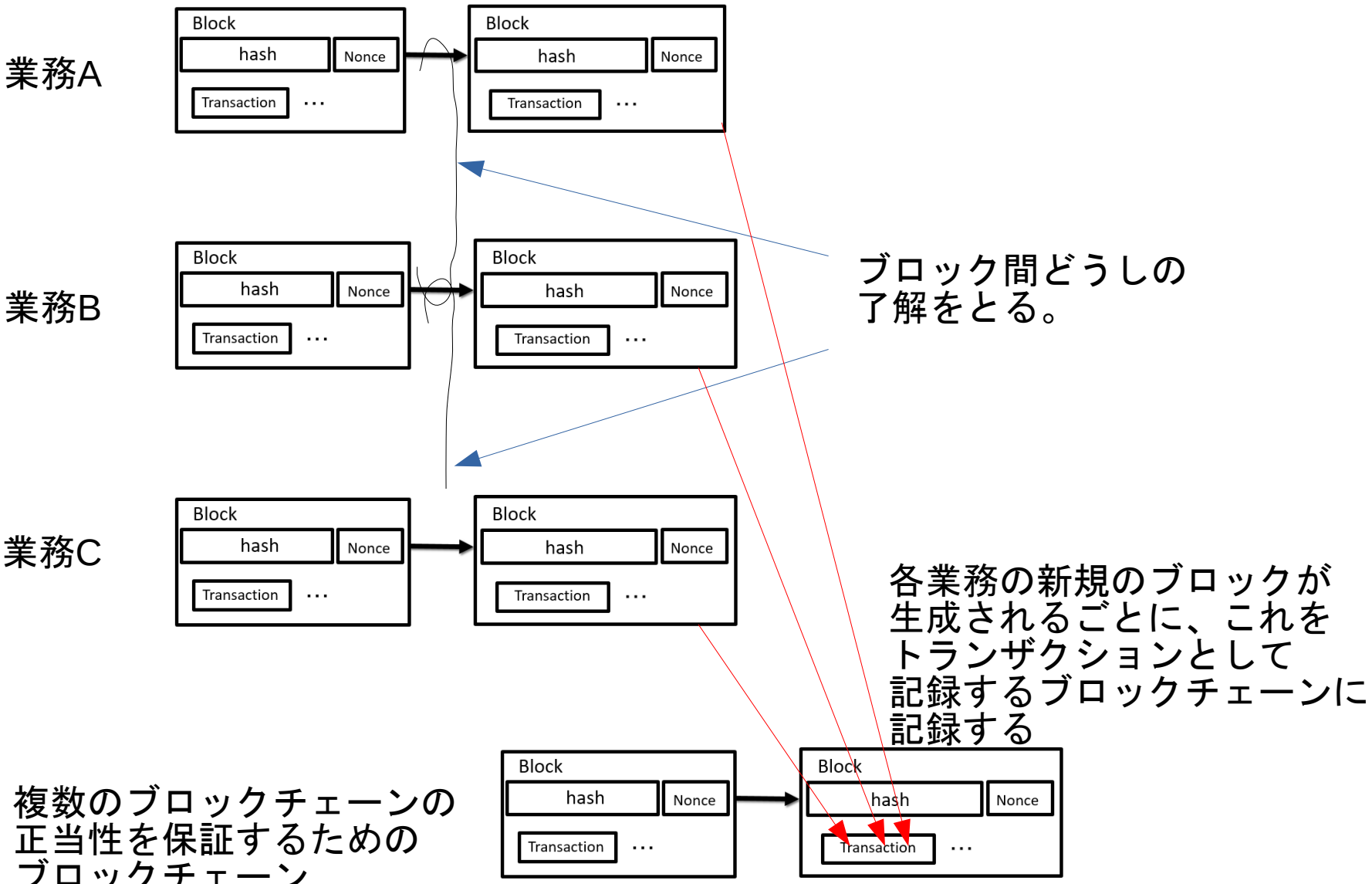
(1)Proof of Consensusは、トランザクションの信用が前提である。

(2)信用できないとすれば、NGである。

(3)そのため、トランザクションの信用を担保したい。そこで、業務ごとのトランザクションをブロックチェーンとする。

(4)複数のコンセンサスが生じるブロックチェーンは本来の使い方ではないが、管理集合ごとの複数本のブロックチェーンどうしの了解をProof of Consensusでとる。

提案モデル Proof of Blockchains



複数のブロックチェーンを使うことの必要性

- 同一社会システムに異なるコンセンサスアルゴリズムが混在している場合に適応すれば、より高いセキュリティーを実現できる。

結論

- データベースに複数のブロックチェーンを適用して、ブロックチェーンどうしのコンセンサスをとり、各ブロックチェーンの正当性を保証するセキュリティモデルをを提案した。
- これにより、高い信用性が確保され、アクセス履歴の改ざんを防ぎ、より安全性の高いセキュリティが実現できると考える。

今後の課題

実際にこの提案モデルをown cloudを適用して、有効性を確認する必要があると考える。