October 22, 2019

ブロックチェーンとビットコインについて

平松　楓也

富山県立大学　情報基盤工学講座

1. はじめに
2. ブロックチェーンとは
3. ビットコインの仕組み
4. おわりに

October 22, 2019

はじめに

背景

5G の時代にブロックチェーンという技術が新しく出てきたが、AI や IoT などと違ってどういったものか理解しづらい。また、ブロックチェーンとビットコインはどう関係しているのかが分からない。

目的

今回はブロックチェーンについて理解してもらうのと同時にビットコインとの関係を知ってもらい、何らかの研究のヒントになればよいと考えている。

ブロックチェーンとは

ブロックチェーンは別名「分散型取引台帳技術」と呼ばれており、ネットワーク上にいる利用者たちがお互いに取引データを「分散」して管理し合う仕組みである。

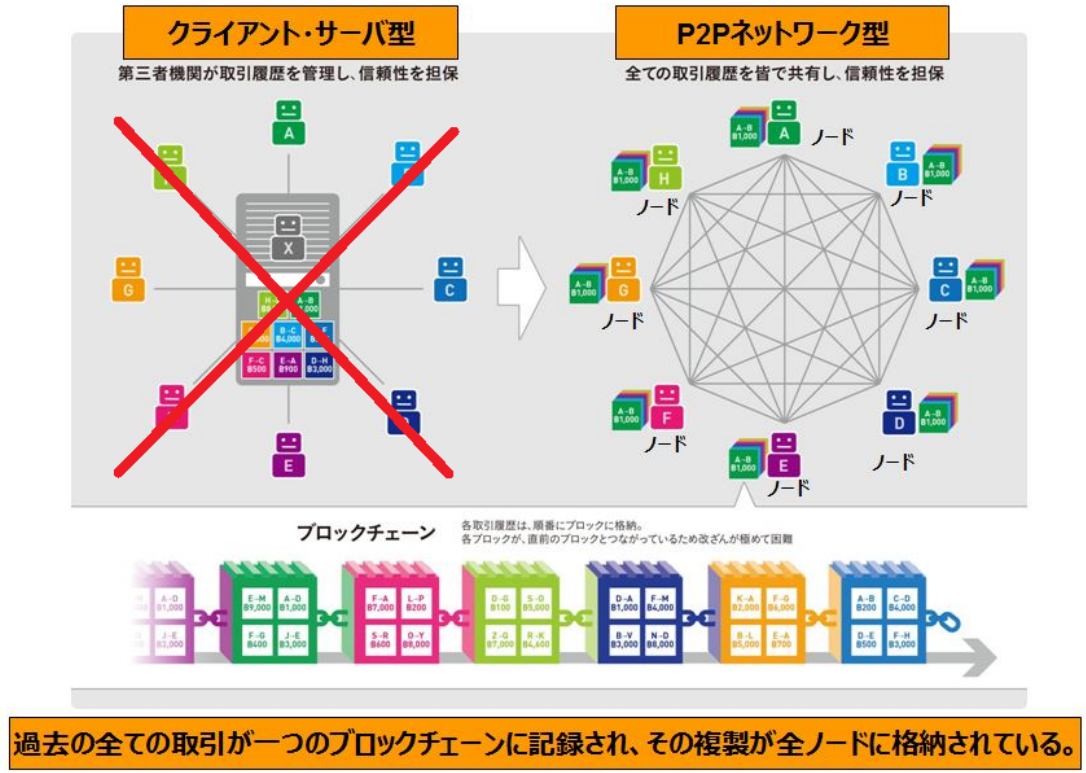

Figure: 分散型イメージ

ブロックチェーンのメリット

１、自律分散型なのでシステム障害に強い
データを一元管理しないことによって、システムが実質的にダウンしない（分散することで他所で復旧できる）

２、データの改ざんが不可能なので信頼性が高い
ブロックチェーンは暗号化され、分散して保存されている。また、意図的に改ざんすれば、分散したデータとの整合性が取れないため、すぐに不正が明らかになる。

ブロックを構成する３つの要素

(A) トランザクションデータ（Tx）:
ユーザー間でやり取りした決済情報などの取引データ

(B) ナンス（Nonce：Number used once）:
使い捨てのランダムな 32 ビットの値

(C) 前のブロックのハッシュ値（Prev Hash）:
ブロック同士を連携させるための情報

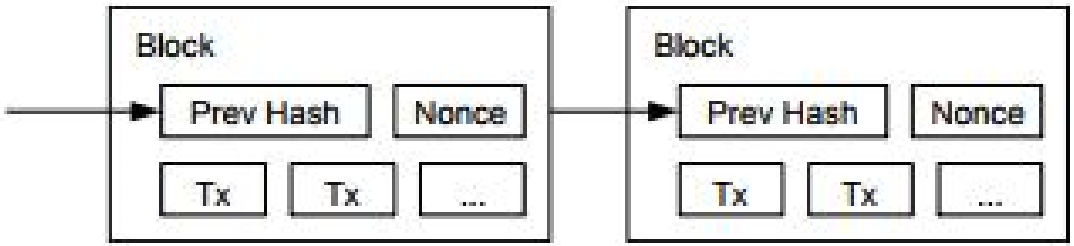

Figure: ブロックの 3 要素

PoW(Proof of Work) と Nonce

・改ざんや不正をチェックするために、ネットワーク上のノードが取引の承認、つまりはその取引が正当なものであると認める作業を行う必要がある。その取引の承認が正しく行われるように承認する人を決める仕組みをコンセンサスアルゴリズム (合意形成) という。
・ビットコインで使われているものが PoW というもので仕事量で承認する人を決めるものである。
PoW ではある特定の条件に当てはまるハッシュ値を探す膨大な量の計算をして承認者を決めている。

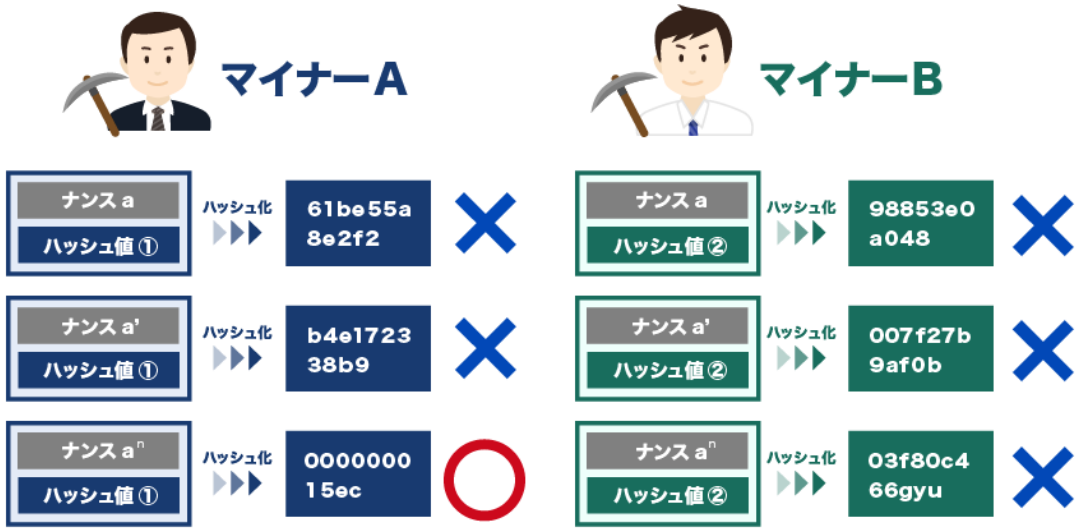

Figure: PoW のイメージ

ハッシュ関数

・ハッシュとは、あるデータを変換して得られる固定長のデータのこと。また、ハッシュを得るための関数をハッシュ関数という。
・どんな値でも指定の長さの数値に変換できる。
・不可逆性を持つ
・元のデータが少しでも変わると変換後のハッシュが全く異なる。
・ビットコインで使われているのは SHA-256（シャニゴロ）である。

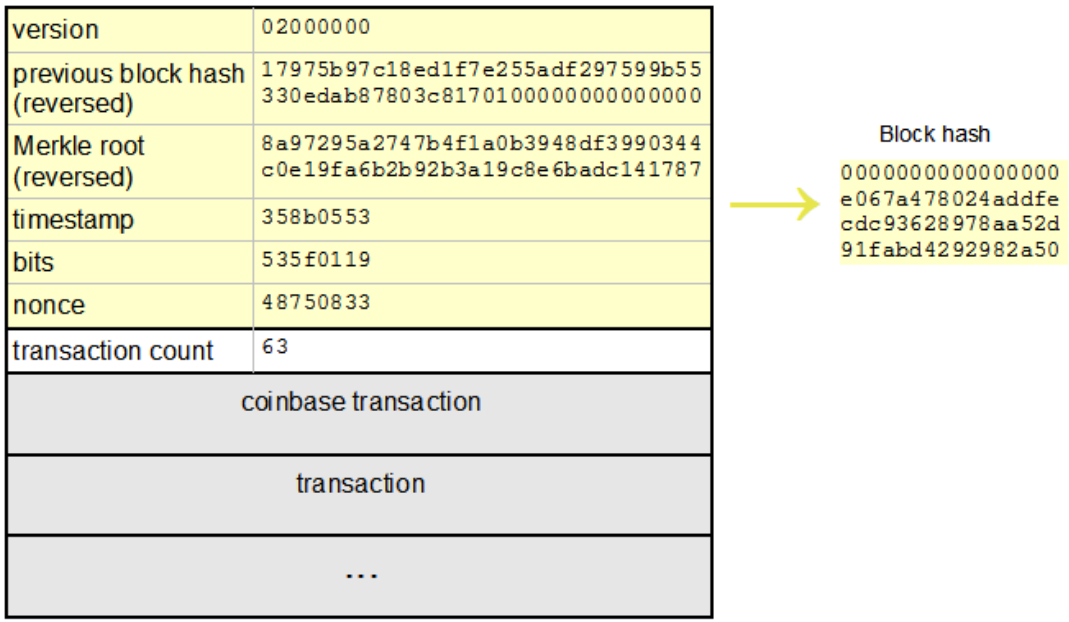

Figure: ビットコインのハッシュ

ブロックチェーンの強み

ポイント

1. トレーサビリティ
2. 高いセキュリティ
3. 第三者による承認が不要
4. スマートコントラクト

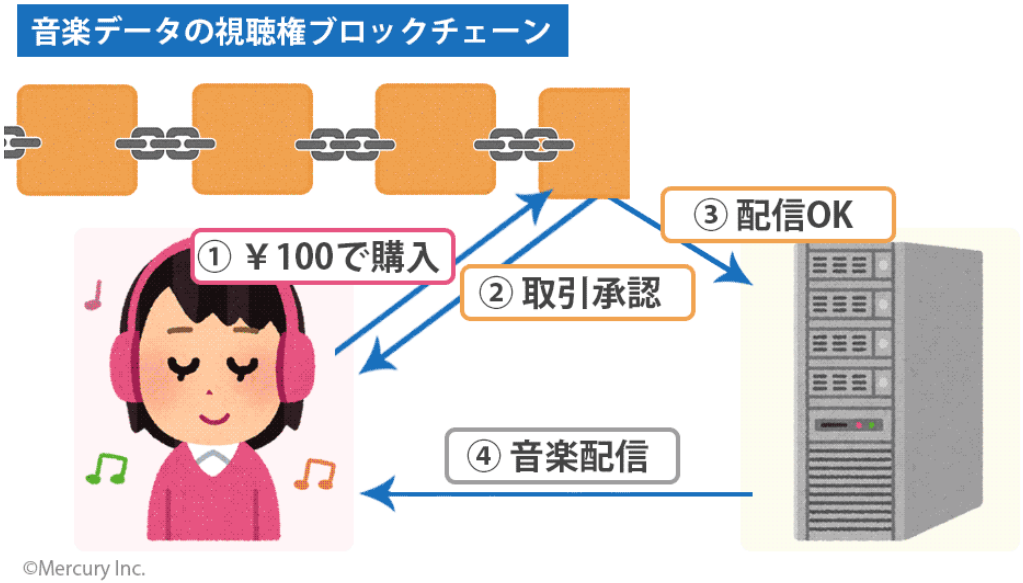

Figure: スマートコントラクト例

ブロックチェーンの活用事例

【今までの問題】
食品に起因する健康被害が発生した場合、その原因を見つけるのには農家・加工業者・流通業者と様々な関係者が関わっており、それぞれが独自にトレーサビリティを実施しているので数日を要することがある。
【ブロックチェーンを使って】
食品安全システムに関わる全ての関係者の連携を迅速、かつ効率的な最善の方法で行うことできる。

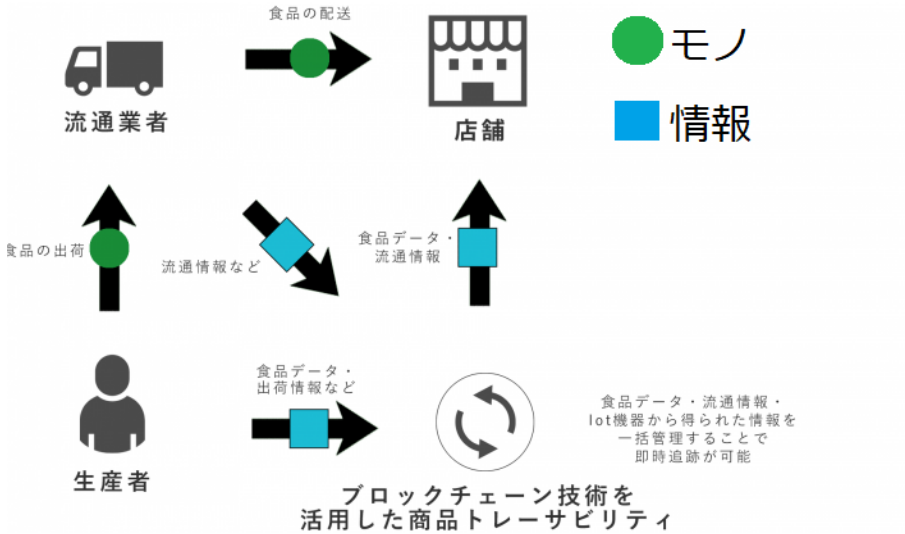

Figure: 活用事例

おわりに

まとめ

1. 現在はまだブロックチェーンの法律の環境が整っていない。
2. 今すぐ、大規模に社会が変わることはないと思われる。
3. 食品の流通のトレーサビリティなど小規模で事例は増えていっている。

今後の課題

1. 今後、ブロックチェーンをどんな分野に使えるかを考えられる力が求められるのではないだろうか。