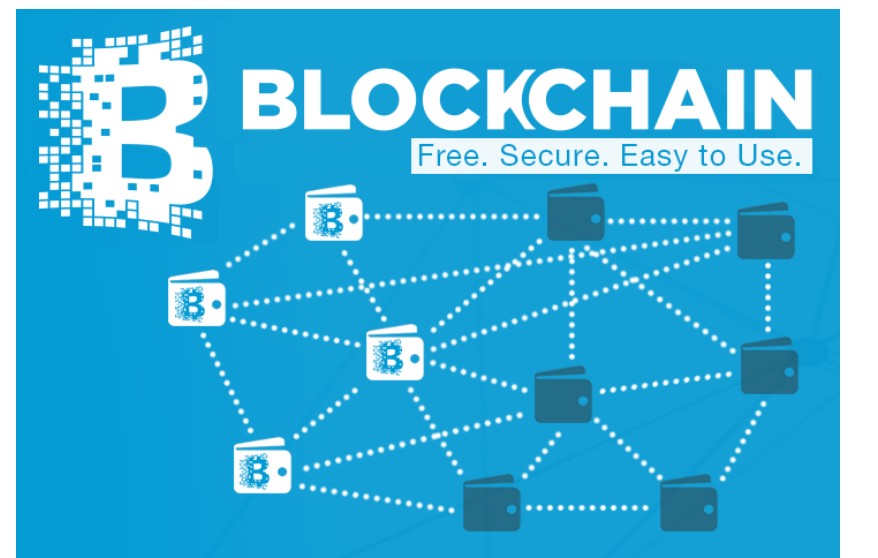


～ Blockchainの仕組みと魅力 ～

created by Gaiax Blockchainゼミ班
石川、菊池(梓)、白木、肥後、峯（五十音順、敬称略）



Blockchainの概要

Bitcoinとは？

『Bitcoin』とは、実体を持たない通貨であり、デジタルな数値自体に価値を持っている仮想通貨。
(実体を持たない新通貨という点で、既存の通貨を用いた電子マネーなどと異なる)

Blockchainとは？

Blockchainは、Bitcoinを「第三者機関を通さず、参加者間の直接的オンライン取引を可能にする」ために提案されたアルゴリズム。

言い換えると、Blockcahinは

改ざんできない オープンで 共有された 取引台帳
(書き換えることができない) (誰でも閲覧できる) (誰でも使える) (取引履歴)

を実現する仕組み。

Blockchain実装の種類

Blockchainの仕組みを使ったプラットフォームで抑えておくべきは『Bitcoin』と『Ethereum』。

Ethereumとは、BitcoinのBlockchainが仮想通貨の取引に最適化されている仕組みになっているのに対して、例えばオンラインショップの商品売買など、様々な合意・契約を得る場面で使えるように通貨ではなく「契約」をやりとりできるようにしたもの。⇒ Blockchainは通貨としての利用に留まらないもの

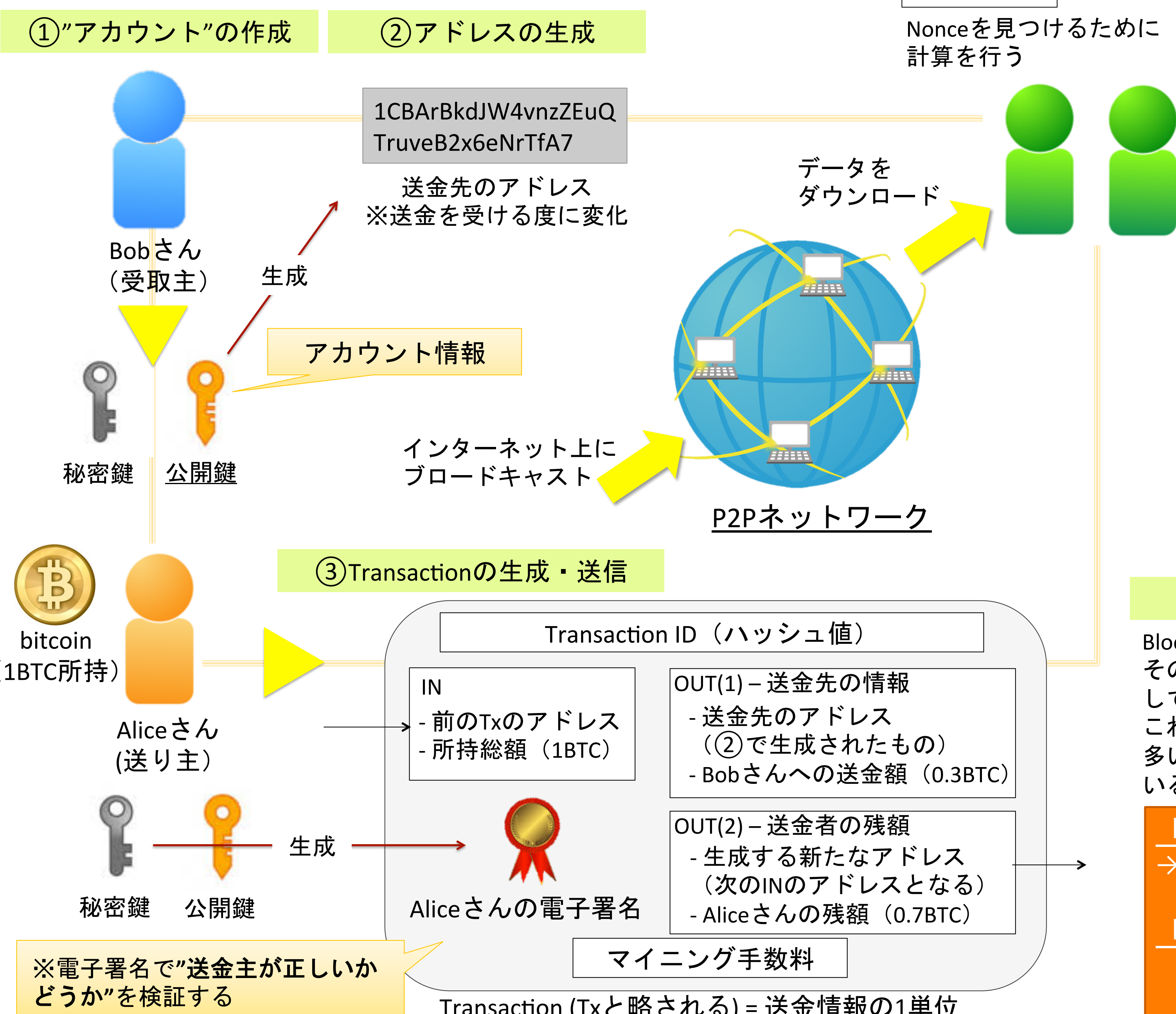
Blockchainの歴史

年表 時系列での、Blockchainの発展について抽出・掲載。

2008年10月	Satoshi Nakamoto によりBitcoin(Blockchain)の現論文が公開される。Bitcoin(Blockchain)の開発がスタート。
2009年1月	Bitcoin v0.1 がリリースされる。
2010年5月	Bitcoinで初の商品購入。10,000BTC＝25ドルでピザを購入する人が現れる。
2010年11月	Bitcoinの時価総額が1億円を突破（Bitcoin交換所運営企業レートで）
2013年3月	キプロス金融危機が発生し、Bitcoinが脚光を浴びる（需要が高まる）。
2013年11月	Bitcoinの時価総額が1兆円に達する。
2014年	Ethereumの開発がスタート。 Dell,PayPal,Microsoftらが次々とBitcoin決済導入を発表。
2015年5月	NASDAQが未公開株式市場のインフラにBlockchainの利用検討を発表。
2015年7月	Ethereum v1.0 がリリースされる。
2015年	銀行業界のBlockchain投資が約1億\$(2015)から約4億\$(2019)に達する見込み cf.) Aite Group(2015), 「Demystifying Blockchain in Capital Markets」 世界経済フォーラムは800名のエグゼクティブにアンケートを取り、2025年までにはGDPの10%がBlockchain上に保存されるという調査結果を出す cf.) WEF (2015), 「Deep Shift Technology Tipping Pointsand Societal Impact」 24p

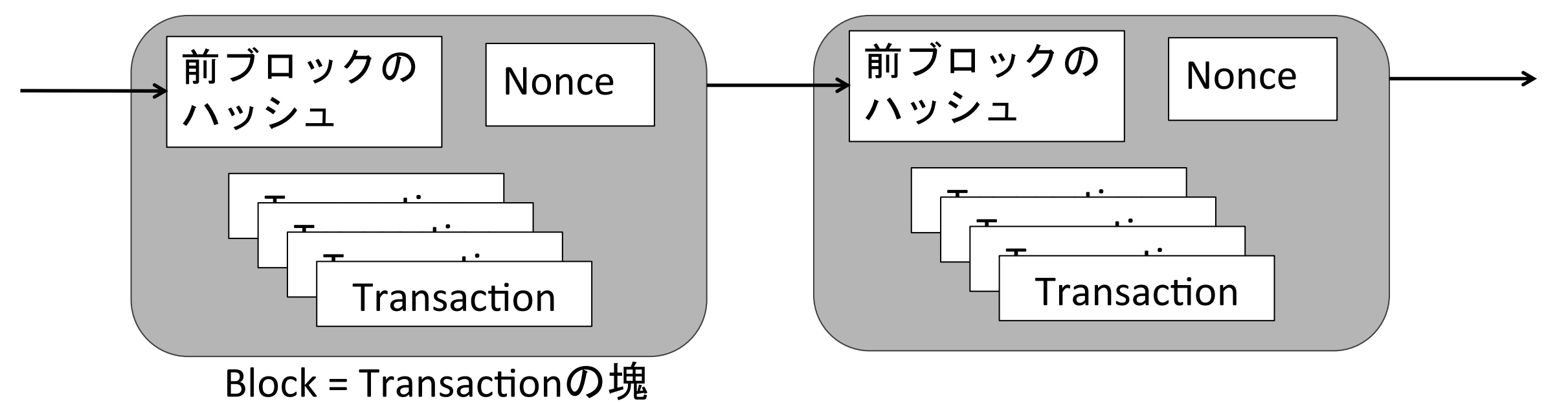
Blockchainの仕組み

例) AliceさんがBobさんに0.3BTCを送る場合



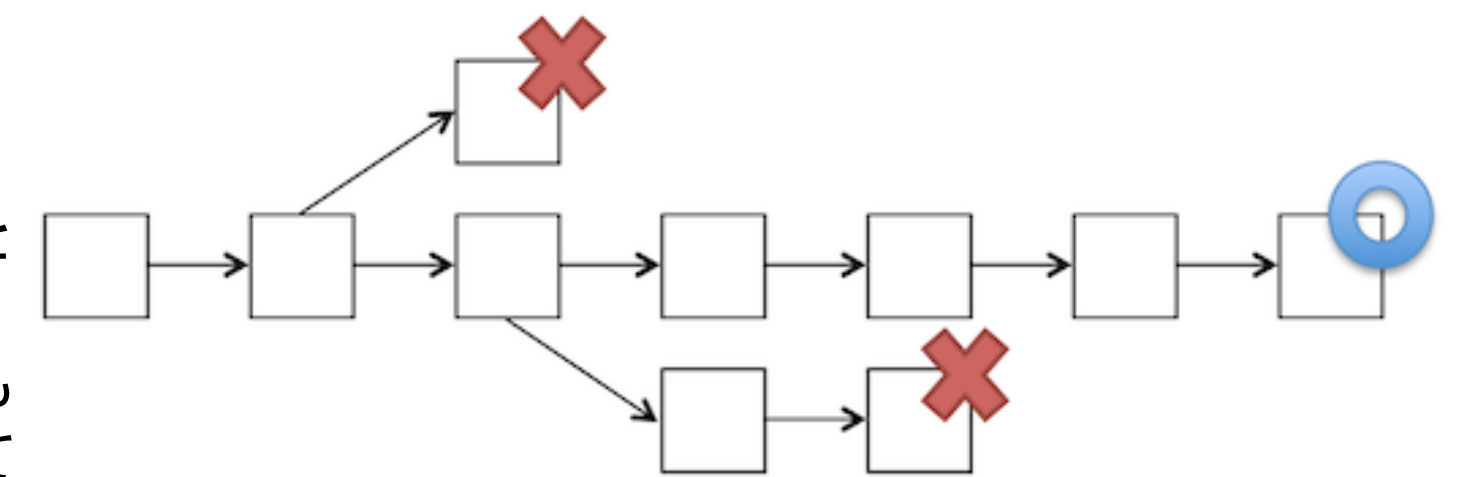
④miningによってBlockを確定する

- ブロードキャストされたTransactionをBlockにまとめる（約 100 transaction/Block）
- minerは、ある条件を満たす値を計算する**
 - 上記の値を見つけることを「mining」と呼び、その値を「Nonce」と呼ぶ
 - Nonceを見つけるには、CPU等の計算資源を使って全探索的に計算するしかない**
 - 約10分に一度nonceを発見できるように自動で難易度が調整される
- 発見されたNonceを他の51%以上のminerが正しいと確認するとBlockが確定する
- 他のminerよりもいち早くNonceを発見したminerには「マイニング手数料 + マイニング報酬（2016年1月現在; 25BTC = 約100万円）」が支払われる（= minerのモチベーション）
- 1.～4.を繰り返して、Blockを鎖のようにつなげていく = 『Blockchain』



⑤正しいチェーンの決定

Blockchainでは、分岐が発生し得る。そのため「最も長いチェーンが、常に正しいチェーンとして認める」という規則が存在する。これによって「攻撃者よりも善意の計算資源が少しでも多い限り、チェーンを乗っ取れない」仕組みを実現している。



「第三者期間を通さず、参加者間の直接的オンライン取引を可能にする」
→ 公開鍵暗号によって、送り主・受取主のアカウントを特定、直接送金できる

「コインの改ざん問題の解決」

- 計算資源を使ってBlockが正しいものと証明
- 攻撃者は善意の計算資源を上回って計算し続けられない限り、取引の改ざんは不可能

Blockchainの魅力

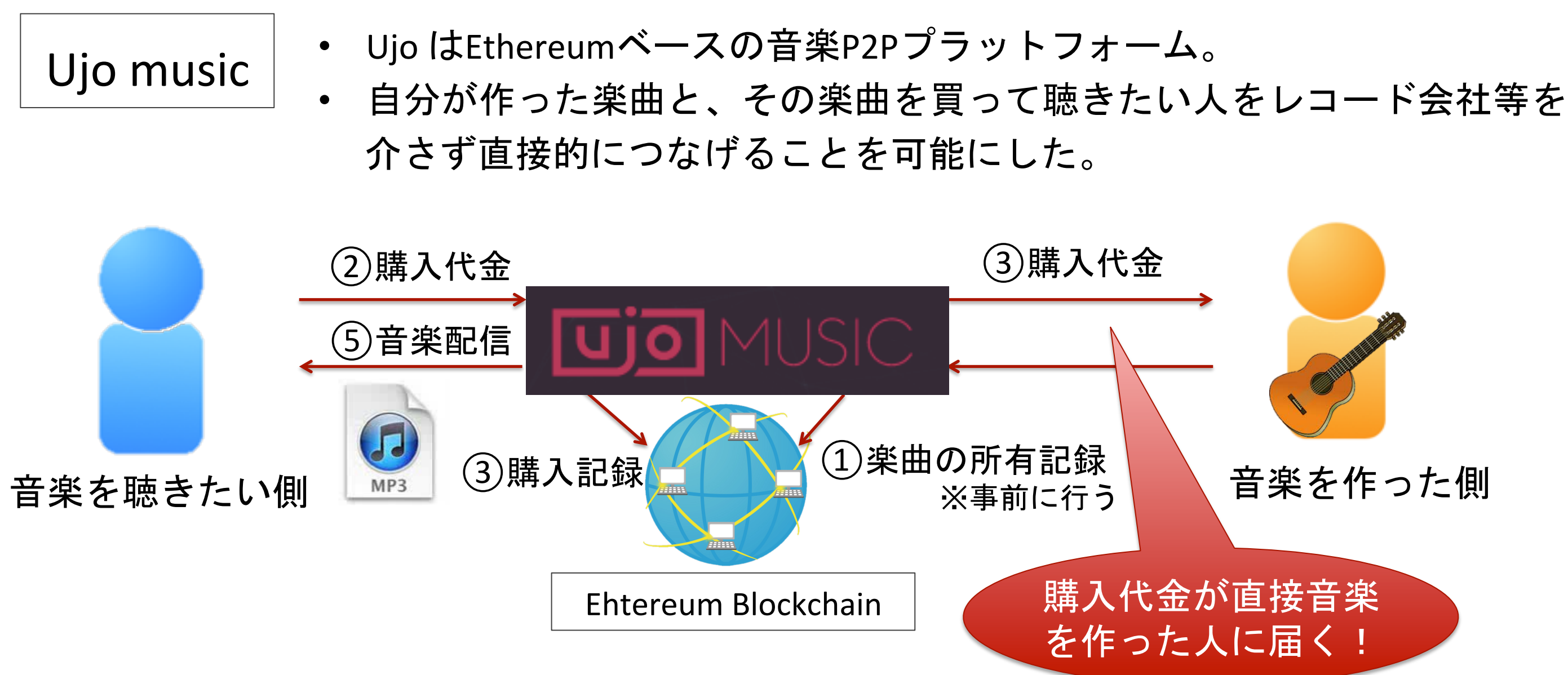
Blockchainには以下の利点がある。

- 管理する人は必要とせず、それに関わらずシステム全体を破壊することができない。
- 全取引履歴が世界中で閲覧可能な状態にでき、取引の透明性が担保される。
- 全取引履歴は正しいものであることが確認されている。
- 参加者間で直接取引することができ、仲介者を省くことが可能になる。
- 利用範囲は通貨だけでなく「誰が誰に何をした」をネット上に記録することができる。

Blockchainを使えば..
第三者機関を介することなく、安全にインターネット上で価値の移動が行えて、それを常に証明され続けることができる！

※ 正確にはサービス運営のための第三者機関は必要だが、必要最低限に留めることができる

Blockchainを使ったサービス例



※ 他にサービス例を見たい場合は「非金融分野 ブロックチェーン」で検索

なぜGX？

ガイアックスはシェアリングエコノミーの領域に注力していますが、それを支える技術としてブロックチェーンは相性がよいという仮説を持っています。単純に、サービスのアーキテクチャとしてブロックチェーンを利用すればよい、というのではなく、以下のような「ブロックチェーンにより可能になる、または進化すること」に着目し、技術蓄積や新しいサービスの発案を行っていきます。

- ビットコイン、通貨**
中央集権なしに、個人間(CtoC)で価値(お金や権利など)を移動することができます。
- 存在や行為の証明**
あるドキュメントがある時点で署名され、その後改ざんされないということを証明できます。シェアリングエコノミーでは、個人の信頼情報を証明・利用できる必要があります。
- スマートコントラクト**
契約(コントラクト)をプログラムで記述し、その記録が残ることで透明性を高められます。契約が履行されると同時に対価の移動も完了することができます。これにより個人間の取引を技術の側面から支援することができます。

予定している取り組み

- ブロックチェーン技術の活用**
自社が提供するサービス群において、ブロックチェーン技術の活用を進めます。
- 新しいサービスの発案と実装**
ブロックチェーンの特色を活かし、社会の変化を推し進める新しいサービスを企画しています。(現在準備中)
「個人の認証」「少額決済」「スマートコントラクト」といったキーワード、領域に意欲を持っています。
- その他**
コンサルティング、活用提言、オープンソースコミュニティへの貢献 等