

ブロックチェーンビジネスモデル

JSSスプリングフォーラム2019

2019-02-22

東京大学 大学院工学系研究科
技術経営戦略学専攻
ブロックチェーンイノベーション寄付講座

特任研究員 芝野恭平

ブロックチェーン技術について

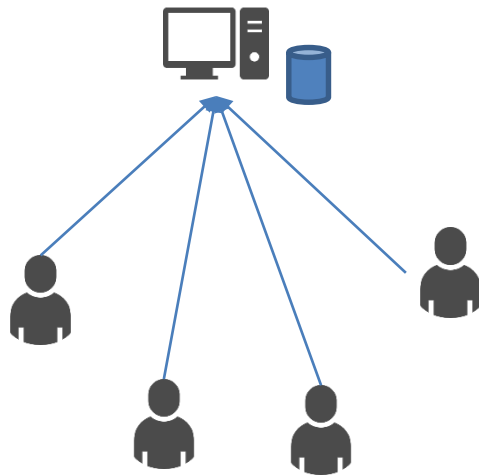
- ブロックチェーンは、ビットコインなど仮想通貨(暗号資産)を実現している仕組み
- 非中央集権型
- 非改ざん性
- の2つの特長がある.
- 今日は、この2つの特長をビットコインを例に説明し、それを活用したプロジェクトを紹介します.

分散的にデータを保管するシステム

- 従来型のシステムと違い管理者不在
- 参加者のノードにはブロックチェーンすべてのブロック情報が保存されている

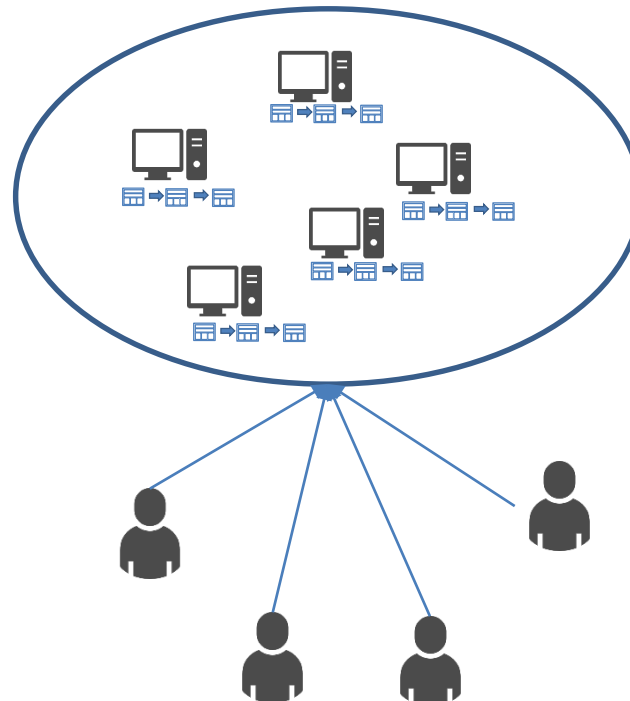
従来型のシステム

- 管理者が必ずいるシステム構成
- ユーザーは管理者が管理しているサーバーにアクセスする



ブロックチェーンのシステム

- 管理者不在のシステム
- ブロックチェーンデータを持っているPCが世界中に分散的に存在している



ブロックチェーン管理者

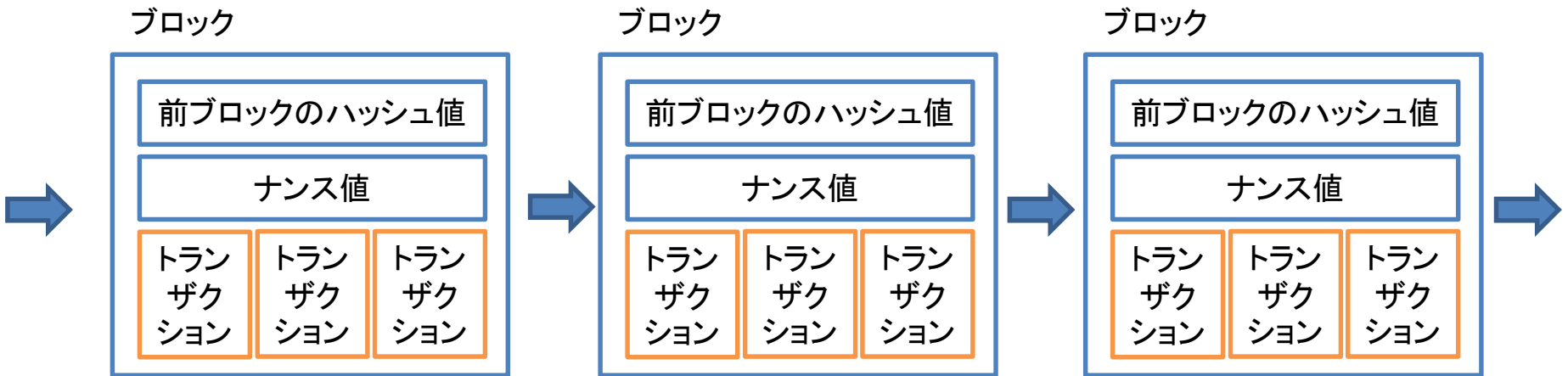
- ノード参加者
- マイナー
- ※ ノード参加者の多くがマイナー

ブロックチェーンユーザー

- 仮想通貨を所有する個人
- 仮想通貨での支払いを受け入れる店舗

Bitcoinにおける、ブロックチェーンのデータ構造

- ブロックチェーンのデータ構造はブロック+チェーンとなっている



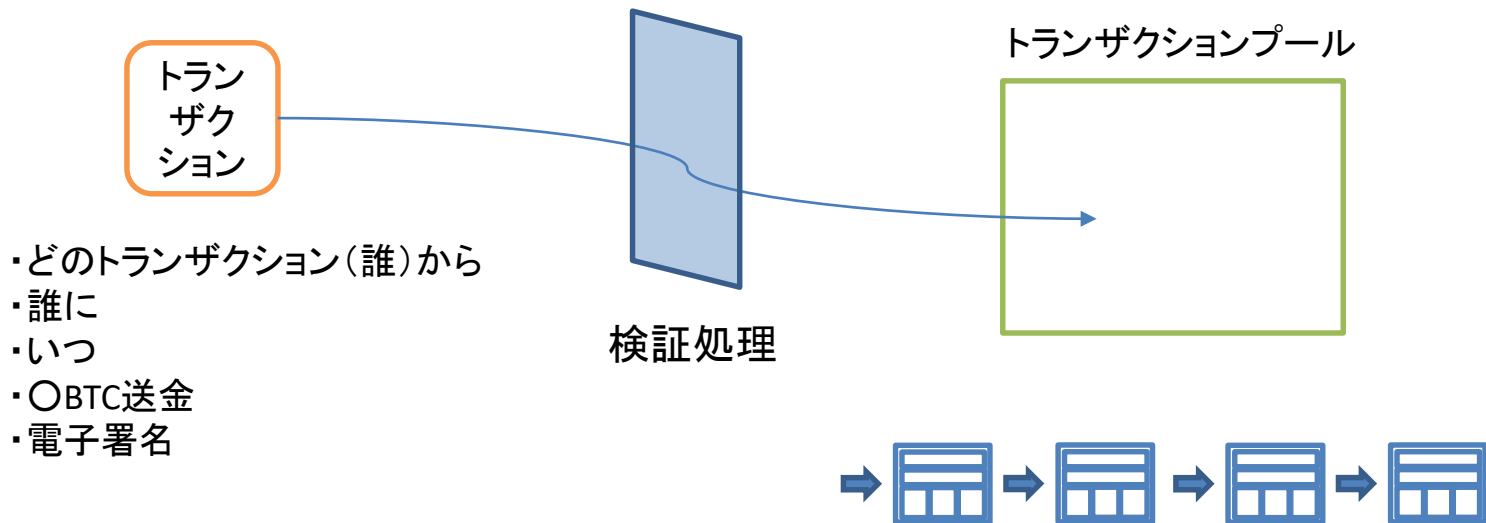
ブロックチェーン上にはトランザクションデータのみ保持されている。
即ち、誰から誰にいつ〇BTC送金した、という記録データのみが保持されている。

ハッシュ値というのは、ハッシュ関数を通した値。

ハッシュ関数とは、一方向関数で、同じ値をInputにすれば必ず同一のOutput値が出力されるが、逆にそのOutput値からはInputの値を導出することはできない。

トランザクションデータの追記

新しいトランザクション



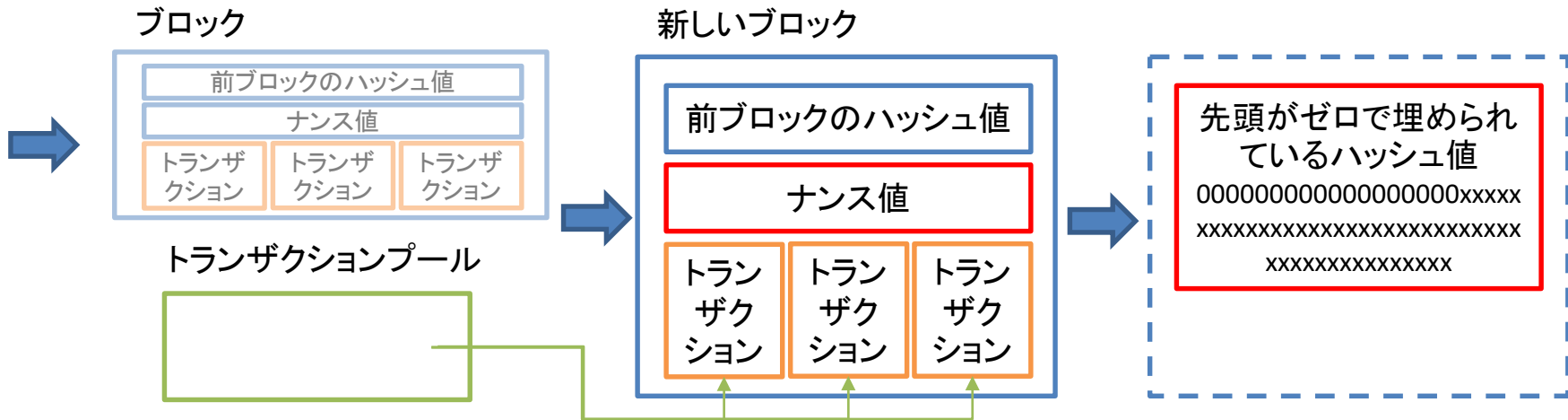
新しいトランザクション(送金処理)がされると、直接ブロックチェーンに書き込まれるのではなく、一旦はトランザクションプールと呼ばれる領域に保存される。

トランザクションプールとは、未検証のトランザクションを一時的に保存している領域です。

※ すべてのトランザクションがトランザクションプールに保存されるのではなく、トランザクションが正しいか検証処理の後に保存される。

ブロックの追加/マイニング

トランザクションプールから、ブロックチェーンにデータが永続化されるにはマイニングが必要



ブロックが追加され、トランザクションがブロックチェーンの一部に記録されるにはマイニングが必要です。

トランザクションプールより、任意のトランザクションがマイナーにより選ばれます

→ 多くの場合、各トランザクションに送金者により設定されている手数料が高い順に選ばれます。

ビットコインはProof of Workを採用しています。

→ ブロックのナンス値を求めさせる仕組み。ブロックに格納されている情報にナンス値の値を組み合わせ、ハッシュ値を求め、そのハッシュ値の先頭にゼロが条件をみたす数並ぶようなナンス値を探す。

→ このようなナンス値を求めるのは、言ってしまうとものすごい出の悪いガラガラくじを振って当たりを当てるようなもの。

ナンス値が発見できたマイナーにはブロックに格納したトランザクションすべての手数料に加えてマイニング報酬を手に入れることができます。

10分に1ブロックが追加されるようになっている。

ブロックチェーンの特長を再度おさらい

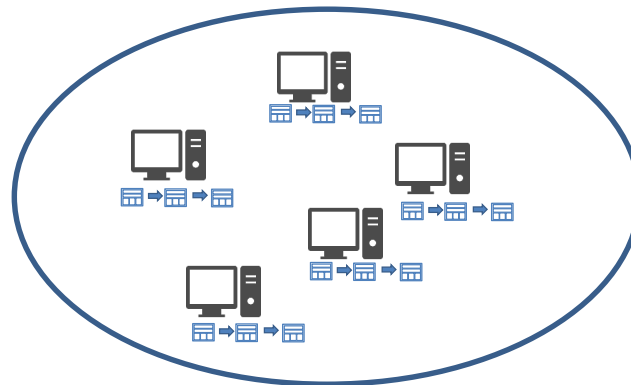
以上の仕組みの中で

- 非中央集権型
- 非改ざん性

を実現できている。

非中央集権型

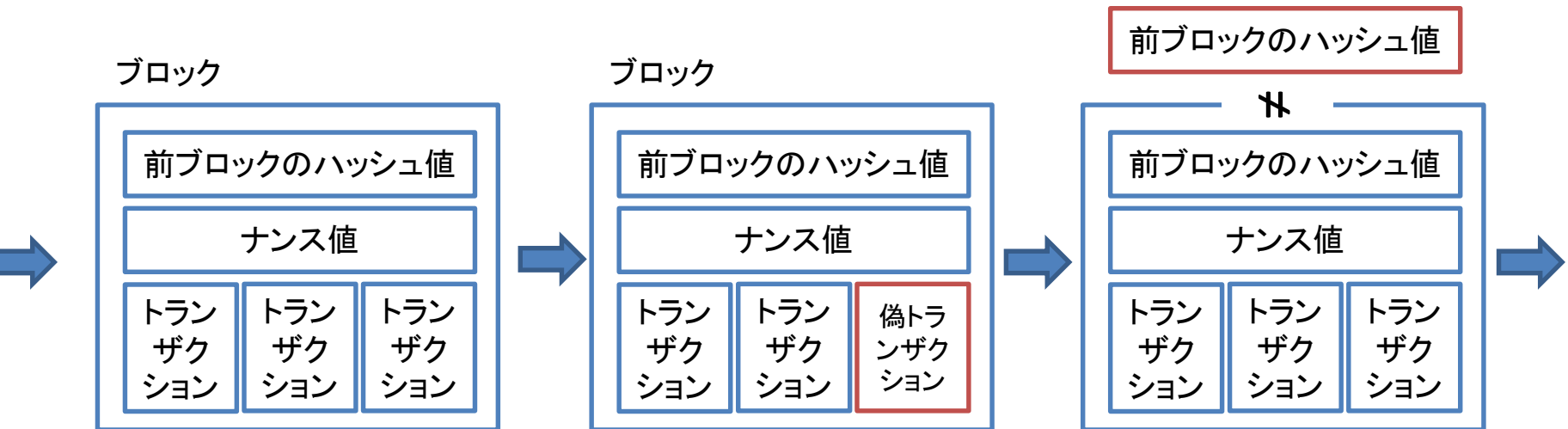
- 非中央集権型
 - マイナーによるたくさんのノードでシステムを運営している



- 世界中に存在しているノード(PC)にブロックチェーンデータが存在している
- 特定のノードが故障しても全体としては稼働し続けることができる
- ビットコインは2009年のサービス開始時より一度もサービスが停止されていない（ゼロダウンタイム）
- 特定の誰かの意図で、サービスが停止したり、仕様が変更されることができない

非改ざん性

- ハッシュ値の連続でブロックが作られているため、途中で改ざんが入るとすぐ判別できる。



また、改ざん箇所からその先すべてのブロックを正しくするには、そのブロックすべてのナンス値を求める必要があり、計算量的に事実上不可能。

スマートコントラクトについて

- 取引履歴(トランザクション)の保持は非中央集権型で非改ざん性, 透明性を保って実現できていることがわかった.
- ブロックチェーンは, 「取引履歴」に限らず広くデータ, さらには処理を保持することができる.
- この「処理」のことをスマートコントラクトという.
- ※ 今日触れないが, ブロックチェーンにデータを格納しスマートコントラクトを実行することに特化したプラットフォームがEthereum

- 即ち, スマートコントラクトとはブロックチェーン上に記録された, 非中央集権型, 非改ざん性2つの要素を持つ処理のこと.
- 例:
 - 全ての支払い時に8%を自動的に消費税として国の管理する口座に送金させる.
 - 40回に1回の確率で, 購入者の口座ではなく, Aさんの口座の残高から全額支払いがされる. (全額キャッシュバック)









- 従来型システムでも自社ECサイトを構築し上記のようなシステムを開発することは可能であるが, スマートコントラクトを利用することで「非改ざん性」により, その処理がサイト運営会社の意図的な措置で変更されることがないことが保証される.

ブロックチェーンプロジェクト事例を紐解いてみる

- 既存の、ブロックチェーンを活用したプロジェクトはどのようなものがあるのか・・・？

Cryptocurrencies の数：2,072 2019-02-15時点 <https://coinmarketcap.com/>

いくつかホワイトペーパーを読んでみて感じた主観的なブロックチェーンプロジェクトの分類

技術		概要	プロジェクト例
・ 非中央集権型	支払い	<ul style="list-style-type: none"> 仮想通貨 支払い 	 
・ 非改ざん性	情報保存 & シェア	<ul style="list-style-type: none"> チェーン上になにか情報を記録していき、みんなで共有する 	 
・ スマートコントラクト	トークンエコノミー	<ul style="list-style-type: none"> 独自トークンを発行し独自の経済圏を形成する 	 
	独自プラットフォーム	<ul style="list-style-type: none"> 各種課題を解決したブロックチェーン 	 
	ICO目的	<ul style="list-style-type: none"> 資金調達的手段 	

非中央集権型 事例

ビットコイン — <https://bitcoin.org/ja/>



- 2009年ローンチ
- 非中央集権型: 法定通貨のように、「国」による発行ではない.
- 非中央集権型で, 誰にも管理者がいない状態で価値(価格)がついており, 実際に取りもされている.
- 支払いに利用できる店舗も存在している.

非改ざん性 活用事例

Factom — <https://www.factom.com/>



FACTOM™

- 非改ざん性をうまく活用している事例
- 文書が存在したことを証明するサービス.
- 例えば保険の契約情報をブロックチェーンに記録しておくことで, その書類が存在したことをブロックチェーンが保証してくれる.
- ブロックチェーンに記録するのは, 文書情報そのものではなく, ハッシュ値のみ.

トークンエコノミーについて

- スマートコントラクトを活用している事例
- トークン(独自通貨)を使った経済
- トークンエコノミーの形成
 - トークンの発行
 - スマートコントラクトの利用(プラグラミング可能なトークン)
- 想定するプレイヤー(ユーザー)に対して, 意図的な用途でトークンをやり取りさせるシステムが構築可能
 - ブロックチェーンを使用しなくても構築可能であるが, トークンの残高やスマートコントラクトが中央管理者の意図で変更することができない, という点が異なる
 - 運営者の勝手な判断でトークンの残高や, 報酬の設計などが途中で変更されることがないことが保証される.

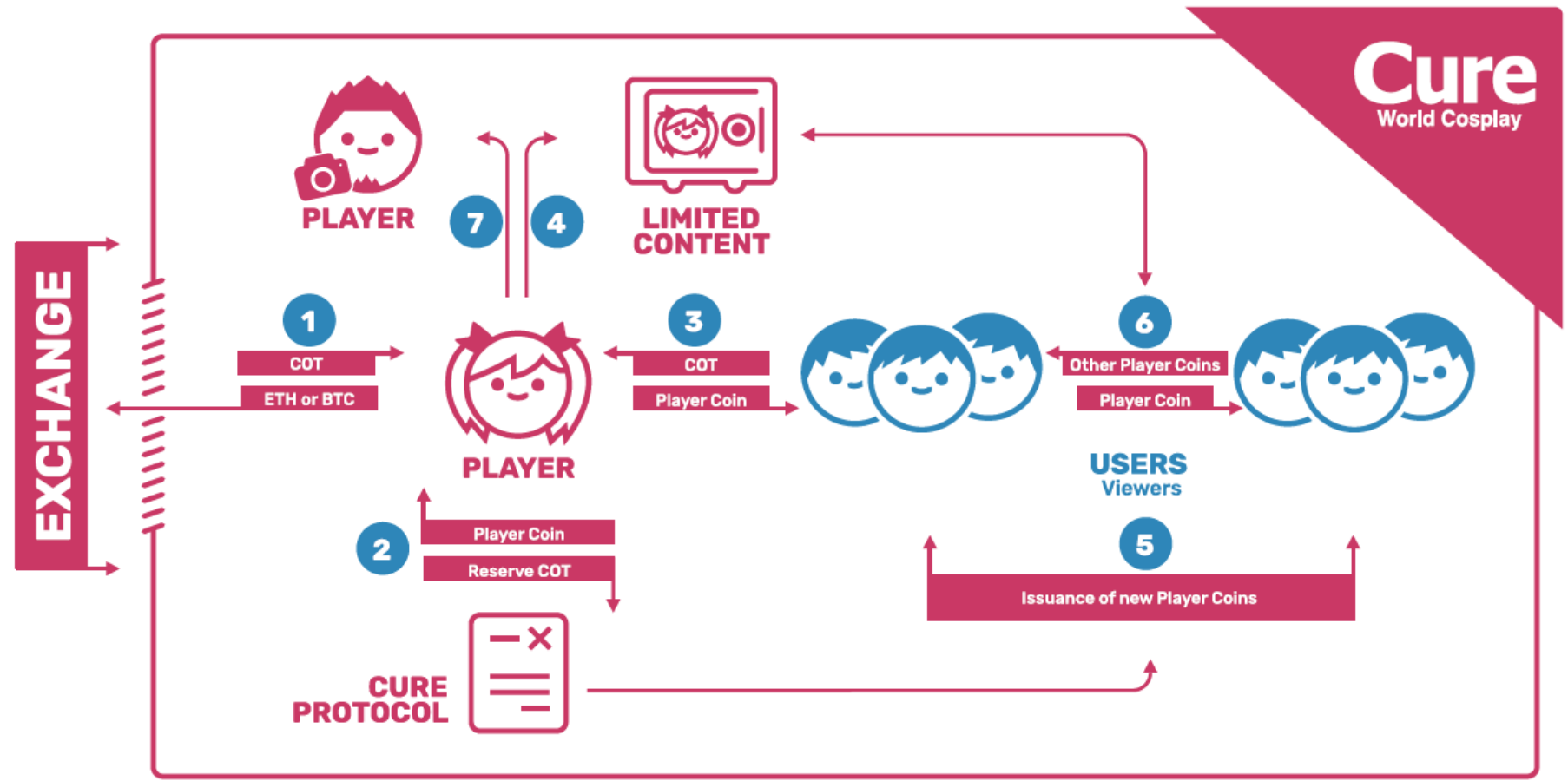
トークンエコノミーの事例

Cosplay Token - <https://ico.curecos.com/>



COSPLAY TOKEN

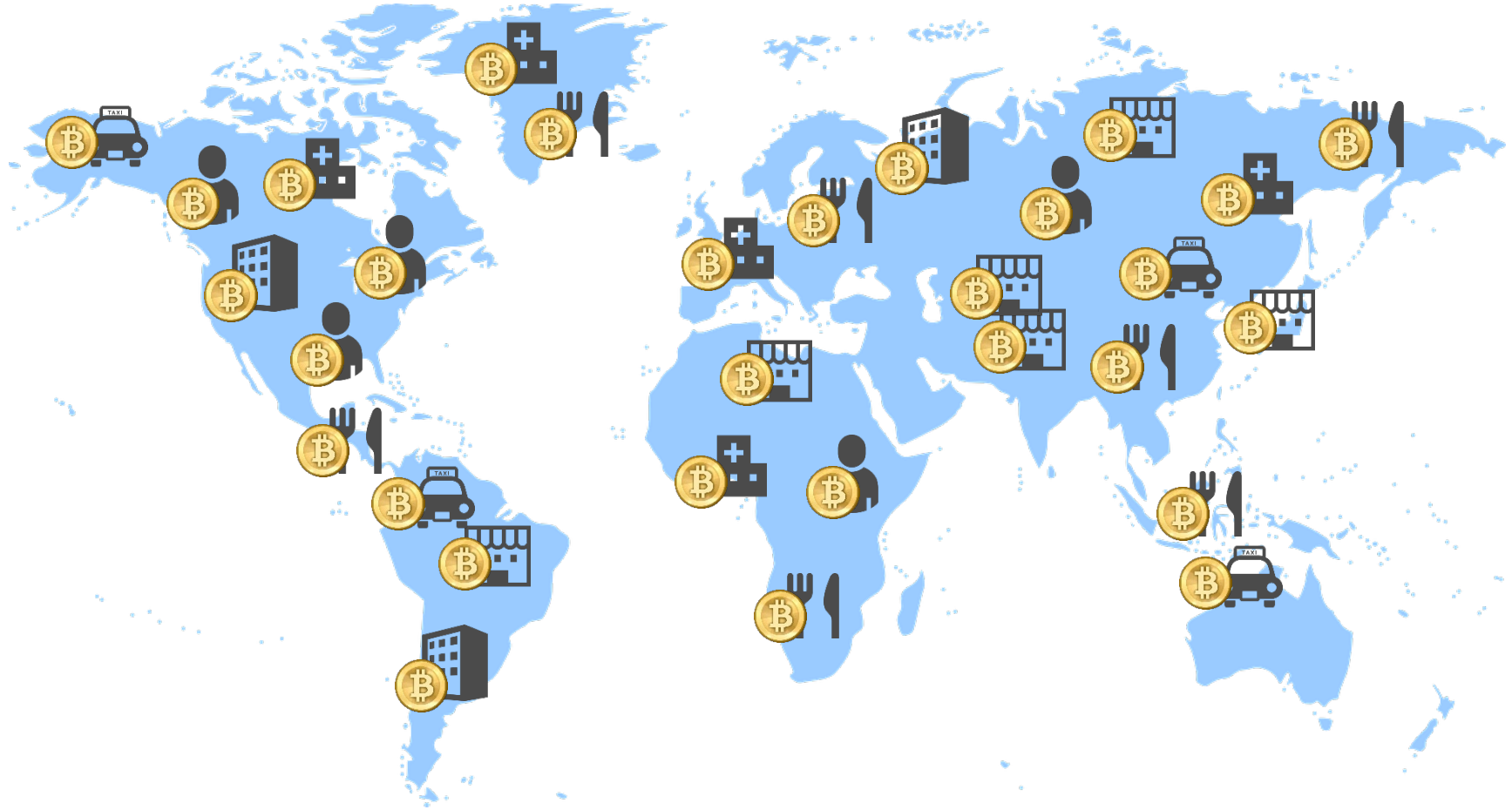
コスプレ界で独自の経済圏を創る



https://cot.curecos.com/docs/Cure-Whitepaper_EN.pdf?t=1550644105

-
- ブロックチェーンのデメリットや弱点はないのだろうか？

もしビットコインが世界で広く普及したら・・・



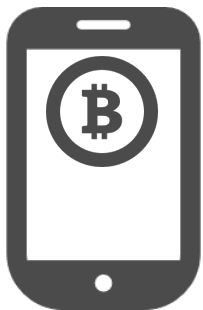
もしビットコインが世界で広く普及したら・・・ 想定されるメリット



- 海外に行くときにその国の通貨を持っていかなくても良い
- その国で流行っている決済手段を考えなくても良い

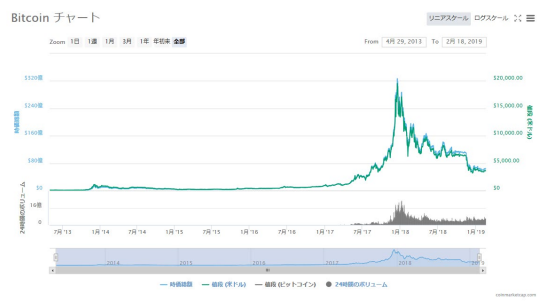


- 国際送金がラク



- キャッシュレス

もしビットコインが世界で広く普及したら・・・ 想定される問題点



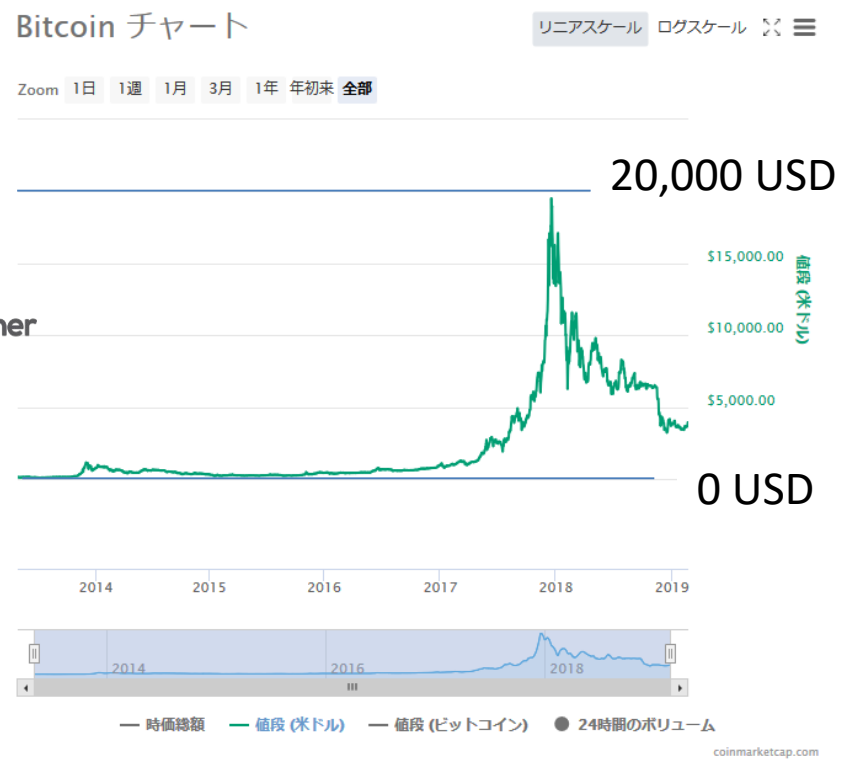
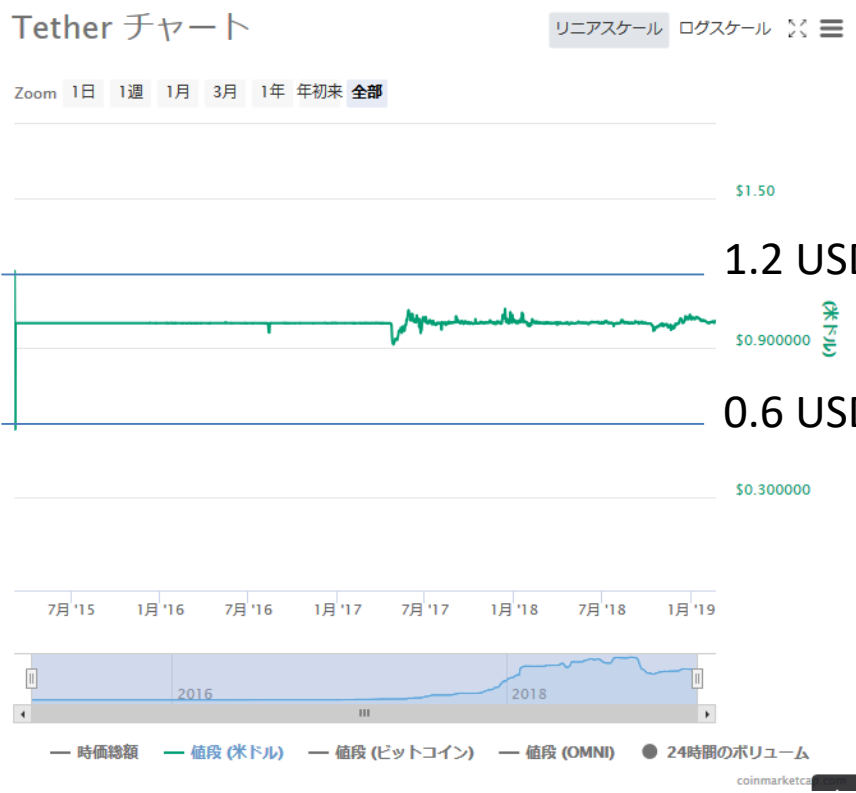
- 価格が過剰に変動してしまう



- トランザクションが確定されるまで時間がかかる
 - ファイナリティに60分

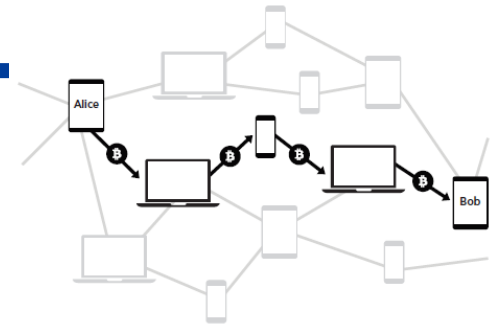
それぞれの課題に対して解決を図っているプロジェクトがある
— 価格が過剰に変動してしまう

- ステーブルコイン Tetherの例 — <https://tether.to/>

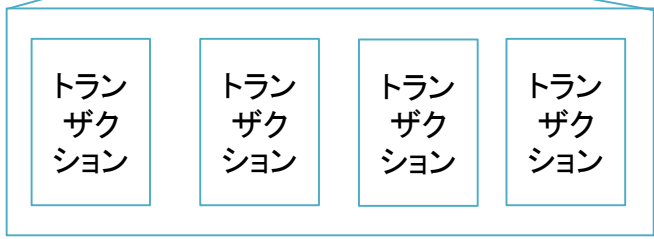


それぞれの課題に対して解決を図っているプロジェクトがある
— トランザクションが確定されるまで時間がかかる

- オフチェーン技術 ライトニングネットワークの事例
 - <https://lightning.network/>



- トランザクション処理をまとめてブロックチェーンの外側で行い, そのまとめられた結果のみをブロックチェーンに記録する, という仕組み.
- これにより, 一回あたりの送金手数料を抑えて, 処理時間を短いトランザクションの完了が実現できる.



チェーンの外(オフチェーン)で処理を行い, まとめられた結果のみをブロックチェーンに記録する

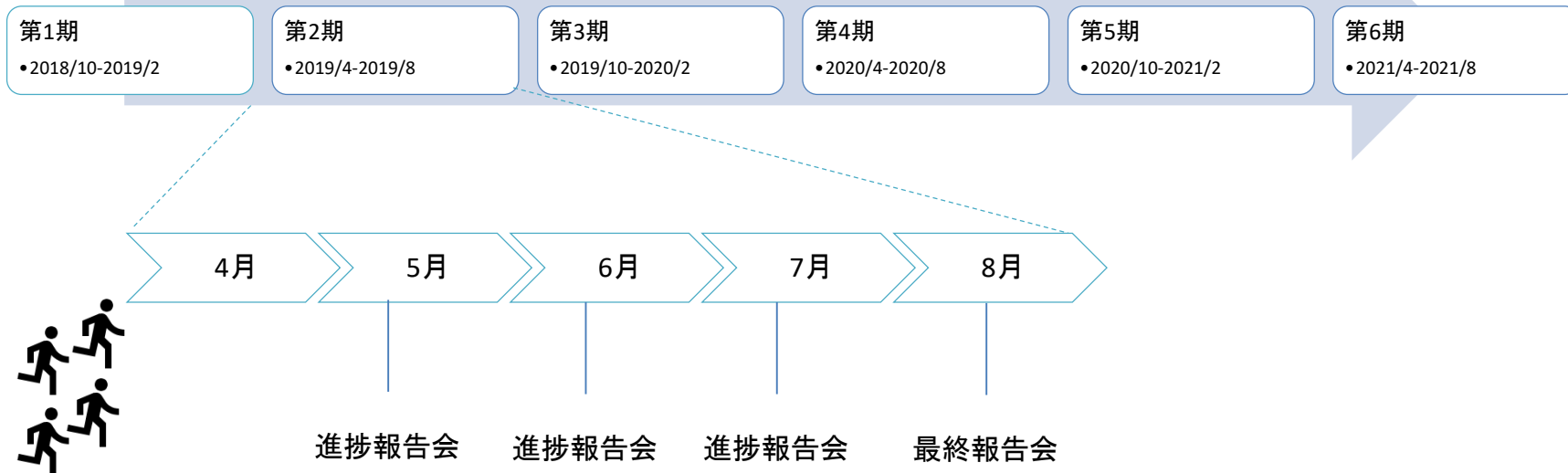
まとめ

- ブロックチェーンの話の一部しか触れられなかったが、ブロックチェーン技術は特長はありつつもまだまだ未成熟の技術領域であり、課題も残されている。
- しかしながら、徐々にそれらの技術的課題を解決している動きが世界的に発生しており、いつかは技術的課題がなくなっていくことが期待される。
- そのようなときを見据えて、自身のビジネスの中に取り入れたり、新しくブロックチェーンを活用したビジネスを検討していくのがよいのではないか。

東京大学ブロックチェーンイノベーション寄付講座 ブロックチェーン学生起業家支援プログラムの紹介

半年に一回実施。第2期の参加学生募集中(～3/3)

<https://www.blockchain.t.u-tokyo.ac.jp/>



人的サポート

上場企業、ベンチャーキャピタル、ベンチャー企業、Tech系企業、ブロックチェーン専門企業、法律家などで構成されるパートナー企業、協力企業・団体から事業立案、アプリ開発など様々なアドバイスを受けることができます。



環境サポート

本郷キャンパス内にある専用スペースの使用権が与えられます。専用スペースは、グループワークなどで使用できるスペースの他、完全個室で知的活動に集中できるスペースが提供されます。

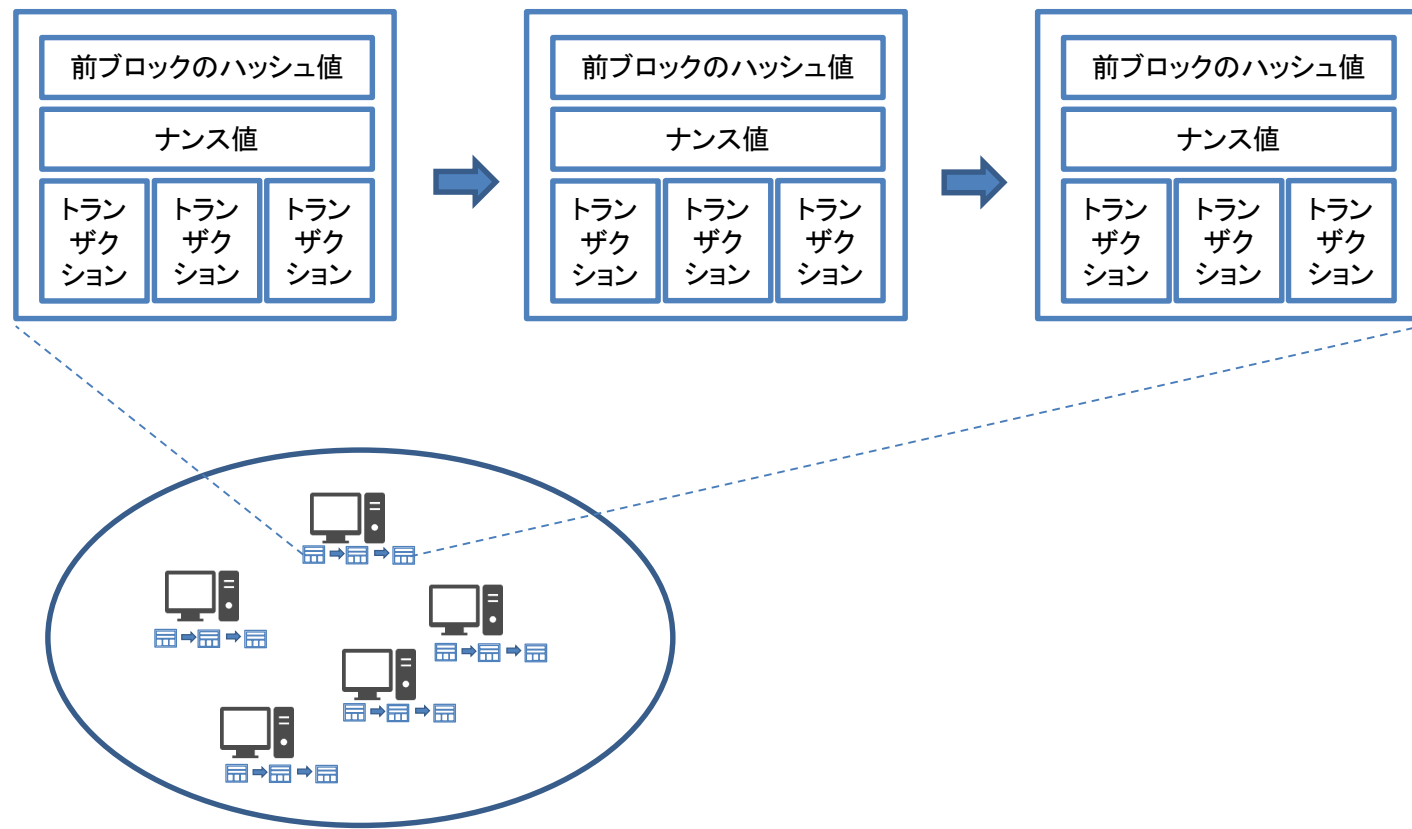


資金サポート

プログラム期間を通して最大45万円の謝金が支払われます。また、各参加者には10万円の予算が与えられます。参加者はこの予算をプログラム期間中に自身の事業計画立案、アプリケーション開発のために使用することができます。

透明性

- 透明性
 - トランザクションのすべての情報が入っているブロックチェーンが誰にでも閲覧可能になっている

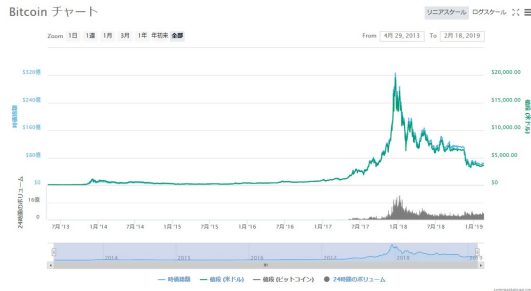


それぞれの課題に対して解決を図っているプロジェクトがある
— 透明すぎて支払い情報が全世界に公開されてしまう

- 秘匿化の技術 Zcashの事例 — <https://z.cash/>
- ビットコインと同様にトランザクション履歴がブロックチェーンに記録されているが、誰から誰に送金された、という情報が秘匿化されている。
- 「ゼロ知識証明」という技術が用いられている。



もしビットコインが世界で広く普及したら・・・ 想定される問題点



2019-02-20 9:00 A→B 1BTC
2019-02-20 9:01 D→K 3BTC
2019-02-20 9:05 E→C 0.1BTC
...



- 価格が過剰に変動してしまう
- 透明すぎて支払い情報が全世界に公開されてしまう
 - アドレス情報と個人は紐付かないという想定しかされていない
- トランザクションが確定されるまで時間がかかる
 - ファイナリティに60分