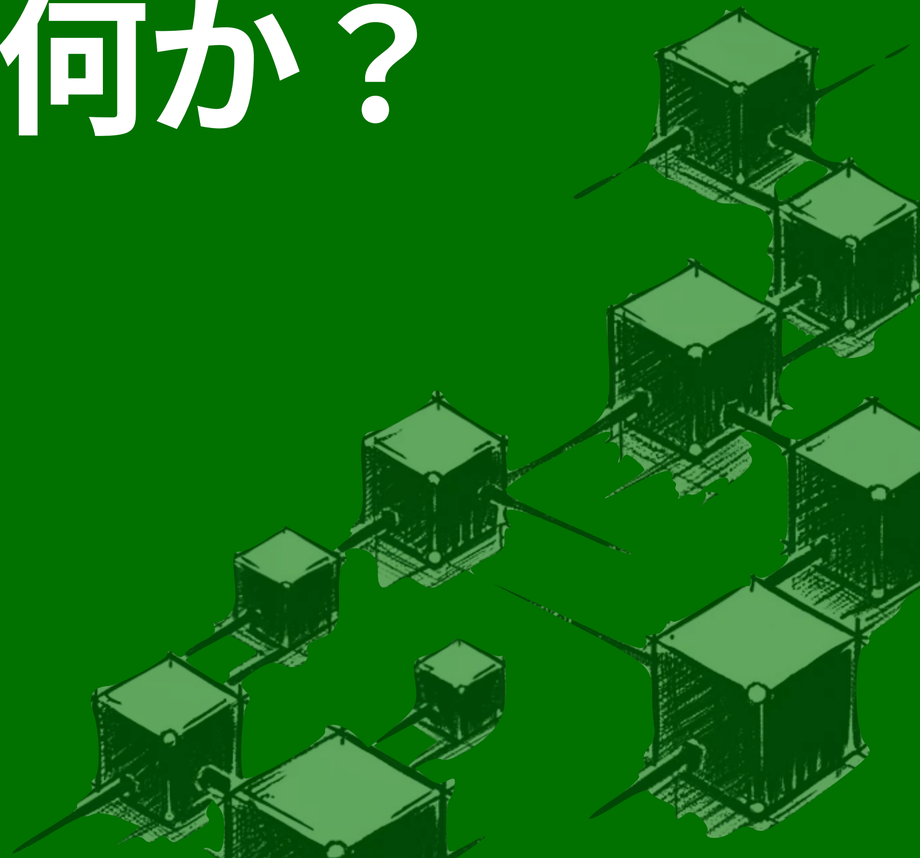
ブロックチェーンとは何か？

What's blockchain tech? (about 30 min)



2024.3.19　Shinji Akematsu (PolarTech.inc)

自己紹介

Self Introduction

- 明松 真司 （あけまつ しんじ）
- 釧路高専情報工学科 → 東北大学理学部数学科
- 宮城県情報サービス産業協会 講師
- 滋慶学園COMグループ 名誉教育顧問
- 東京、大阪、名古屋、仙台等、全国でAI入門研修
- 高専のための学習塾「ナレッジスター」創業者
- 【著書】

  「線形空間論入門」(プレアデス出版)

  「徹底攻略ディープラーニングG検定問題集第2版」(インプレス)

  「Pythonで超らくらくに数学をこなす本」(オーム社)

  「１週間でLaTeXの基礎が学べる本」（インプレス）

「インターネット以来の大発明！！」

NFT!!

ブロックチェーン(block chain)

仮想通貨！チェーン

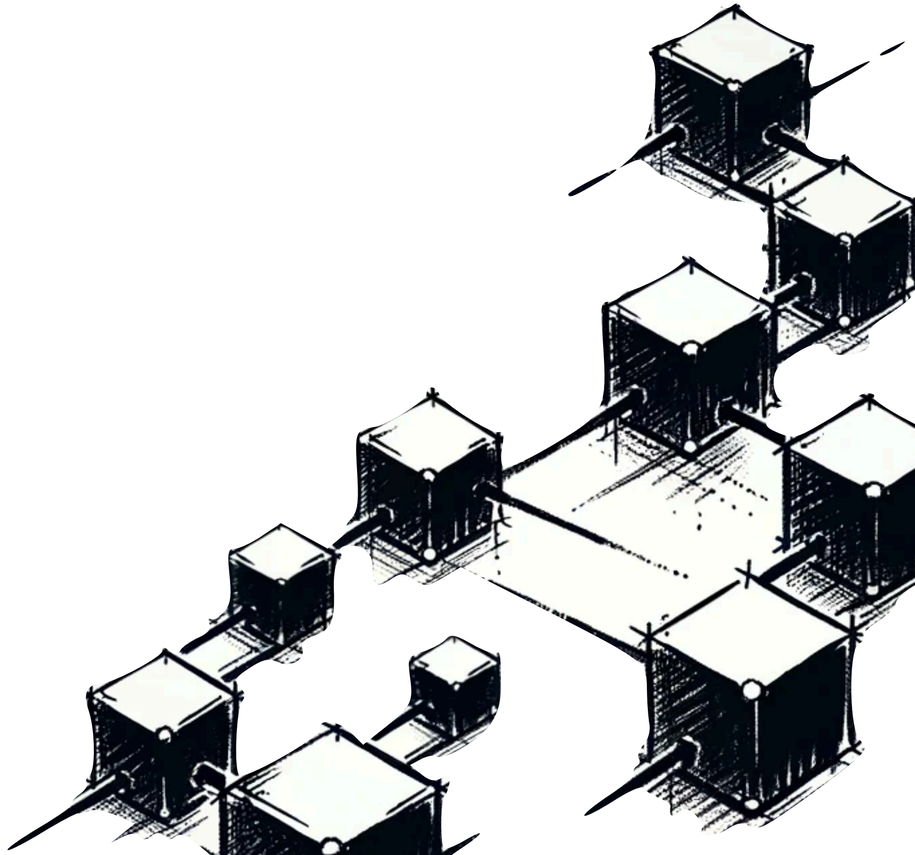
非中央集権!!

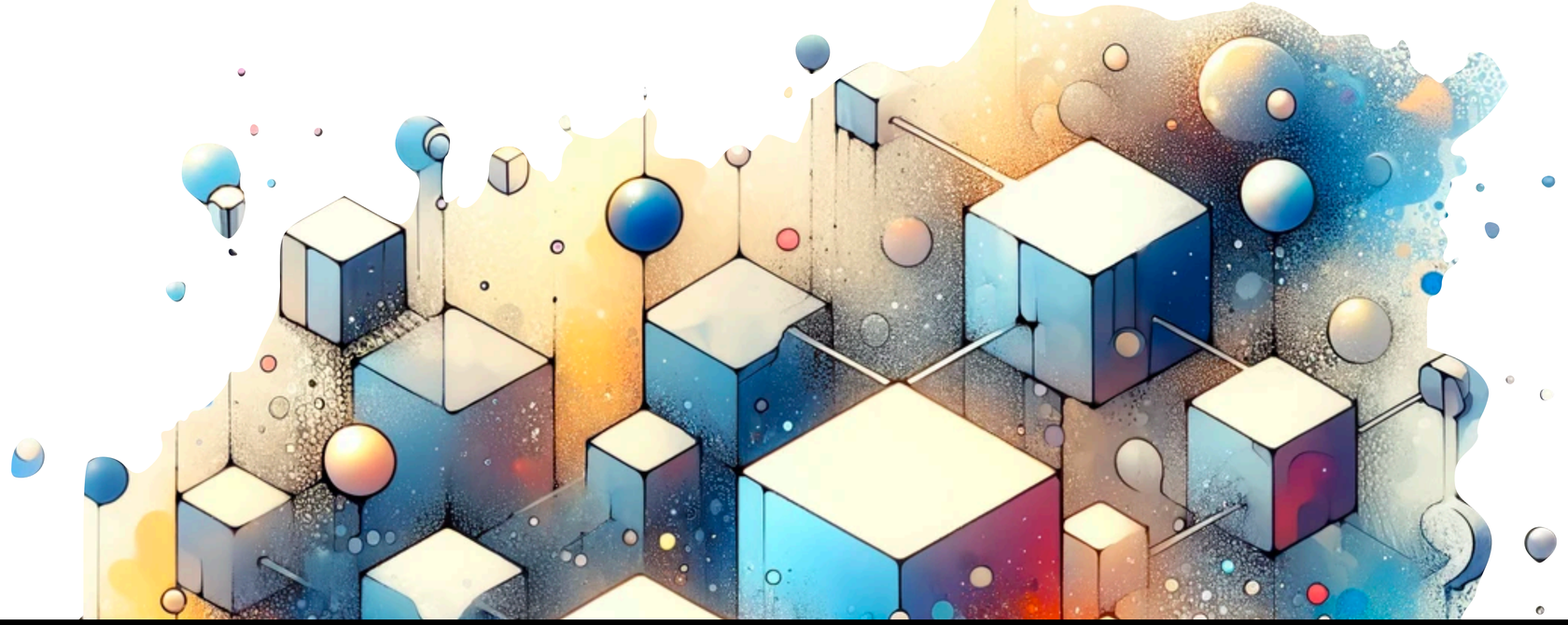
億万長者！

Web3.0!!

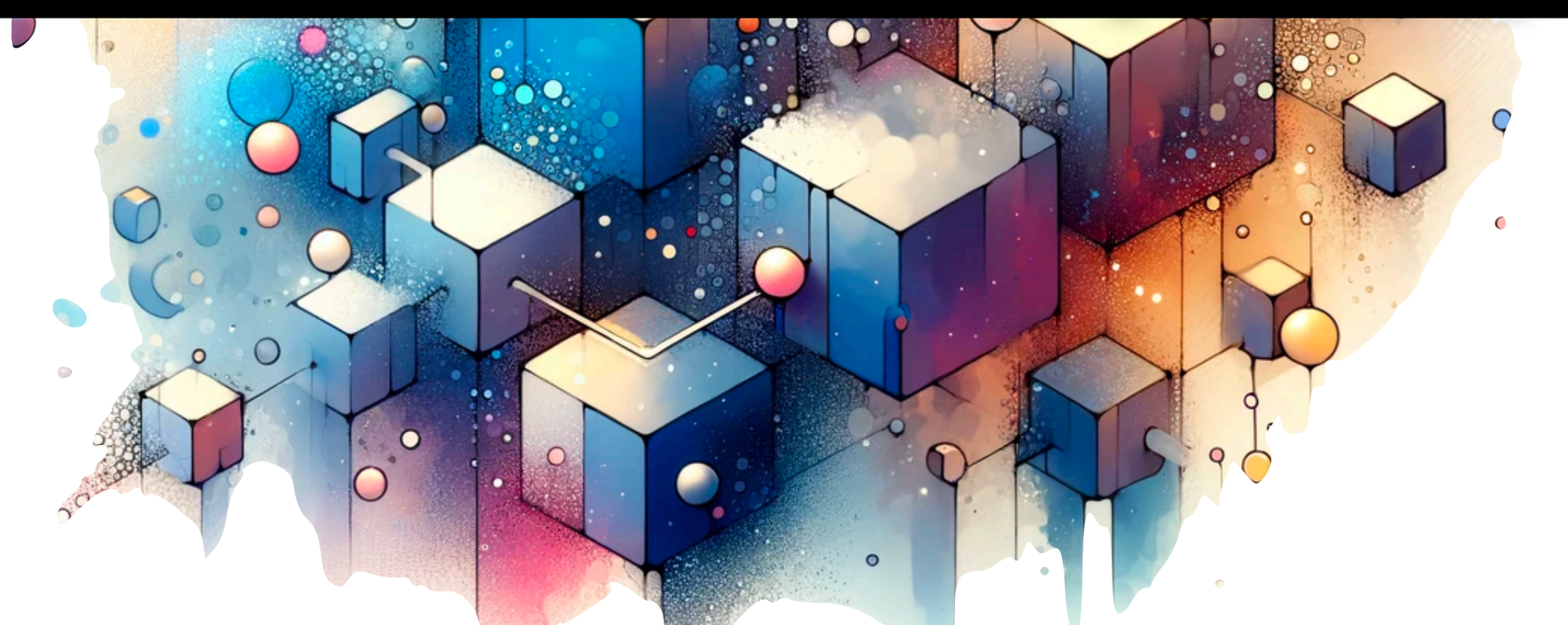
残念ながら、思われがちなこと

- 怪しいのではないか。
- 意識高い系なのではないか。
- 詐欺的なのではないか。





「可能性のかたまり」な技術



新しいお金の形。

ブロックチェーンのはじまり

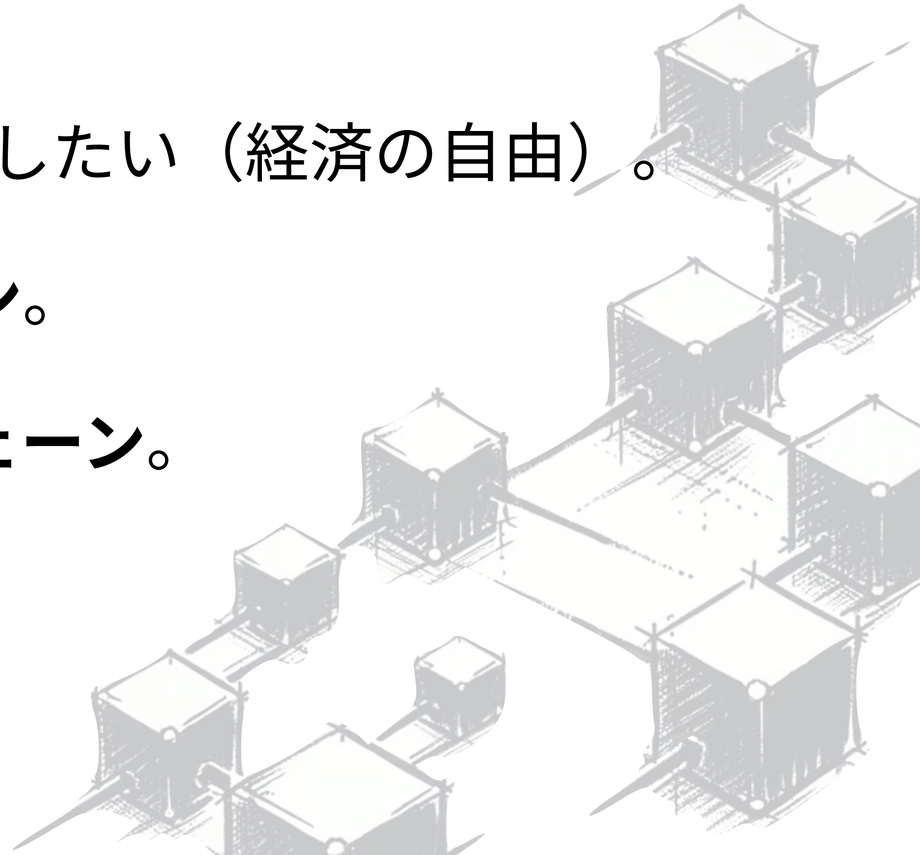
beginning of blockchain.

- ブロックチェーンが初めて提唱されたのは、**ビットコイン**を実現するための仕組みとして（Satoshi Nakamoto 『Bitcoin: A Peer-to-Peer Electronic Cash System』）。
- 現代は、ビットコインだけではなく、様々な分野にブロックチェーンが応用されている。
- その仕組みの見事さのあまり、**インターネット以来の大発明**と呼ばれる（...こともある）。

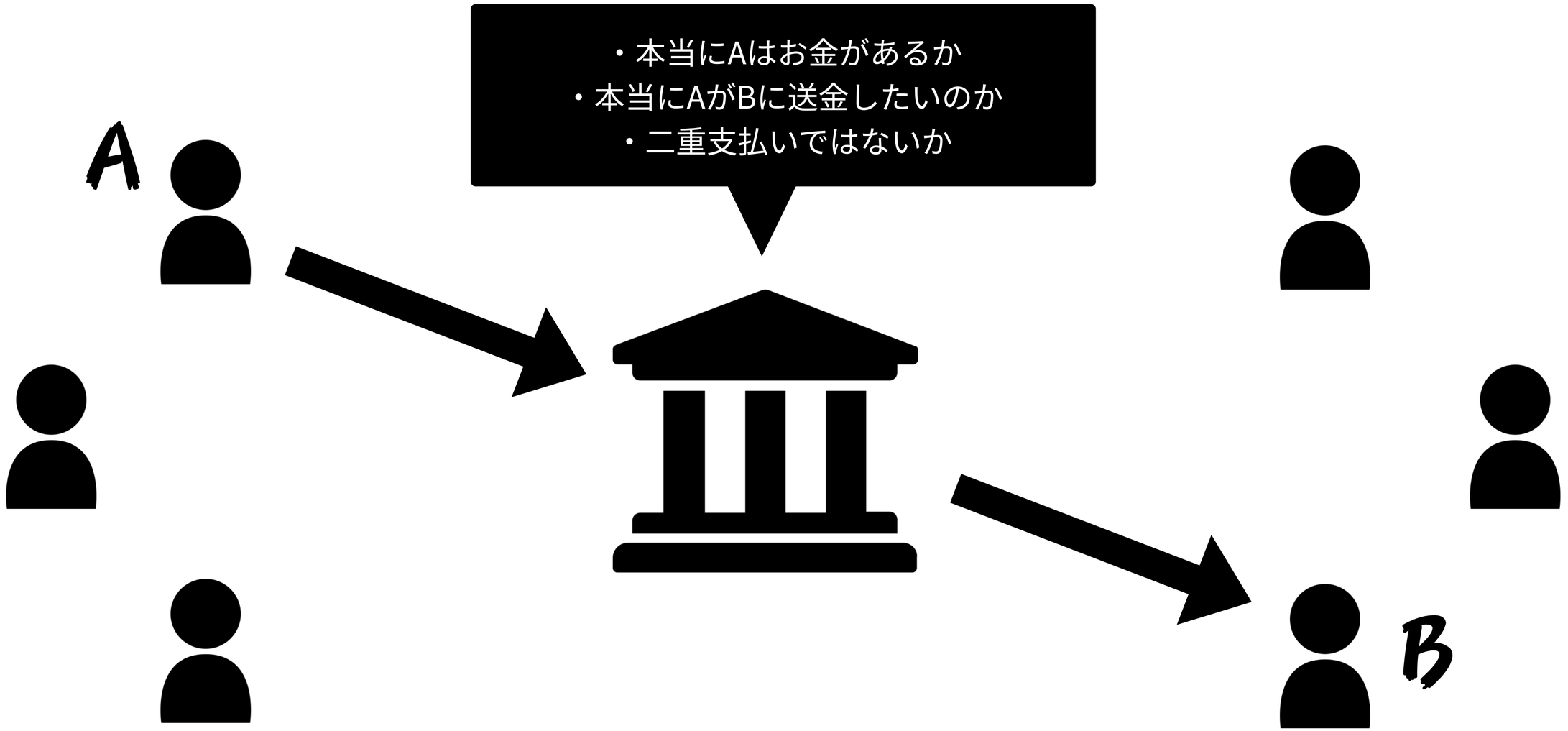
リバタリアニズム
libertarianism

- 根本には **リバタリアニズム**（個人・経済の自由を重視する自由主義のひとつの形）という自由思想。

- **誰にも管理されない、 みんなが平等なお金**を実現したい（経済の自由）。
- それを実現した画期的な新しい通貨が**ビットコイン**。
- ビットコインが運用されるシステムが**ブロックチェーン**。



従来のお金
traditional money system

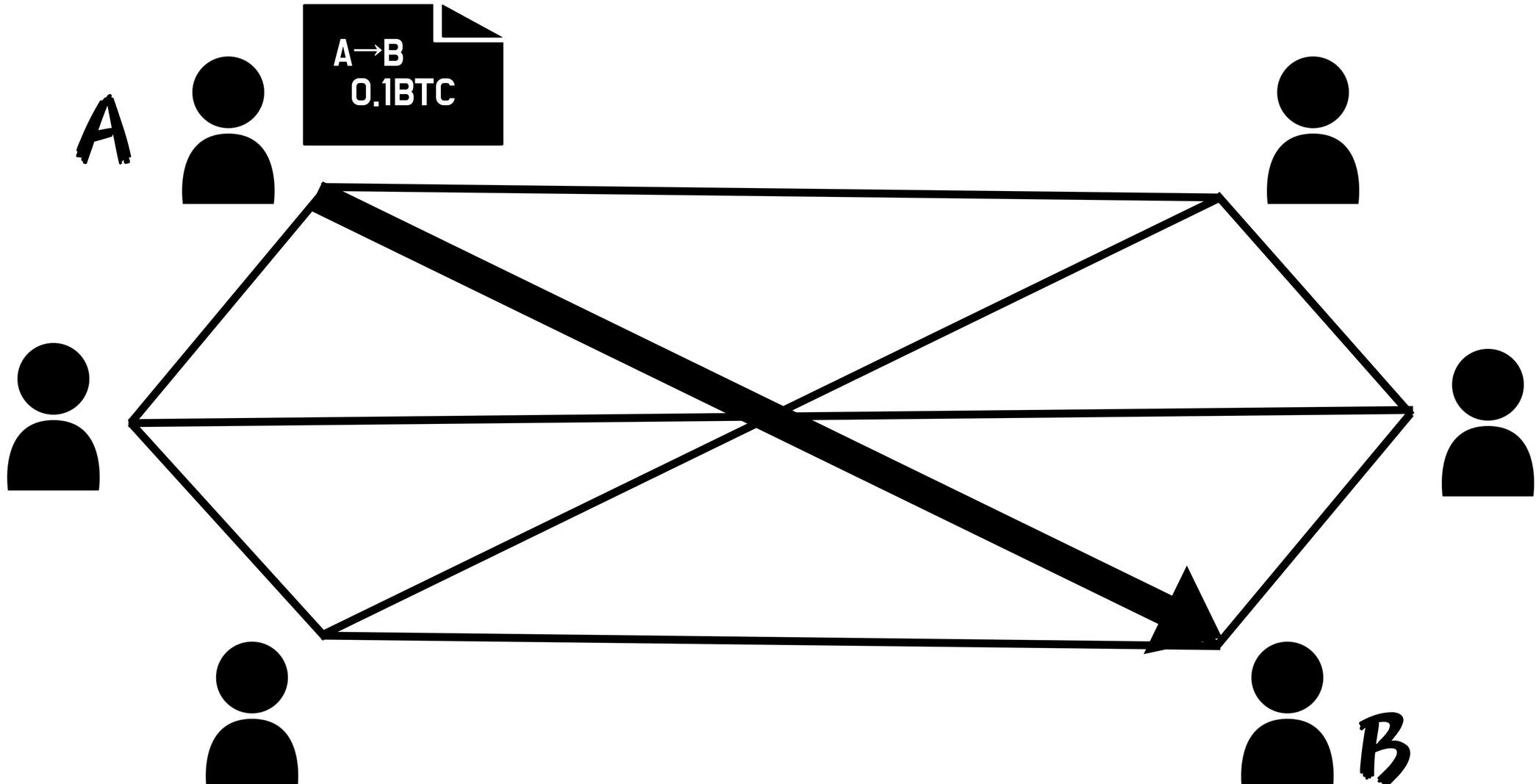


従来のお金
traditional money system

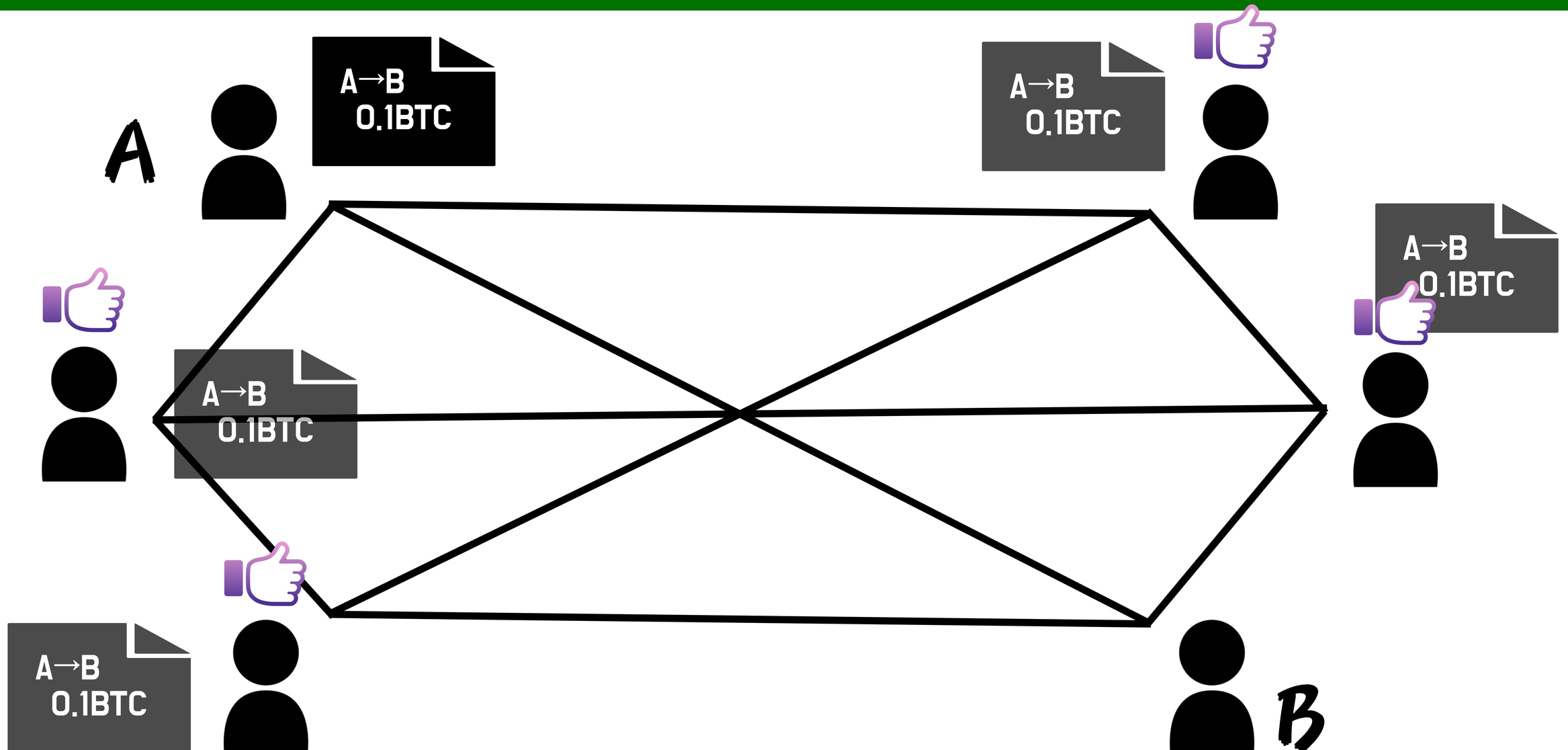
- 従来のお金は**中央集権的**。

ビットコイン

Bitcoins system

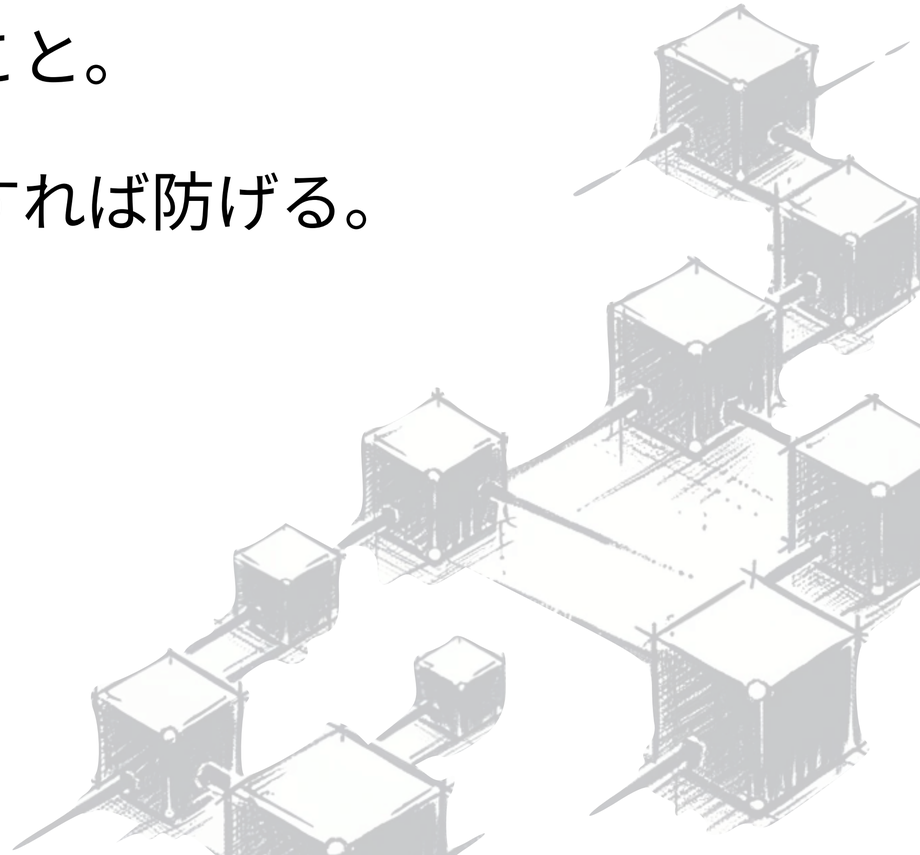


ビットコイン
Bitcoins system



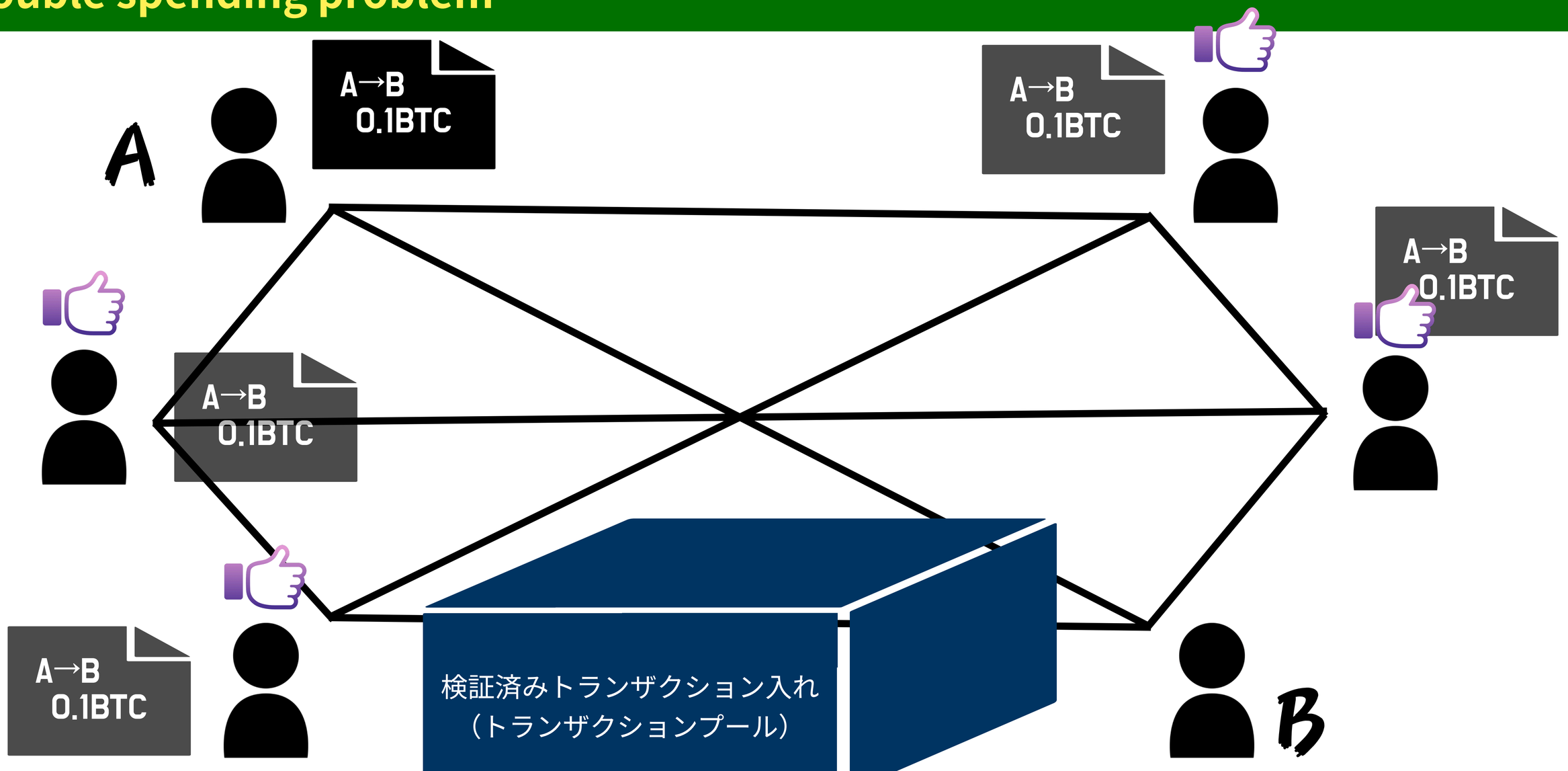
二重支払い問題
double spending problem

- ビットコイン以前の仮想通貨で最も問題だったのが**二重支払い問題**
- 二重支払いとは、同じお金を複数回使ってしまうこと。
- 中央集権型であれば、中央機関が取引履歴を管理すれば防げる。
- 仮想通貨ではこれが難しかった
- **ビットコインでは、これが防がれている！**

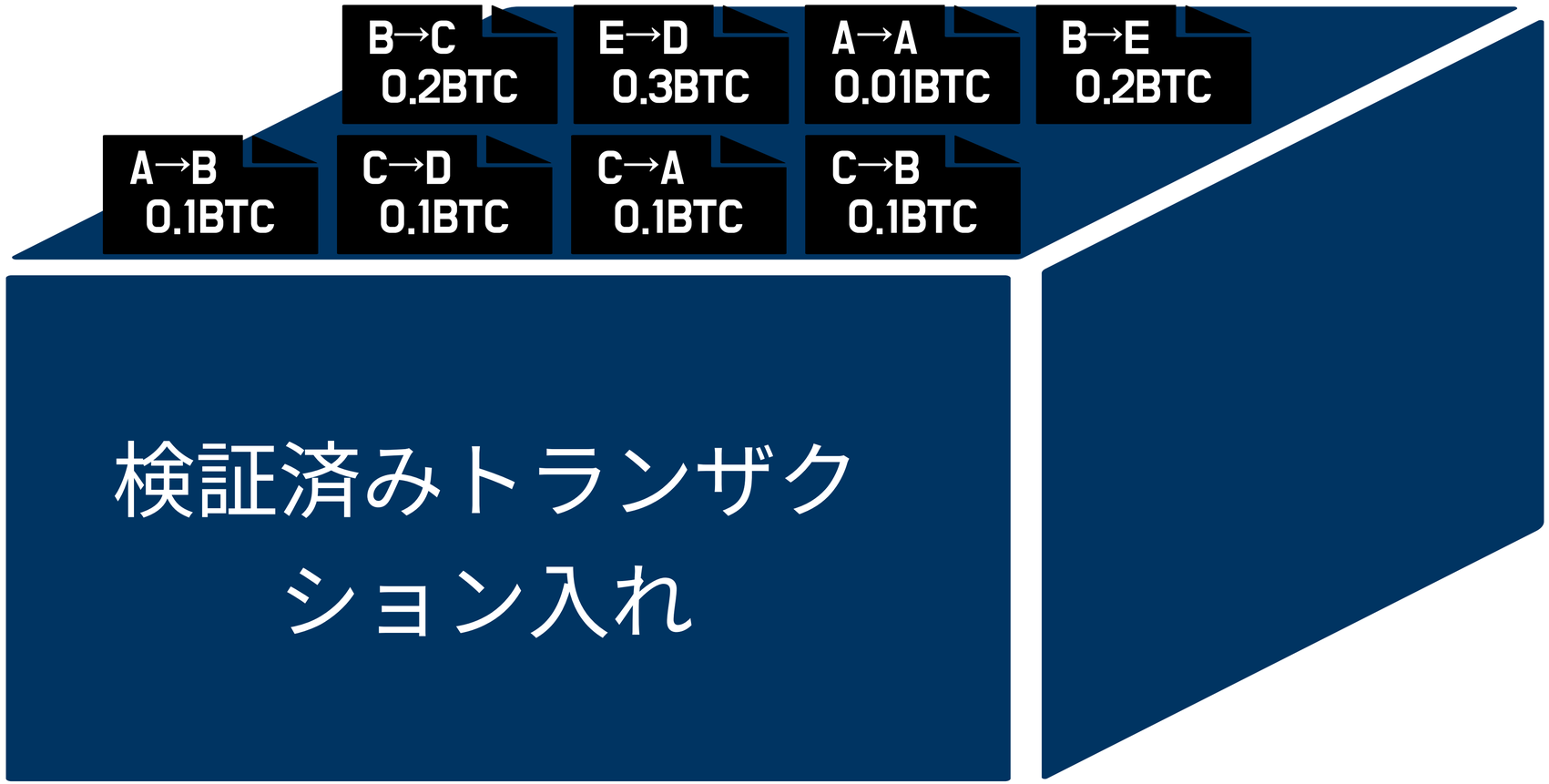


二重支払い問題

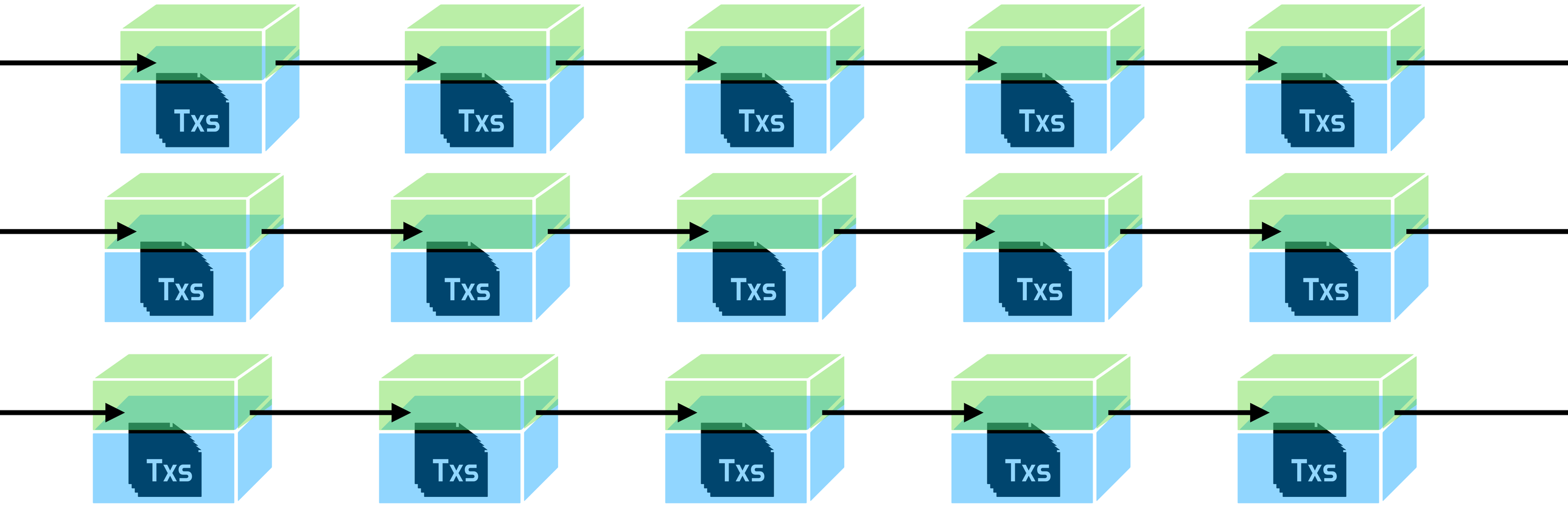
double spending problem



二重支払い問題
double spending problem



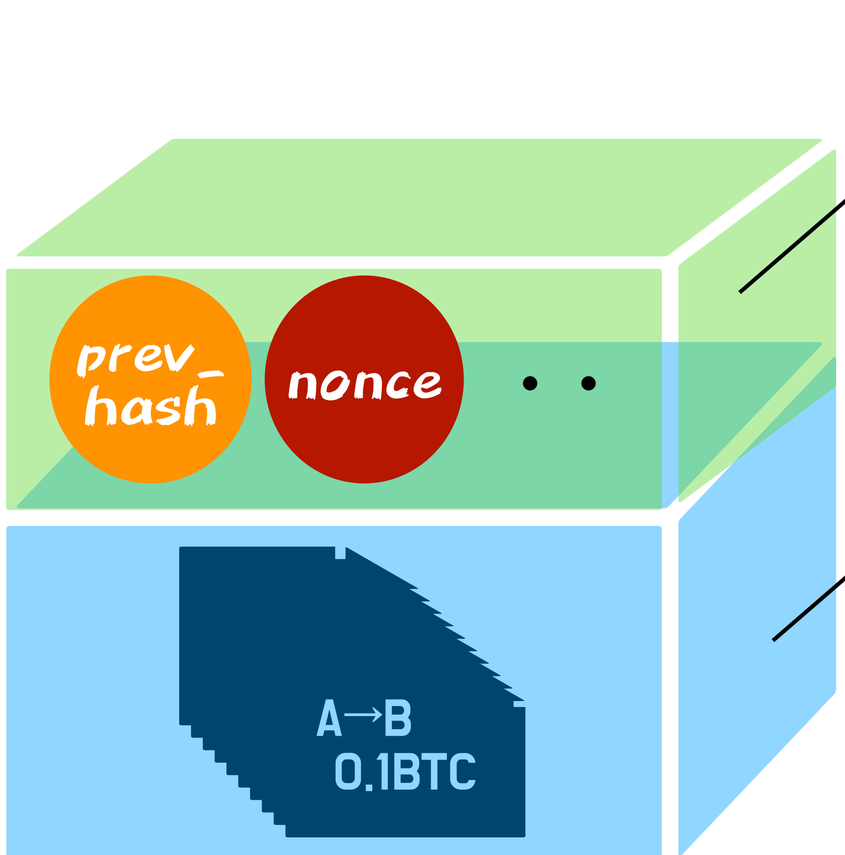
二重支払い問題
double spending problem



ブロックチェーン（事実上改ざんができない）

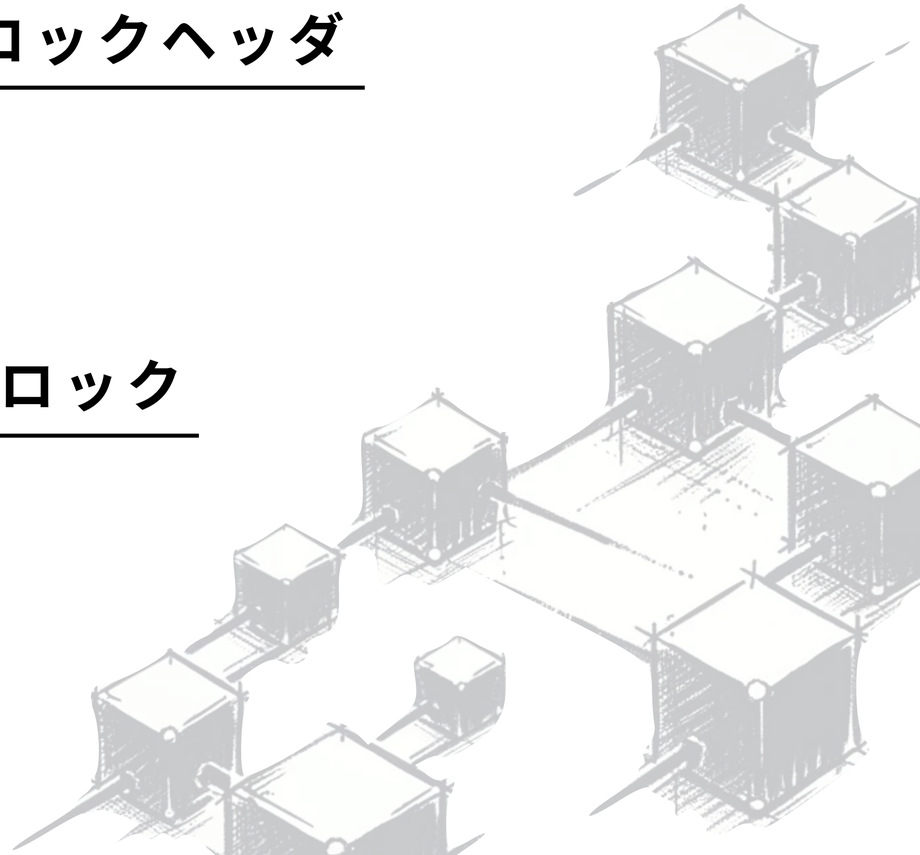
ブロックとブロックヘッダ
Block and block header

- **ブロック**はトランザクションの集まり。**ブロックヘッダ**には様々な情報が入っている。



ブロックヘッダ

ブロック

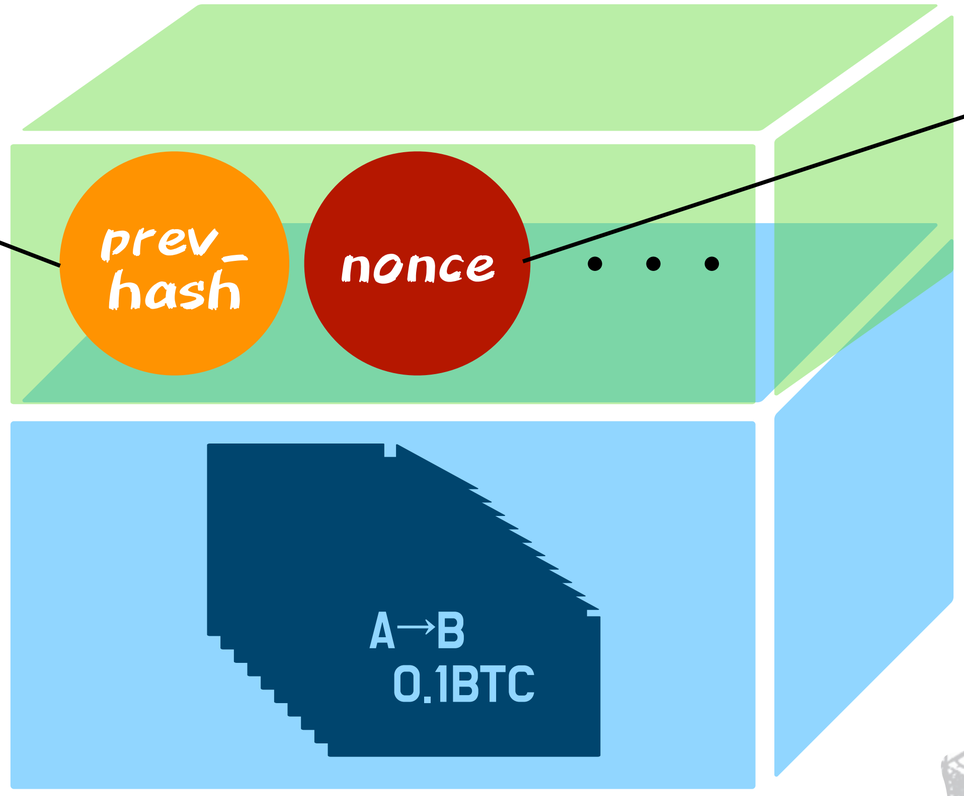


ブロックヘッダの構造

Structure of block header

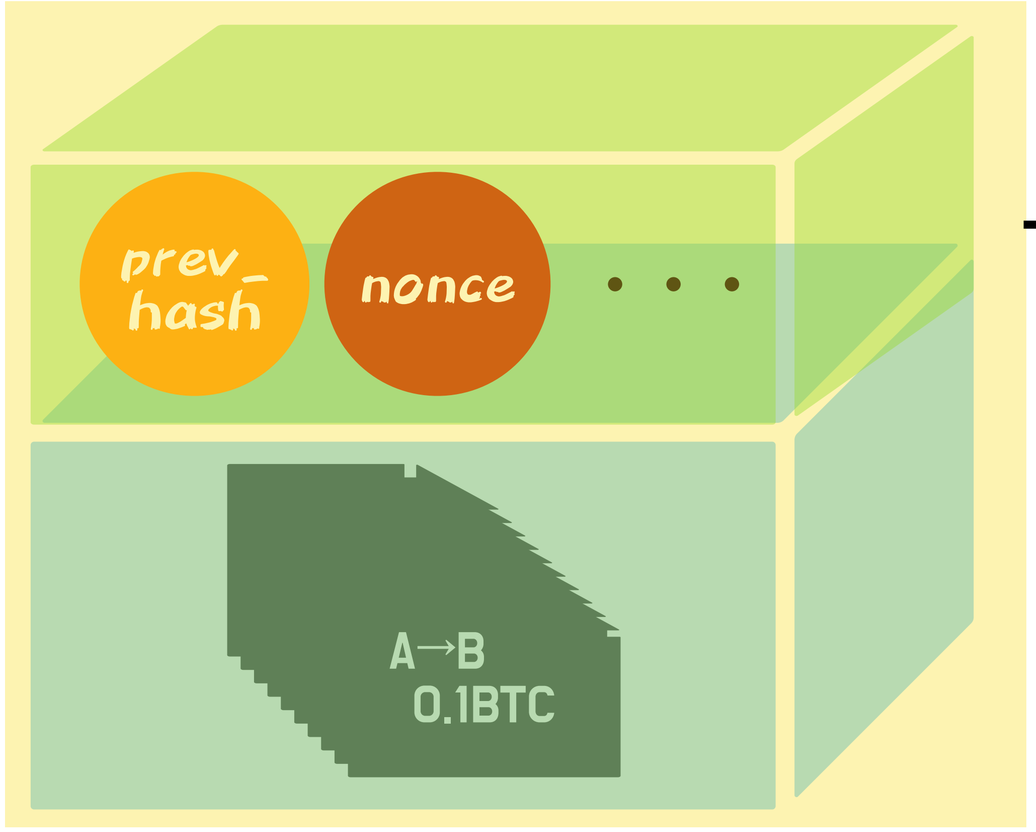
前のブロックの
ハッシュ値

無意味な数



ブロック条件
Block condition

- 以下の条件を満たさないと、**ブロックはブロックとして認められない。**



ハッシュ化

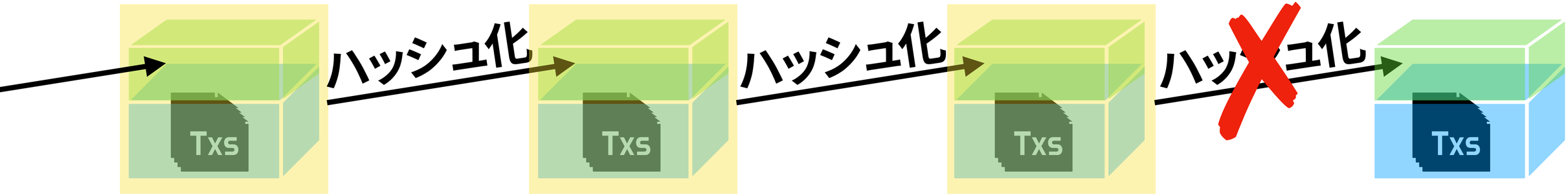
9c6d73d245a26fcb2
788435f7017e84f80
5352c9c720181ddc6
2061d5ae84b6a

< difficulty

e.g.
0x000000FFFFFFFFF
FFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF

注意
important notice

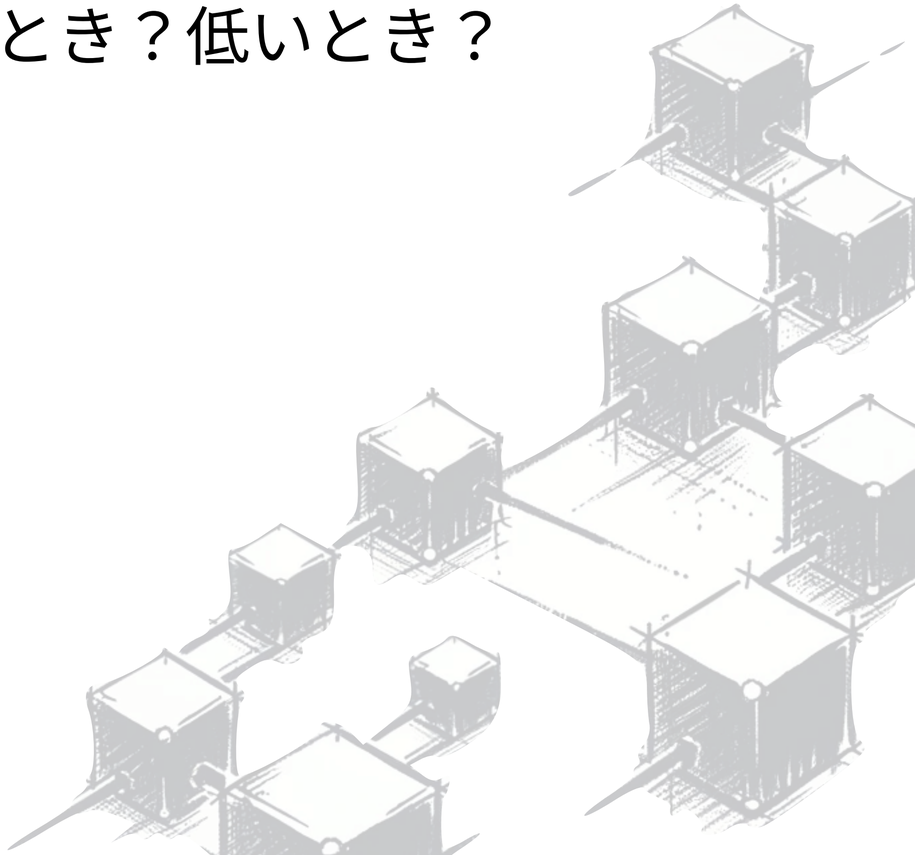
- ブロック条件を満たしていなければ、チェーン更新（マイニング成功）できない。



【マイニングに必要な手順】
・トランザクションを集める（簡単）
・ブロック条件を満たさせる（これが難）

difficultyの調整
tuning of difficulty

- difficultyは**約10分**に1回ブロックが繋がるように自動調整される。
- 【**演習**】マイニングが難しいのは、difficultyが高いとき？低いとき？
- 【**演習**】最新のdiffifultyを調べてみよう。



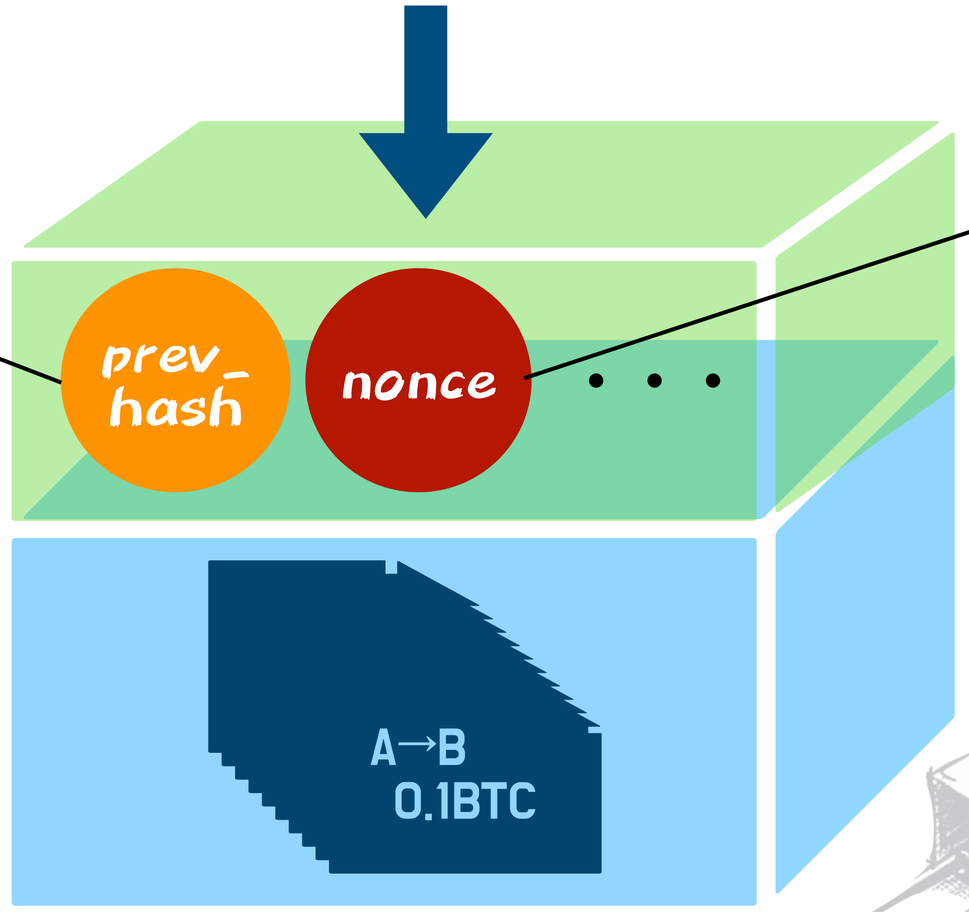
ブロック条件を満たさせるには

how to meet the block condition

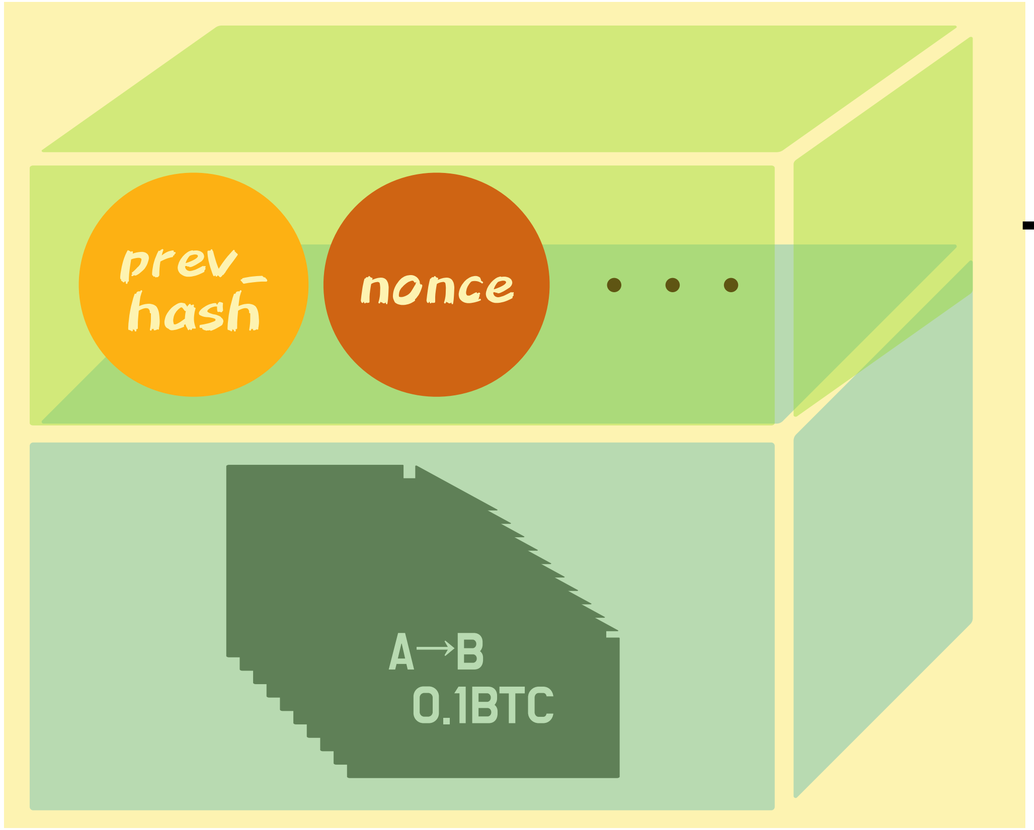
ハッシュを変えるためにはnonceを変える！

前のブロックの
ハッシュ値

無意味な数



nonceを探す
find a nonce



ハッシュ化

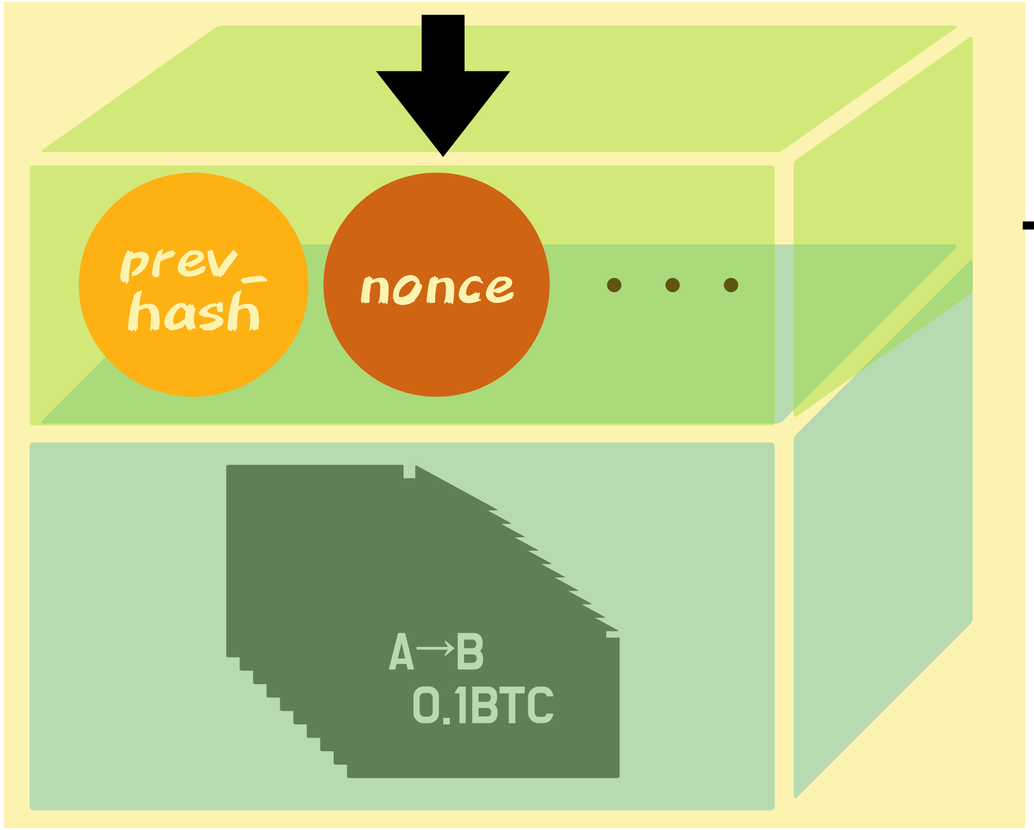
```
9c6d73d245a26fcb2
788435f7017e84f80
5352c9c720181ddc6
  2061d5ae84b6a
```

> difficulty

条件NG
→ 失敗

nonceを探す
find a nonce

nonceをいじってハッシュ値を変える。



ハッシュ化

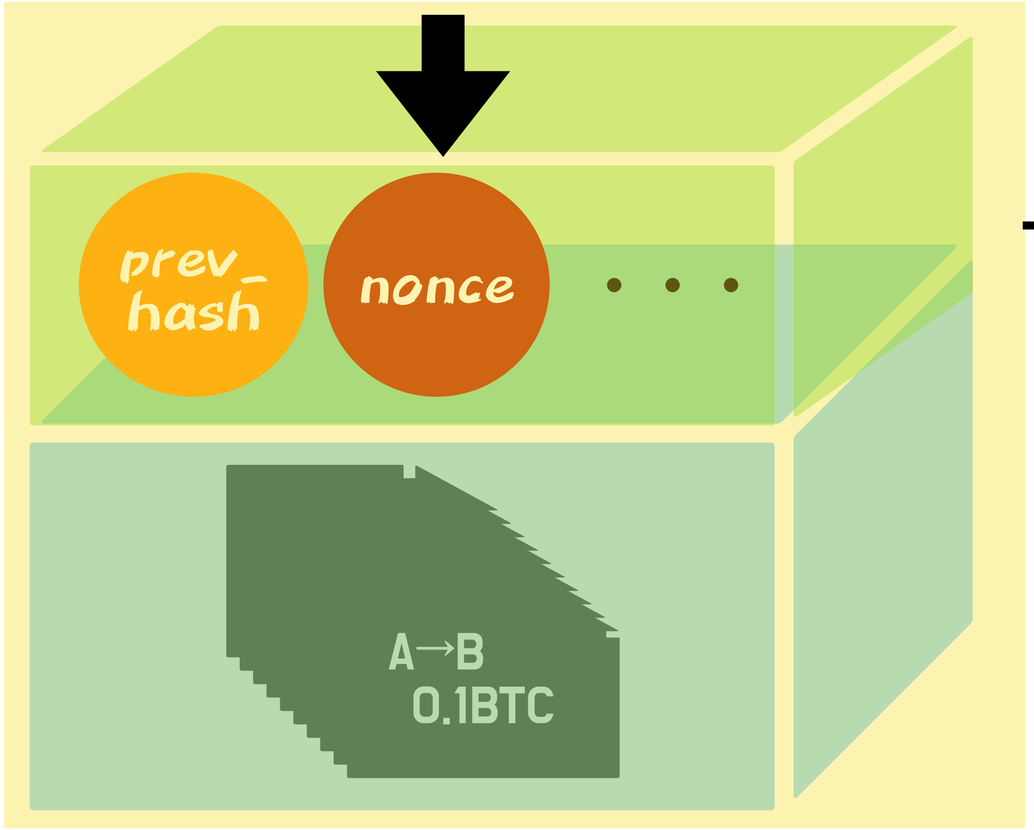
```
18ac3e7343f016890
c510e93f935261169
d9e3f56543642983 0
   faf0934f4f8e4
```

> difficulty

条件NG
→ 失敗

nonceを探す
find a nonce

nonceをいじってハッシュ値を変える。



ハッシュ化

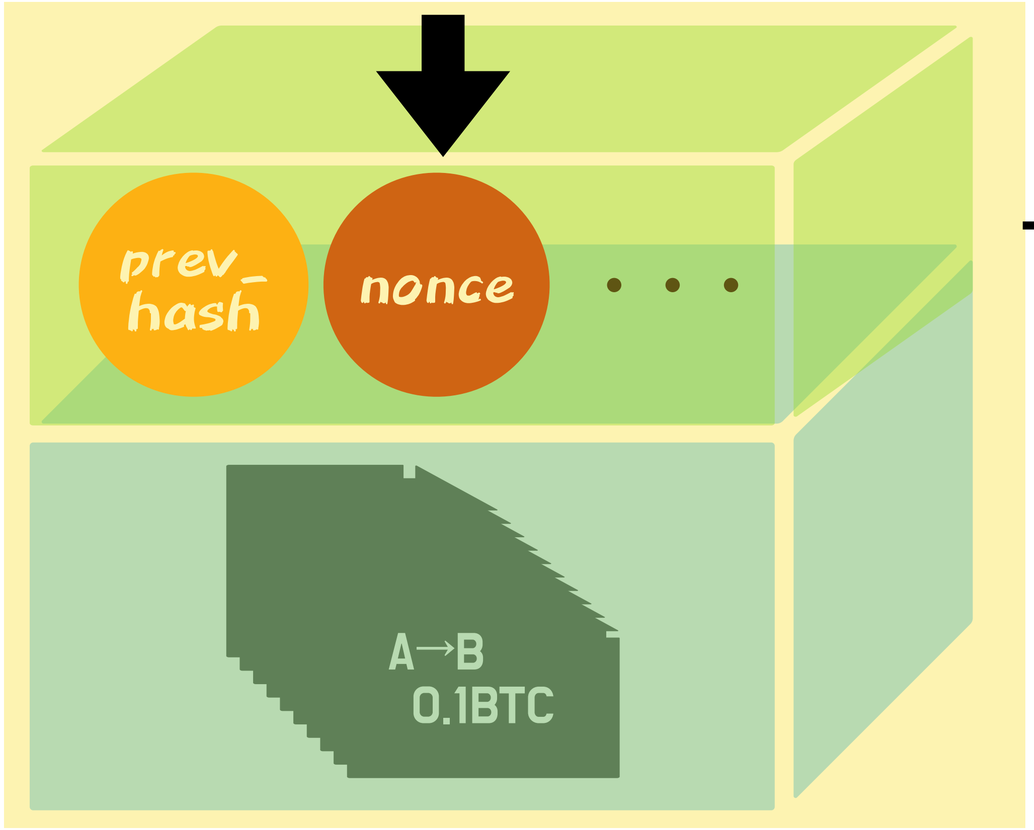
```
de7d1b721a1e0632b
7cf04edf5032c8ecf
fa9f9a08492152b92
  6f1a5a7e765d7
```

> difficulty

条件NG
→ 失敗

nonceを探す
find a nonce

nonceをいじってハッシュ値を変える。



ハッシュ化

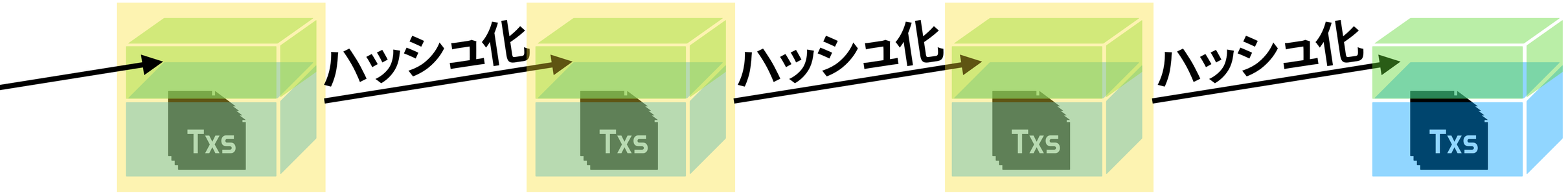
```
0000000000000000
0000000000000000
0000000000000000
  0f1a5a7e765d7
```

< difficulty

条件OK
→ 成功!!

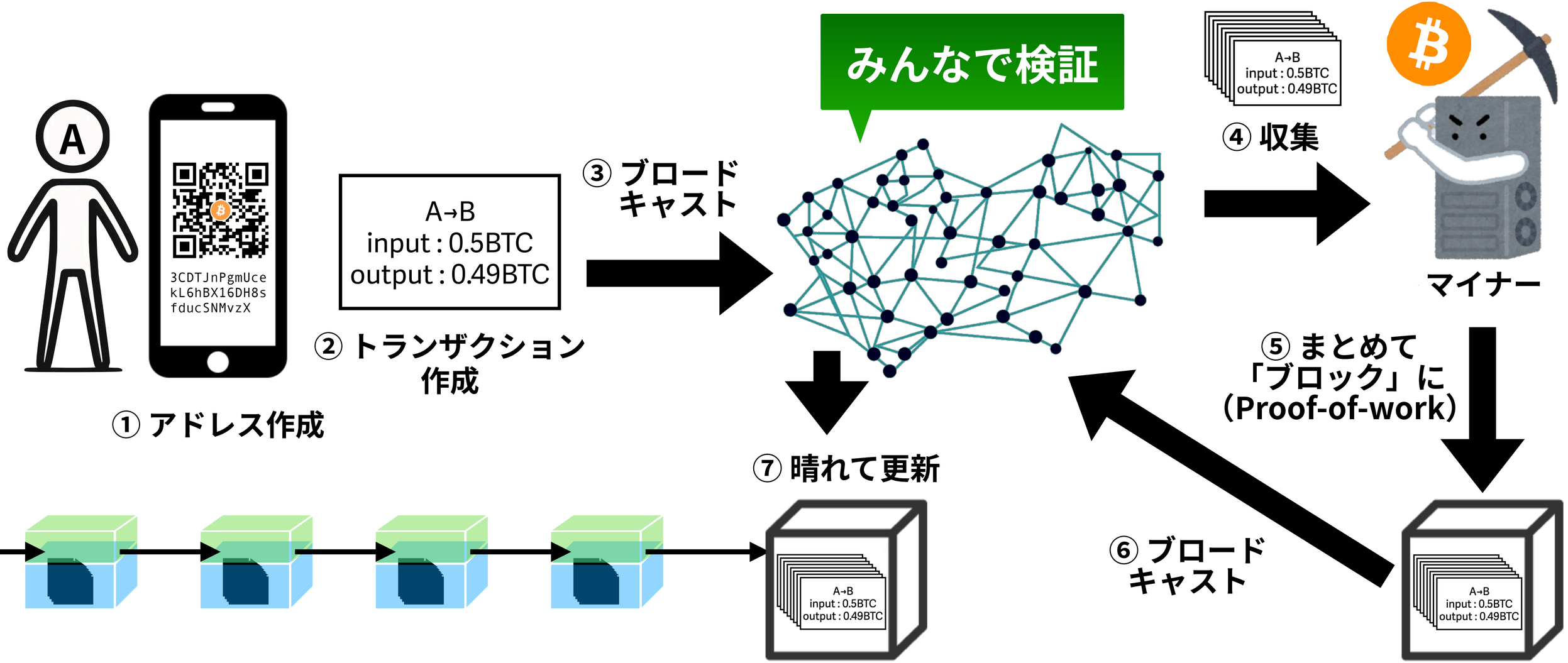
マイニング成功
success mining

- ブロック条件を満たすnonceが見つかったらマイニング成功！
- これを世界中で競うのがProof of Work。
- インセンティブにより、24時間365日これが回り続けている。
（インセンティブで自律的にこれを実現したのがSatoshiの大発明）



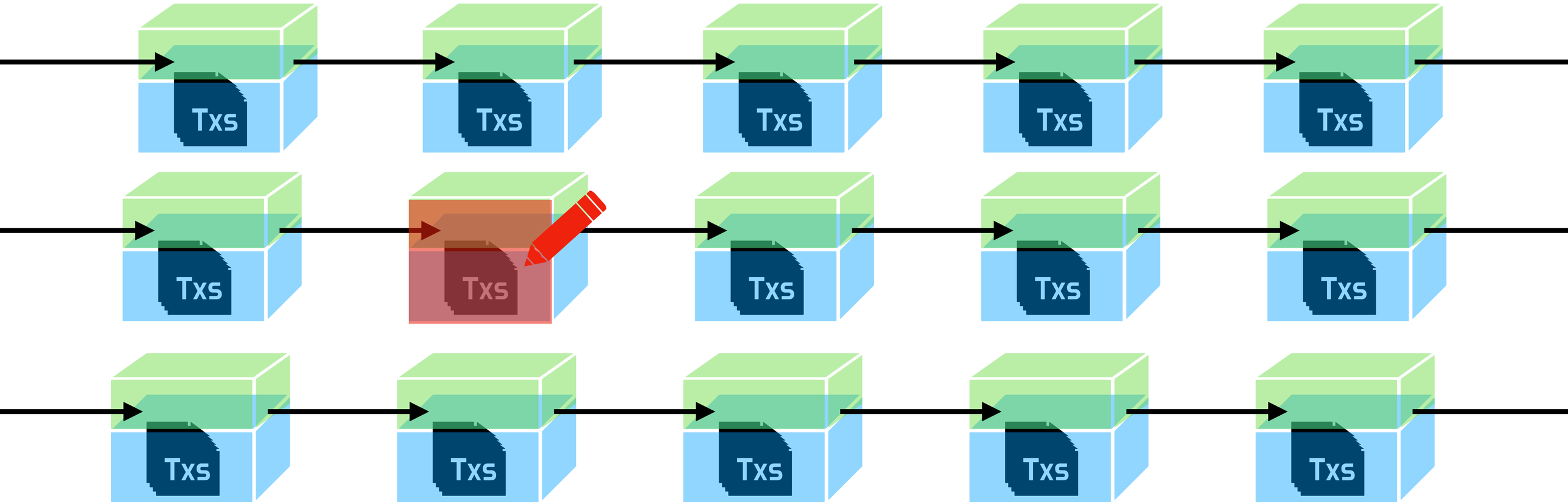
ブロックチェーンの全体像

overview of blockchain

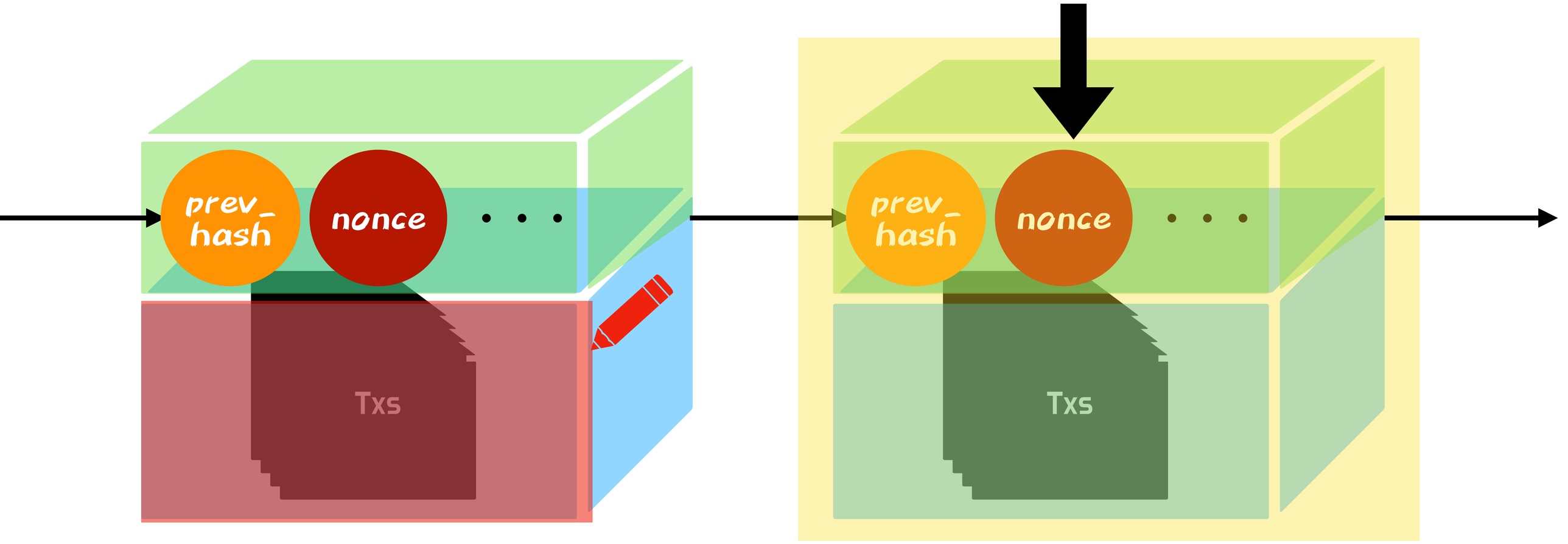


改ざん困難性
Difficulty in tampering

- ブロックチェーンの「改ざん困難性」はProof of Workにより保証される。



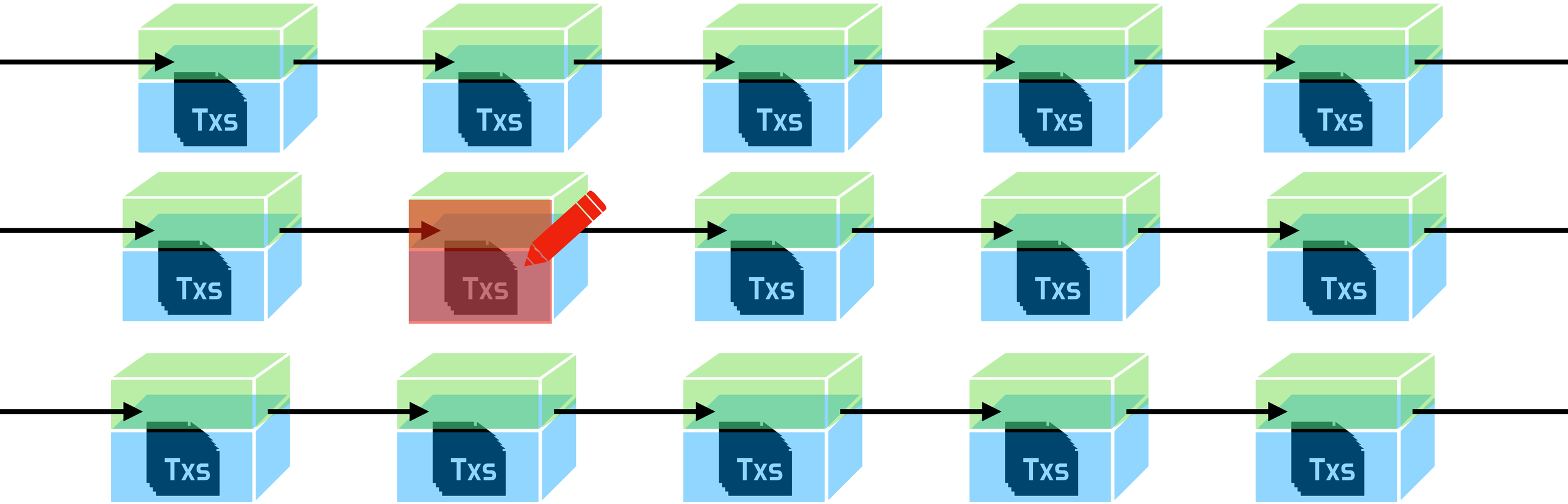
新たなnonceを探さなければならない



ブロック条件を満たさなくなる

改ざん困難性
Difficulty in tampering

- つじつま合わせには、**「最先端に追いつくまでProof of Work」**が必要。

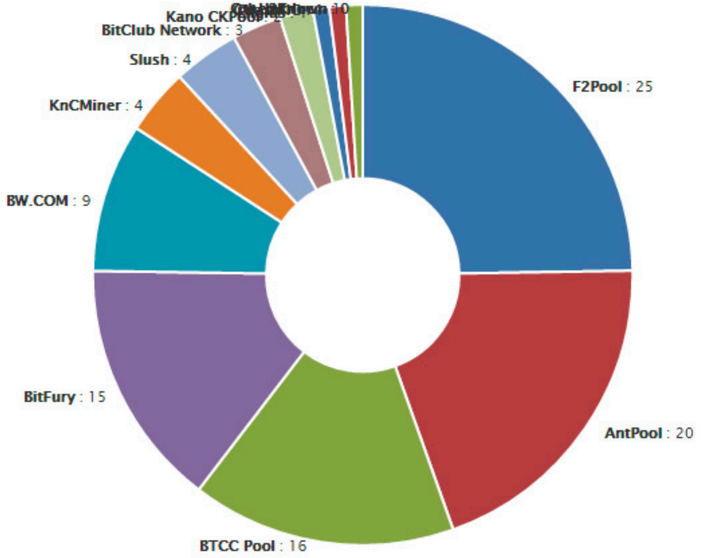


51%攻撃

51% attack

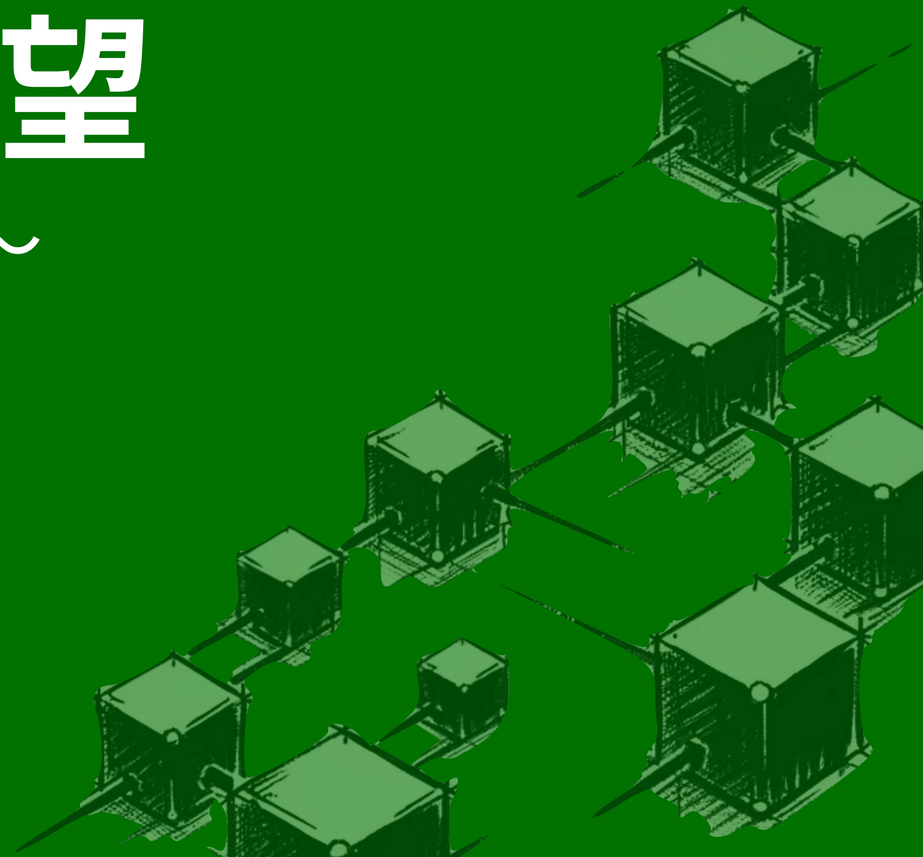
- ネットワークの合計計算能力（**ハッシュレート**）の51%以上をある1人またはグループにより支配されると、改ざんが可能になるおそれがある。

- 分散化の強化（マイナーを分散させる） or コンセンサスアルゴリズムの変更（たとえばProof of Stake など）などが対処として考えられる。



ブロックチェーンの展望

～ブロックチェーンで何が変わるのか？～

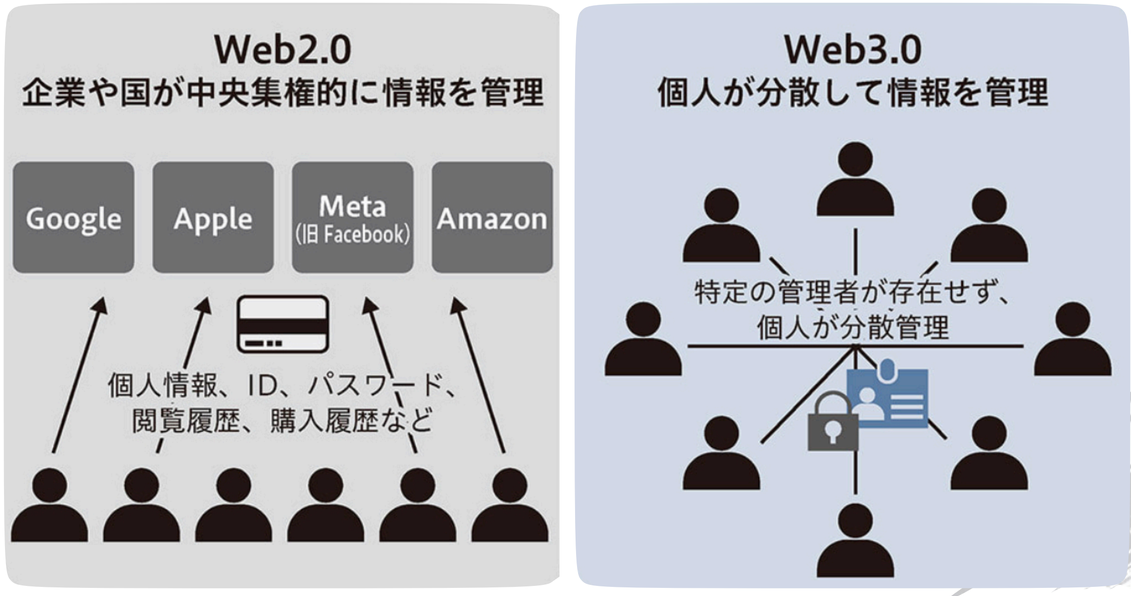


Web3.0

Web3.0

- **Web3.0**とは、ブロックチェーン技術を応用し、今までのインターネットの問題点を解決しようというムーブメントのこと。

- 誰もが公平に利用でき、中央集権的な管理者のいない分散型のインターネットインフラを作ろうという動きを指す。



引用.「Web3.0の教科書」（のぶめい）インプレス

送金が簡単にできる

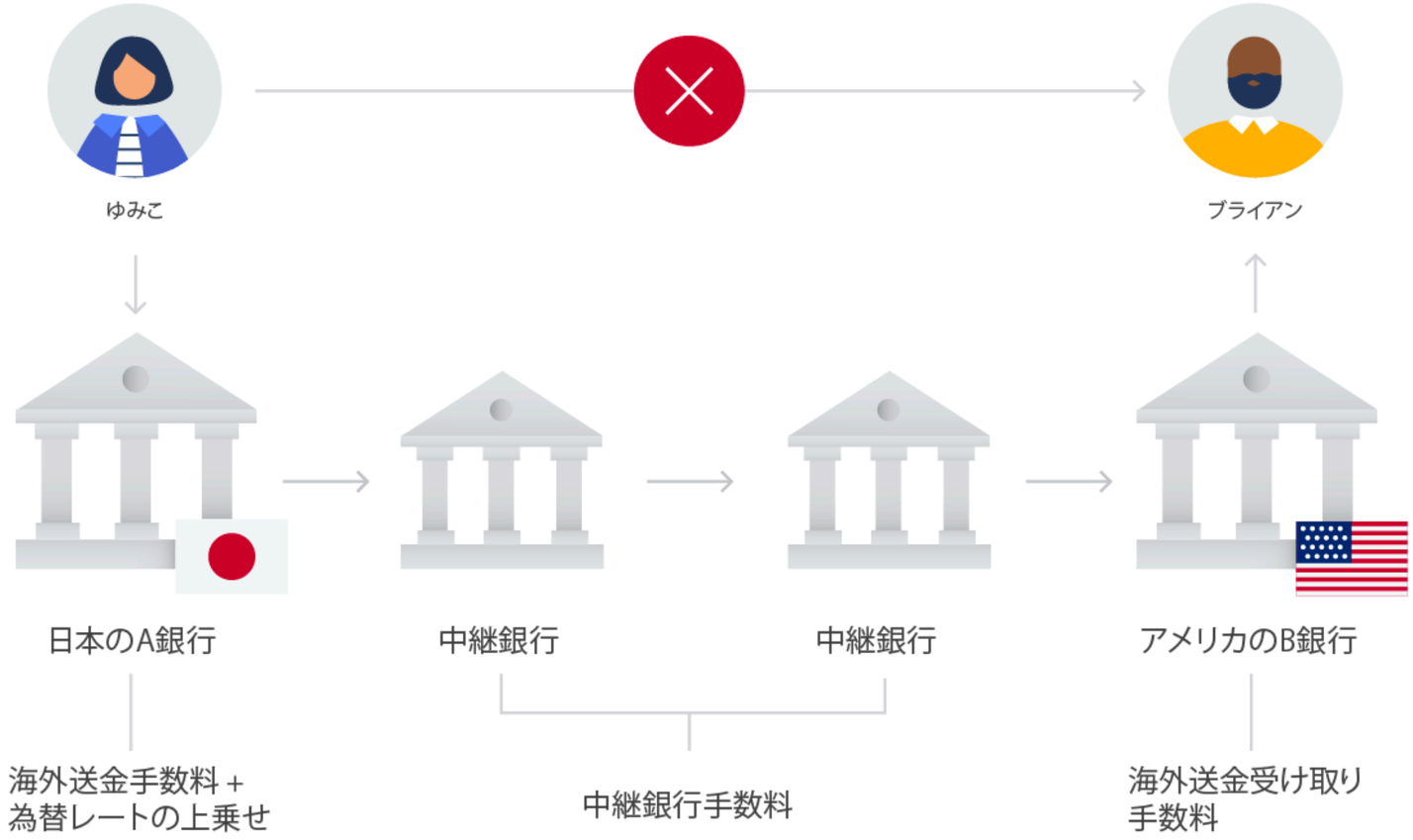
payment

- ブロックチェーンを使うことで、送金を簡単に行える未来。
- （将来的には）少額手数料であらゆる送金ができるようになる。
- 【例】**マイクロペイメント**（yenpoint）
  少額の支払いを暗号通貨の仕組みで簡単にできるように。
  （ネット記事1つ10円、Youtube1再生5円、ChatGPT1質問5円 など）

送金が簡単にできる

payment

- 海外送金なども簡略化＆手数料も安くなる未来（現在はかなり複雑＆手数料高）

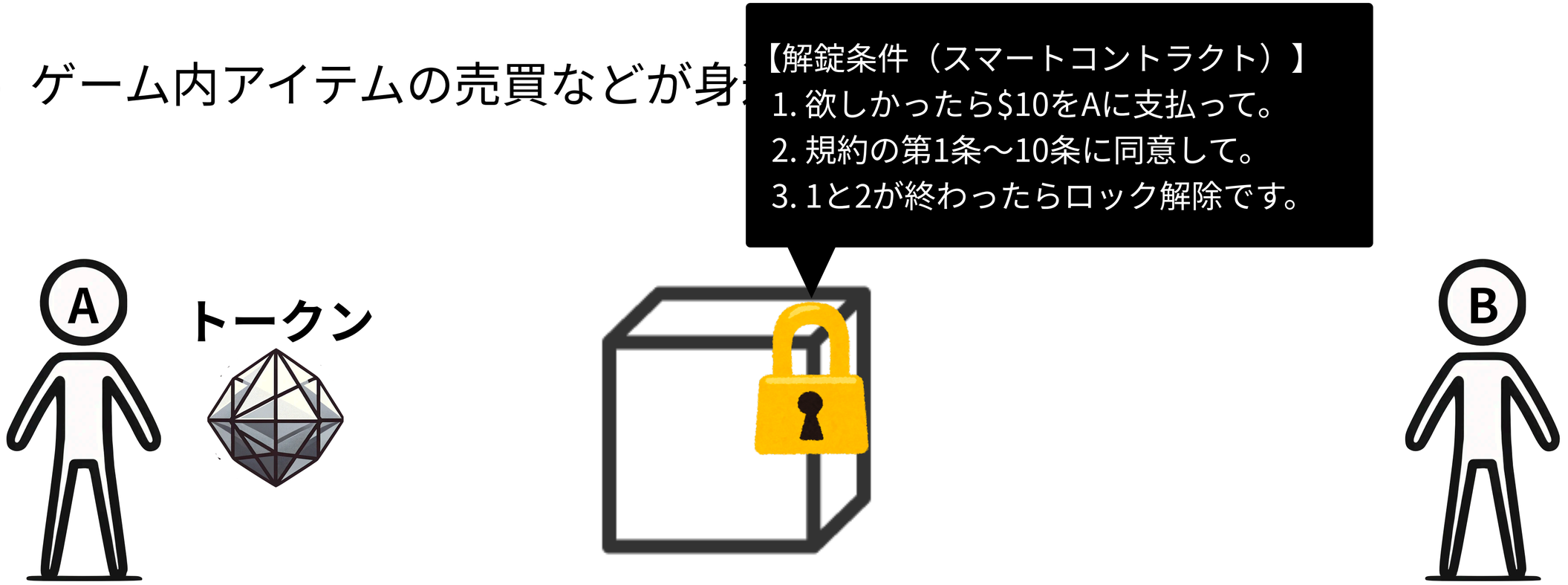


引用. https://wise.com/jp/blog/correspondent-bank

非中央集権型サービス（Dapps）

Decentralized applications（Dapps）

- 管理者がいなくても取引などを行える非中央集権型サービス（**Dapps**）
- **トークン**、**スマートコントラクト**を使って取引が自動化される。
- ゲーム内アイテムの売買などが身

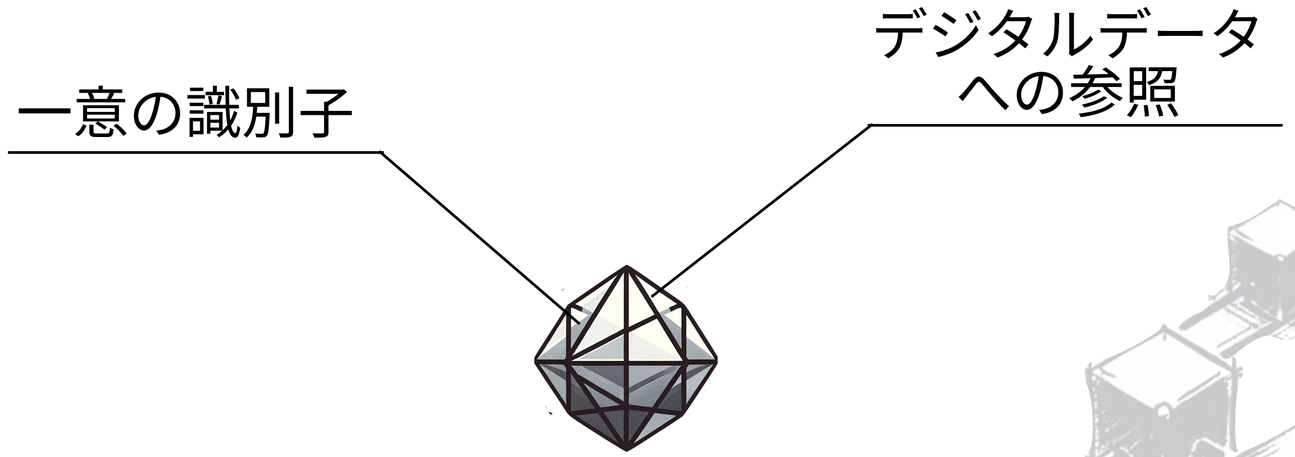


デジタルデータが資産価値を持つ

NFT（Non-fundgeble token）

- **非代替性トークン（Non-fundgeble token）**により、デジタルデータに資産性がうまれる。

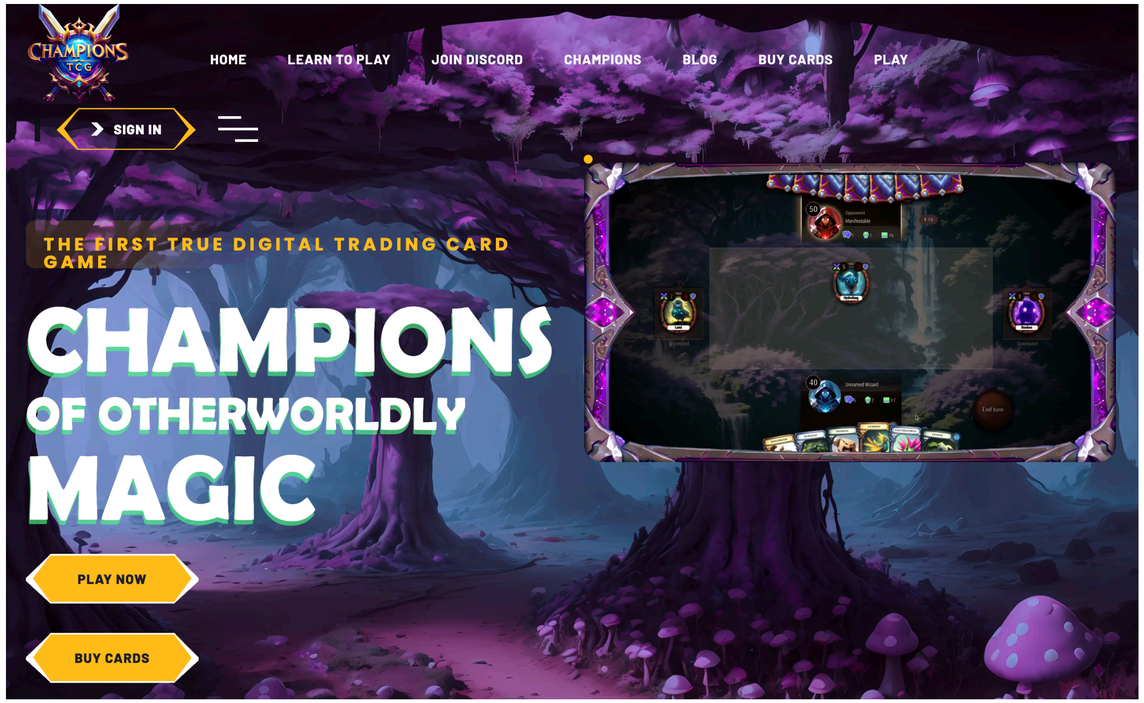
- ※「所有権の証明」とはちょっと違うことに注意。
  （デジタルデータの所有権はそもそも現行法では定義されていない）

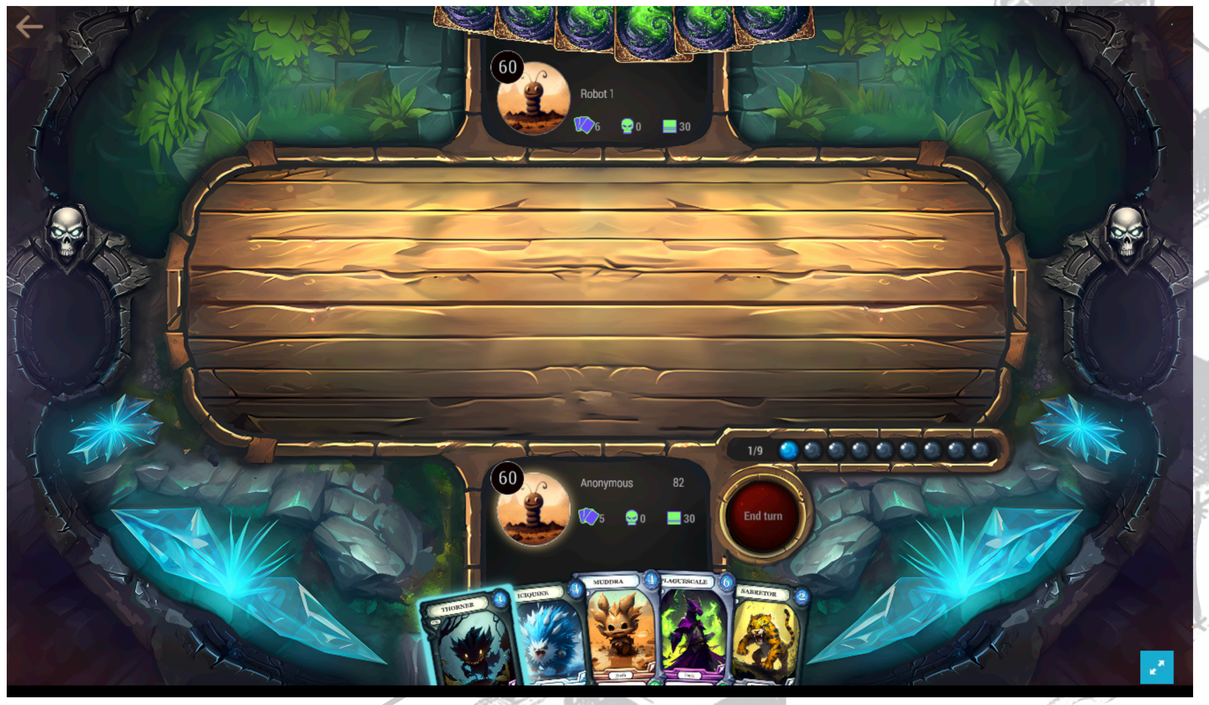


【事例】Champions TCG

Champions TCG

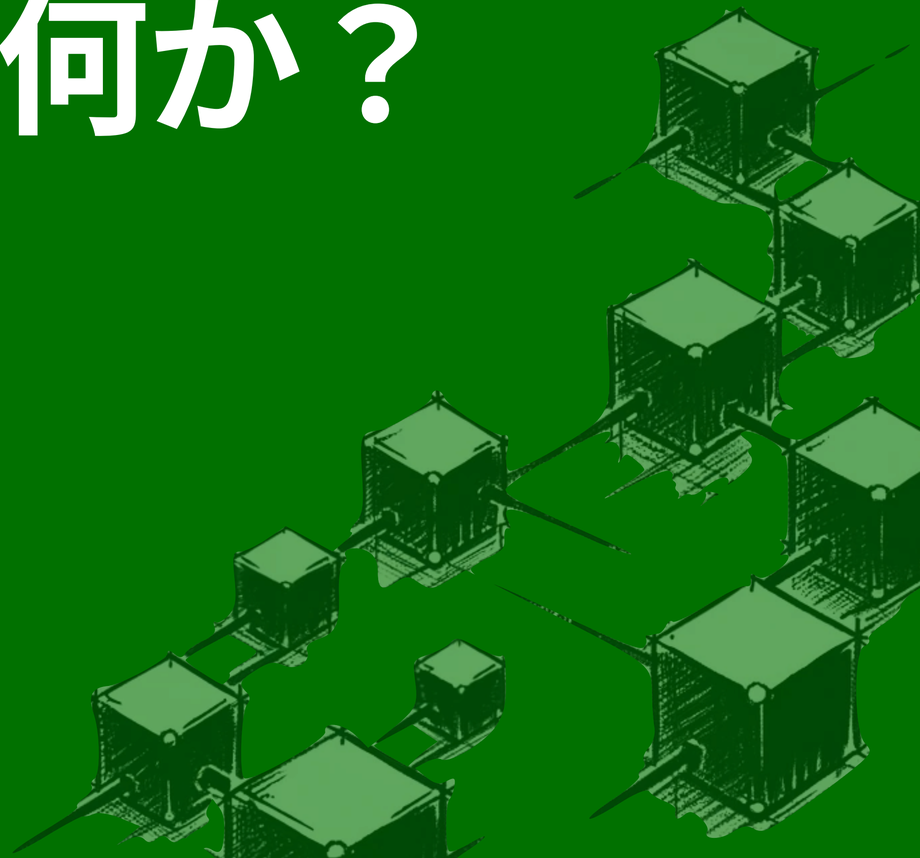
- BSVというチェーン上のNFTを使ったカードゲーム。
- e-sports界隈でけっこうな賑わいを見せている。





ブロックチェーンとは何か？

What's blockchain tech? (about 30 min)



2024.3.19　Shinji Akematsu (PolarTech.inc)