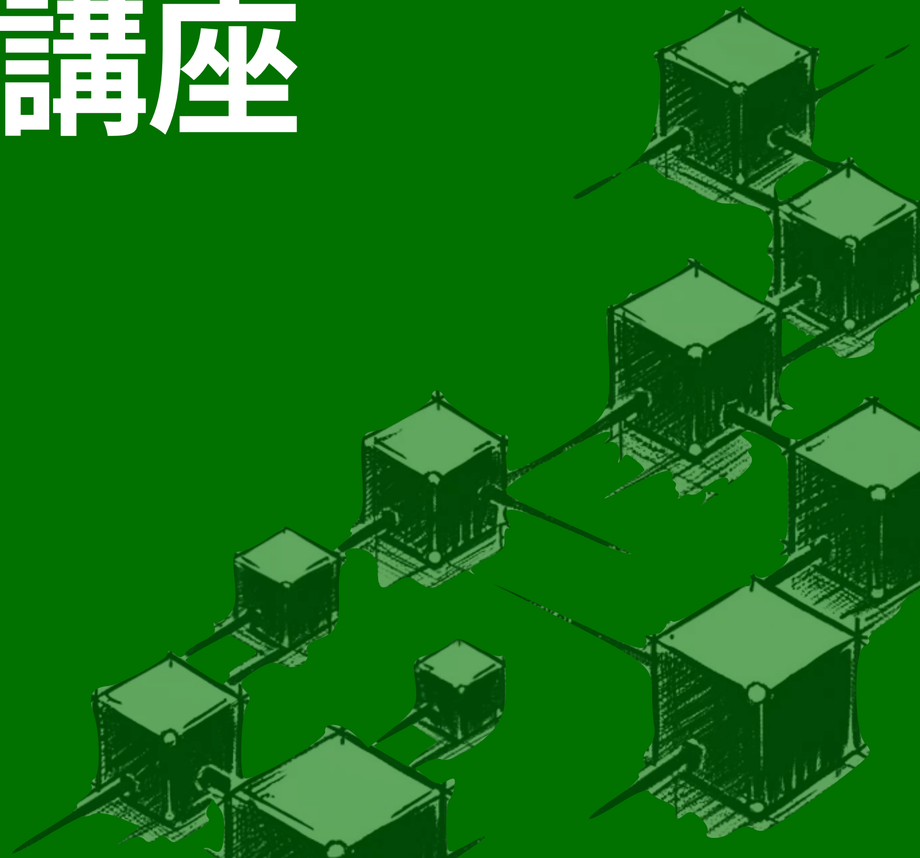
ブロックチェーン基礎講座

The fundamental of blockchain.



2026.03.19 / Shinji Akematsu

改ざん困難な分散型台帳

インターネット以来の大発明

ブロックチェーンのはじまり

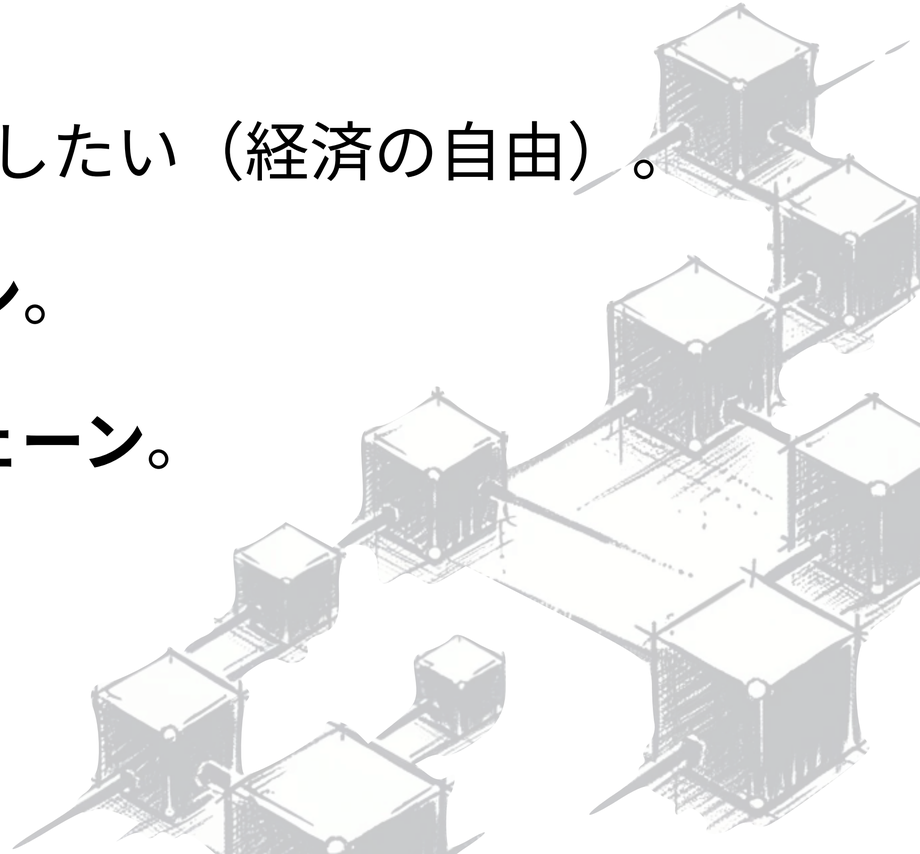
beginning of blockchain.

- 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

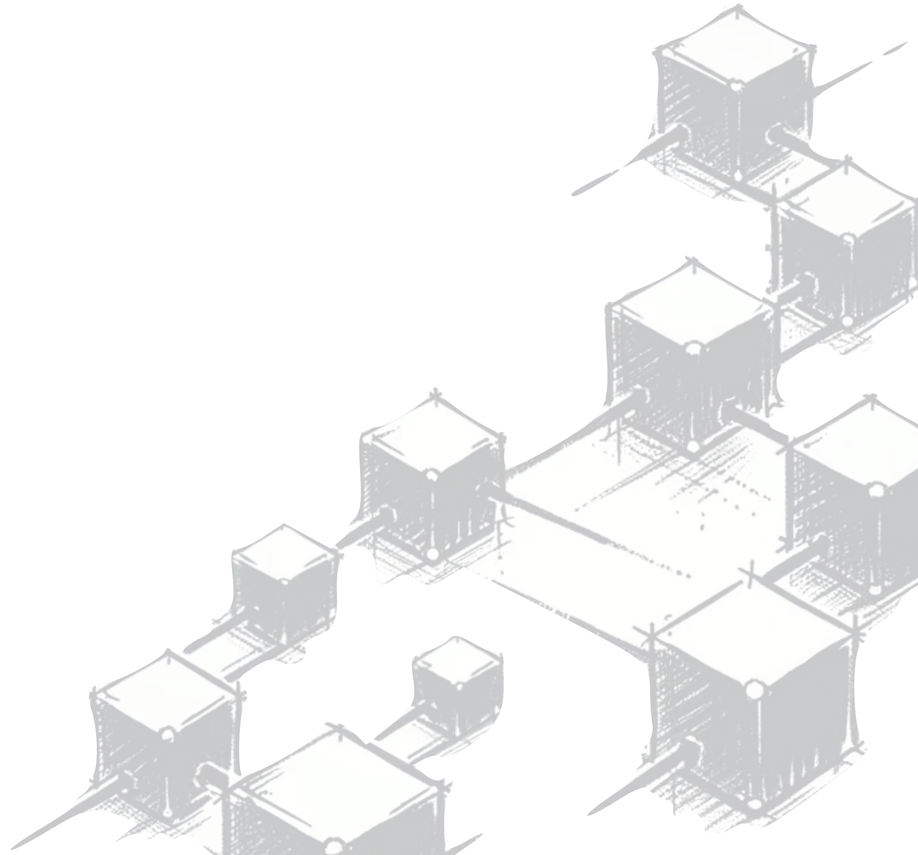
- 根本には **リバタリアニズム**（個人・経済の自由を重視する自由主義のひとつの形）という自由思想。

- **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**。

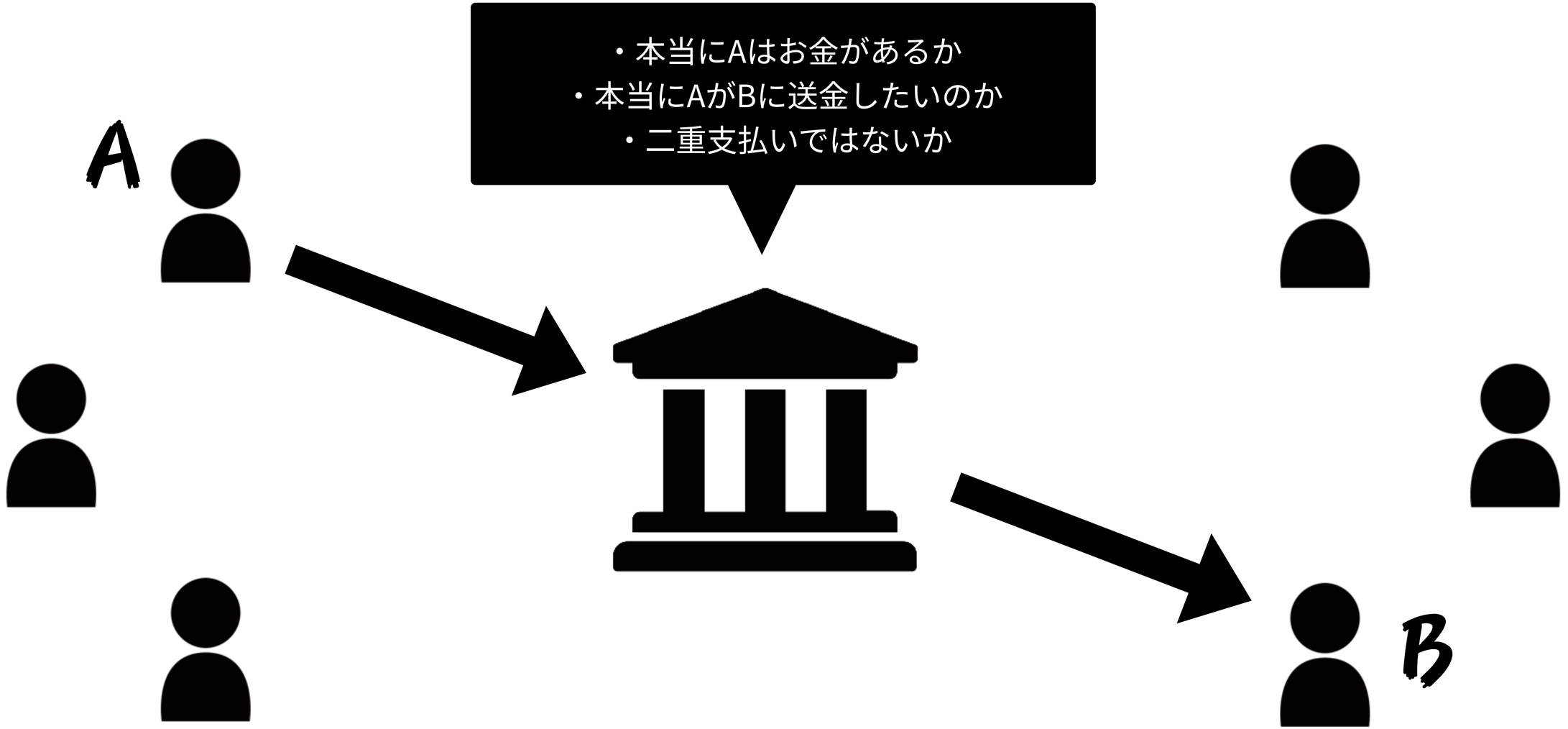


演習
Work

- 現在の1BTCは何JPY？
- ビットコイン運用開始当時の1BTCの価格は？



従来のお金
traditional money system

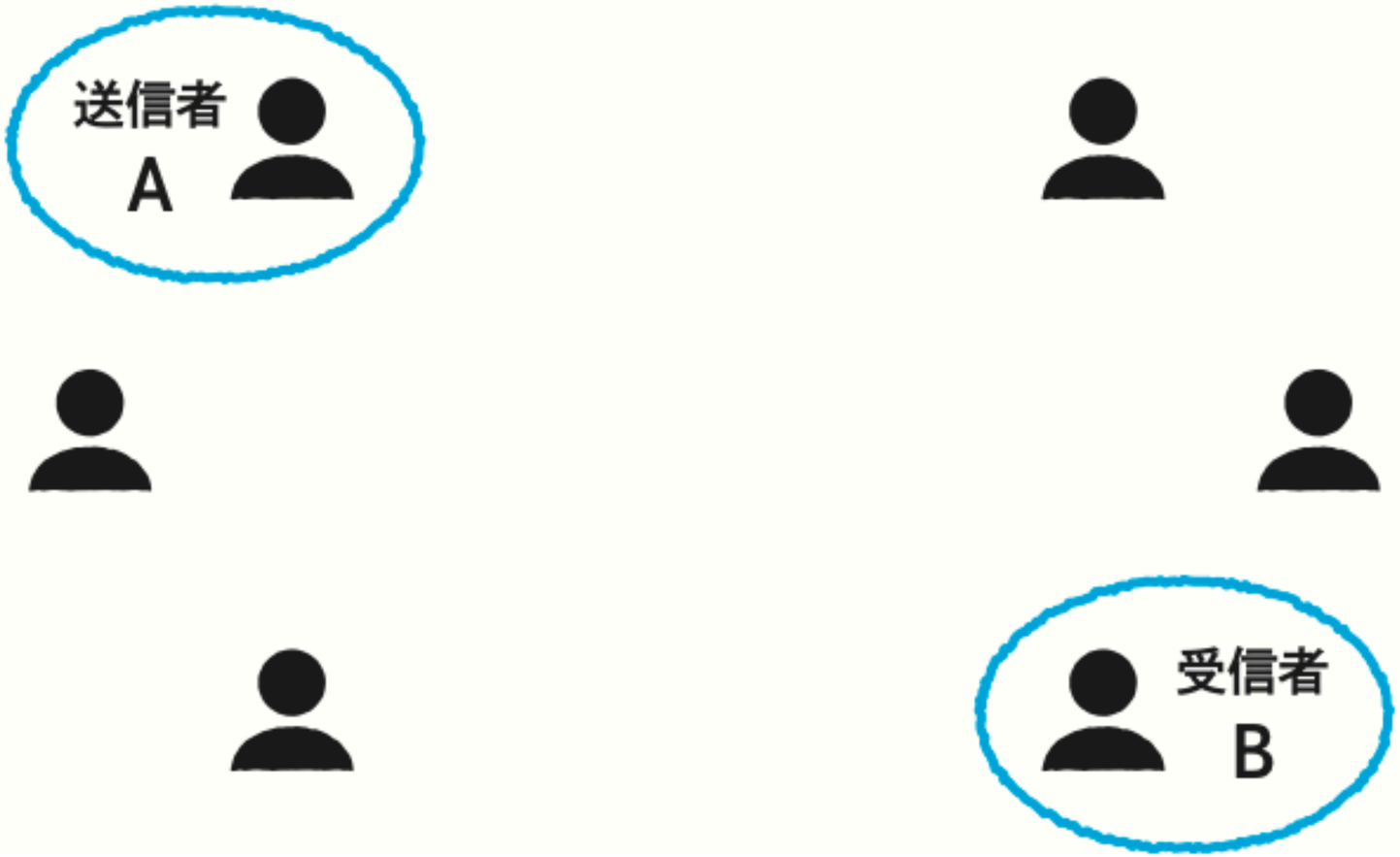


従来のお金
traditional money system

- 従来のお金は**中央集権的**。

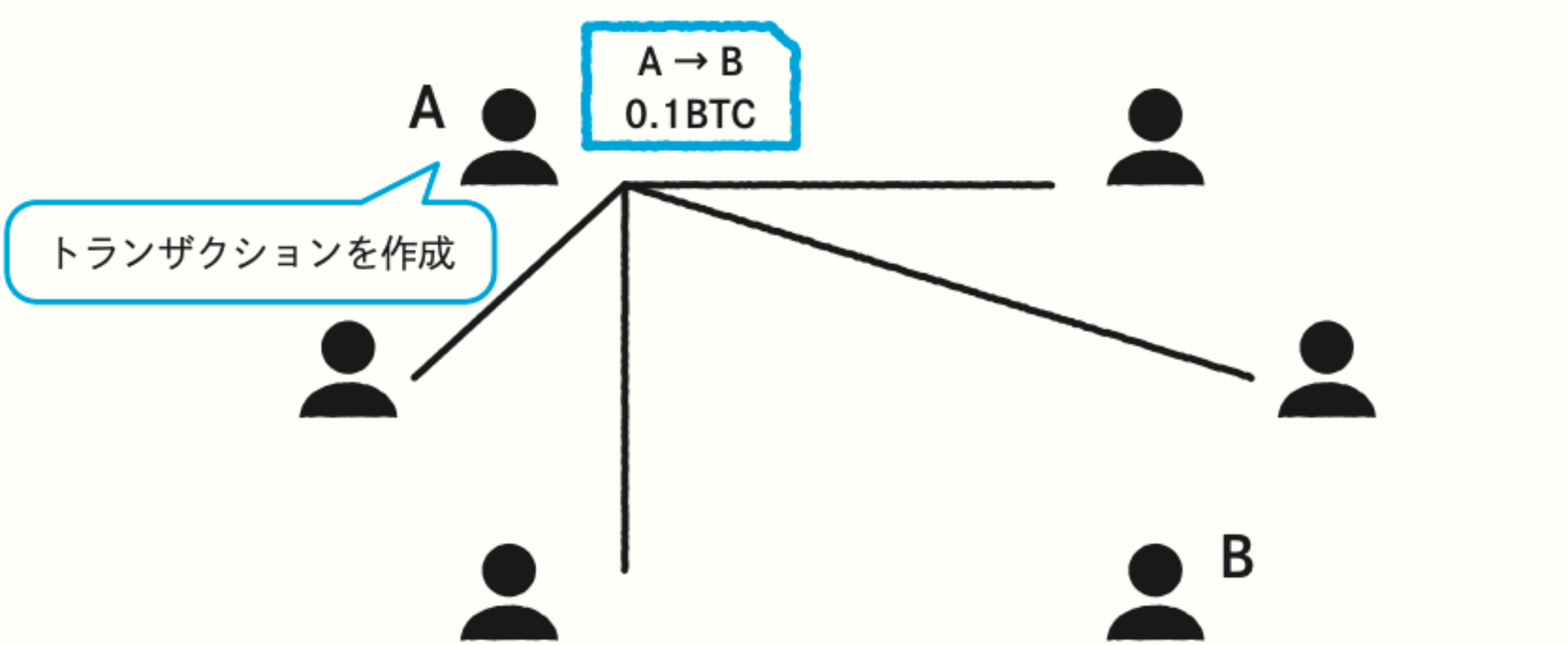
中央集権型システムのメリット・デメリットは？

ビットコイン
Bitcoins system

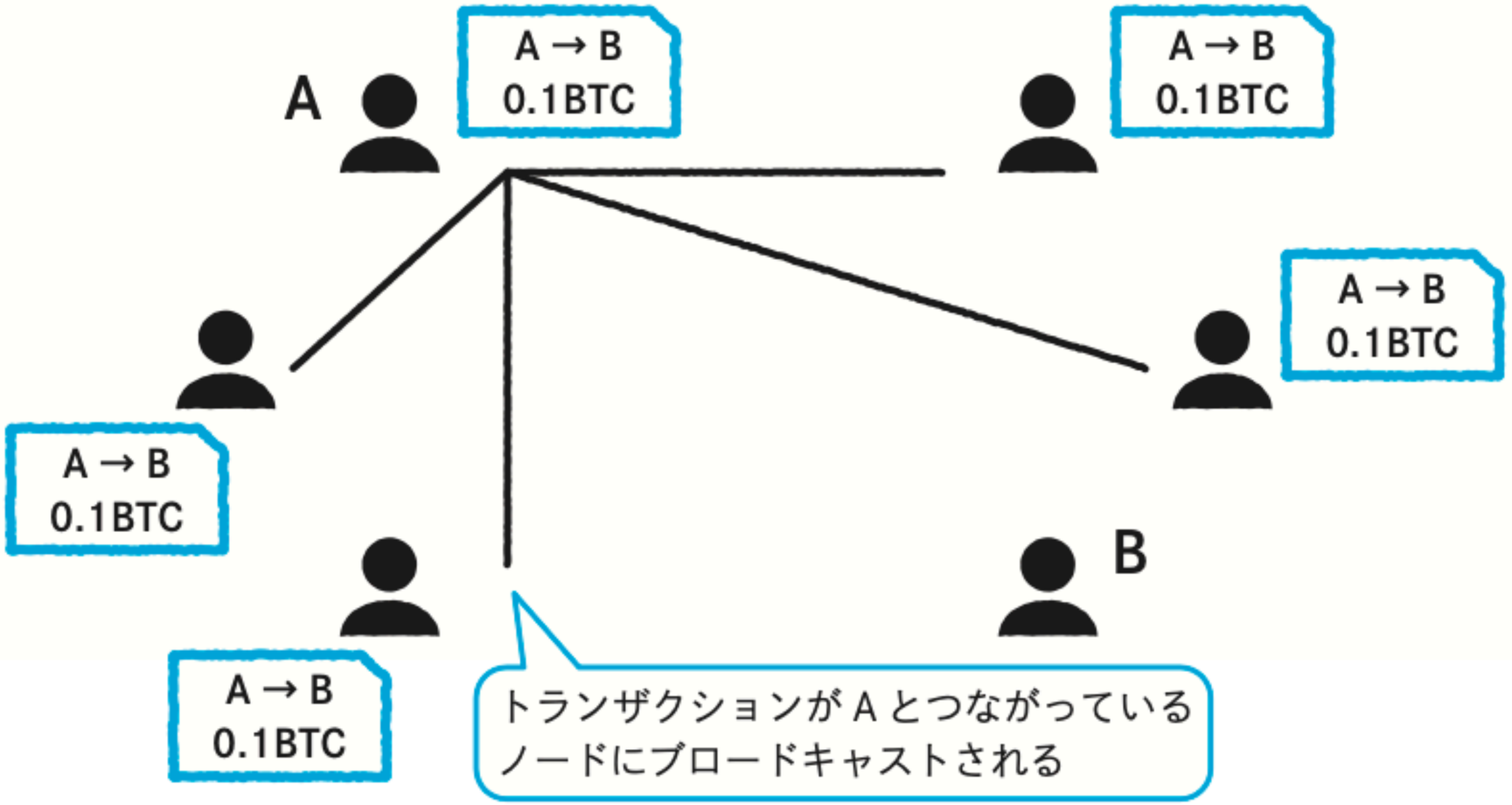


ビットコイン

Bitcoins system

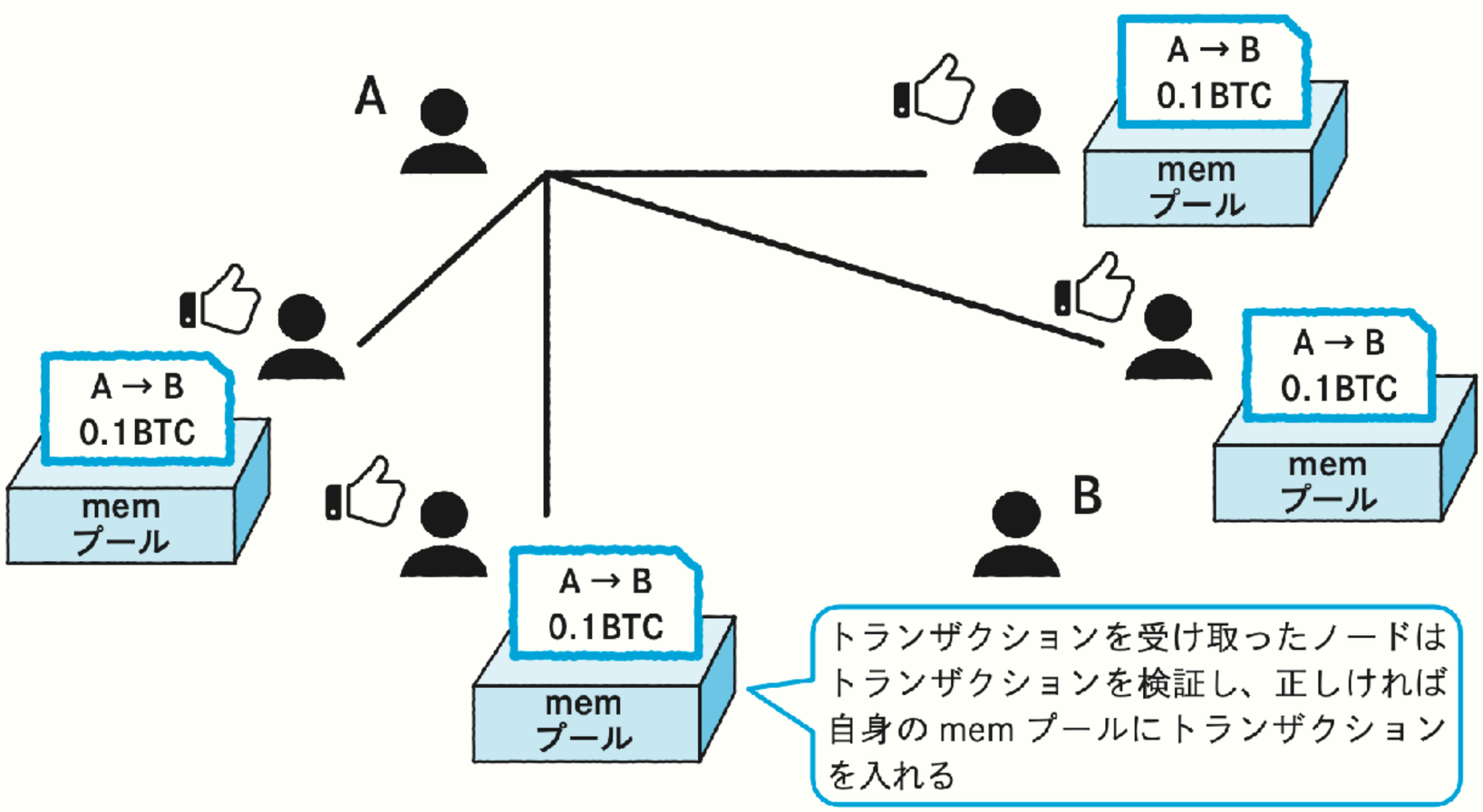


ビットコイン
Bitcoins system

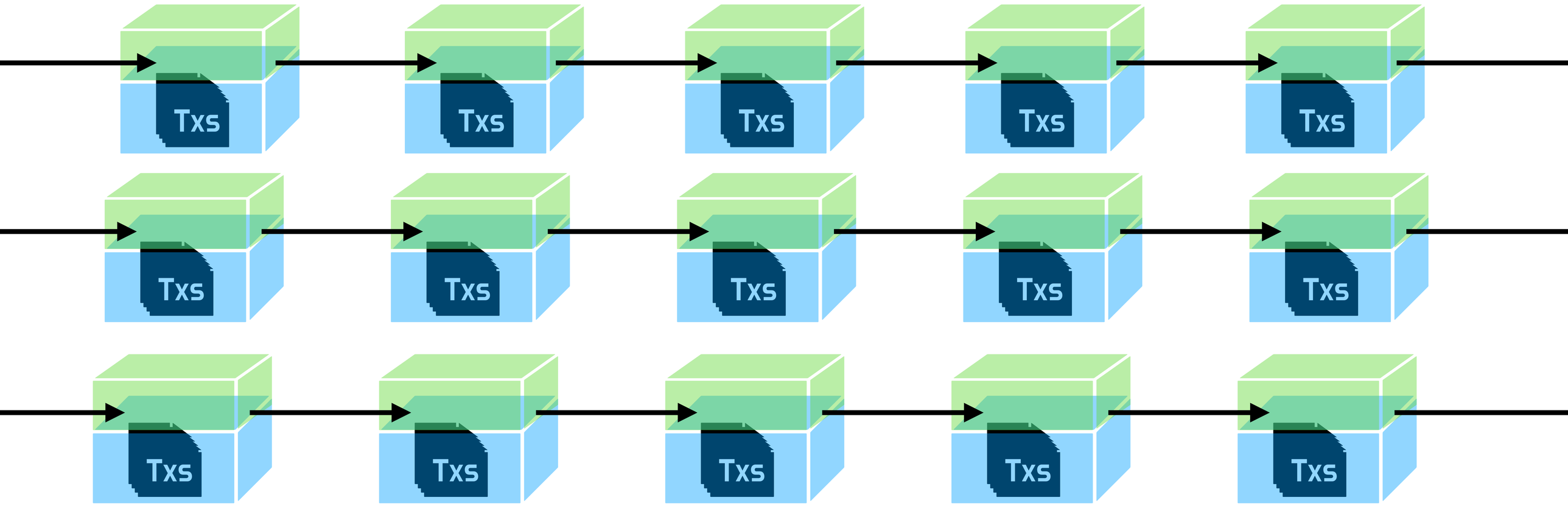


ビットコイン
Bitcoins system

- 参加者全体でチェックが行われる



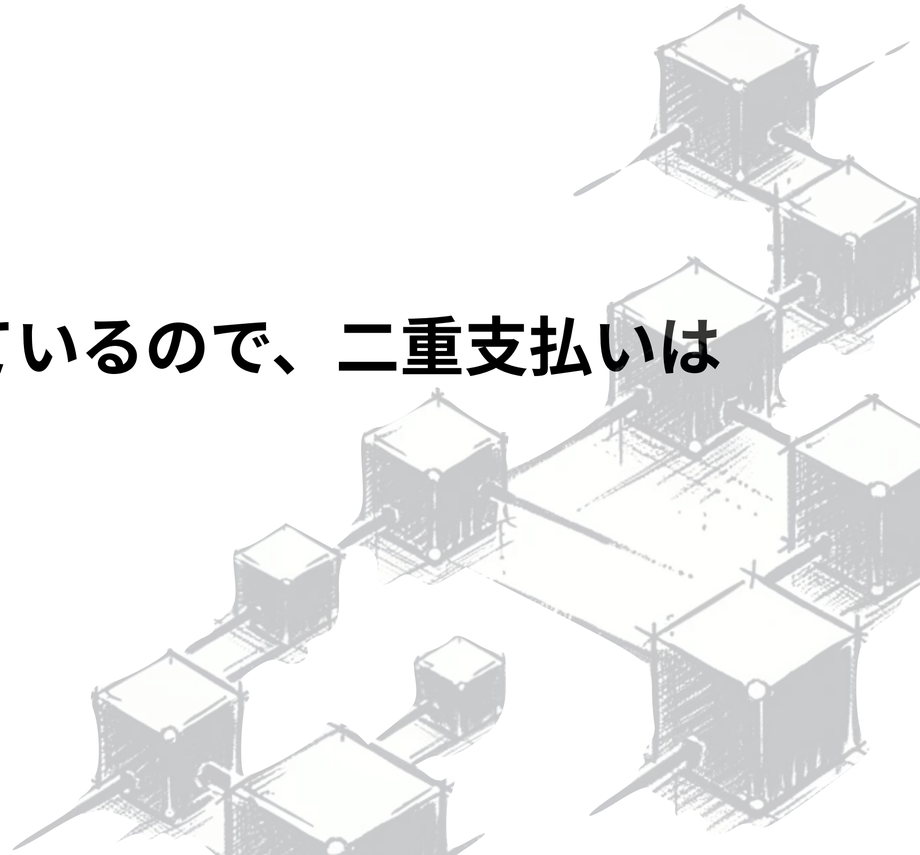
二重支払い問題
double spending problem



ブロックチェーン（事実上改ざんができない）

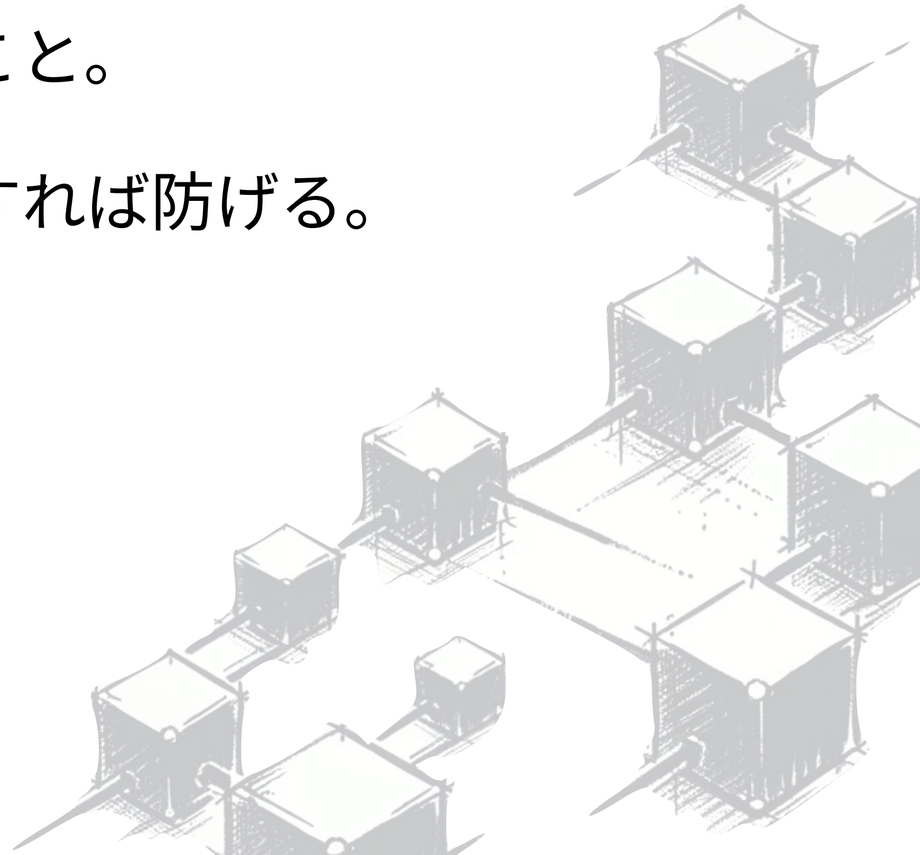
ブロックチェーン
blockchain

- ブロックチェーンは、ビットコインの送金のすべての履歴（台帳）
- 誰でもいつでも見ることができる
- 改ざんが事実上できない（後述）
- **正しい送金の履歴は、ブロックチェーン上に残っているので、二重支払いはすぐにバレる！**

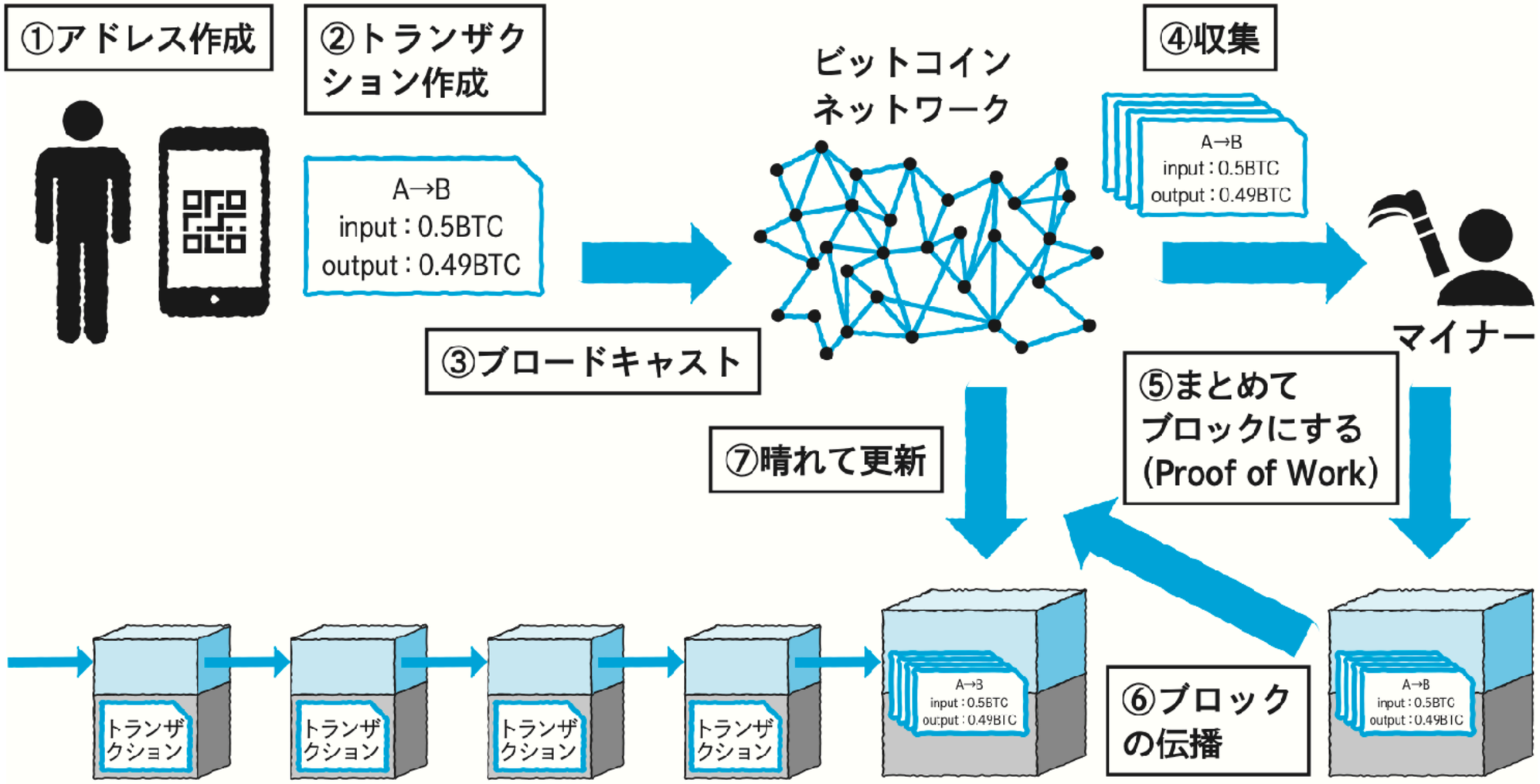


二重支払い問題
double spending problem

- 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！**

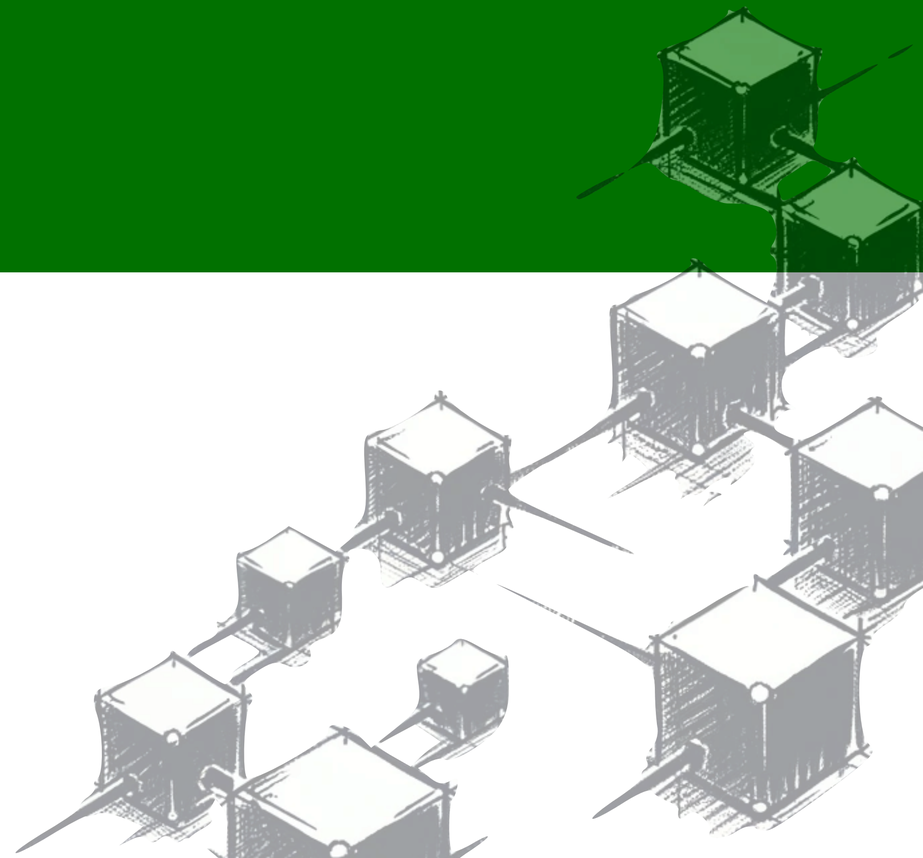


ブロックチェーンの全体像
overview of blockchain



アドレス

Bitcoin address



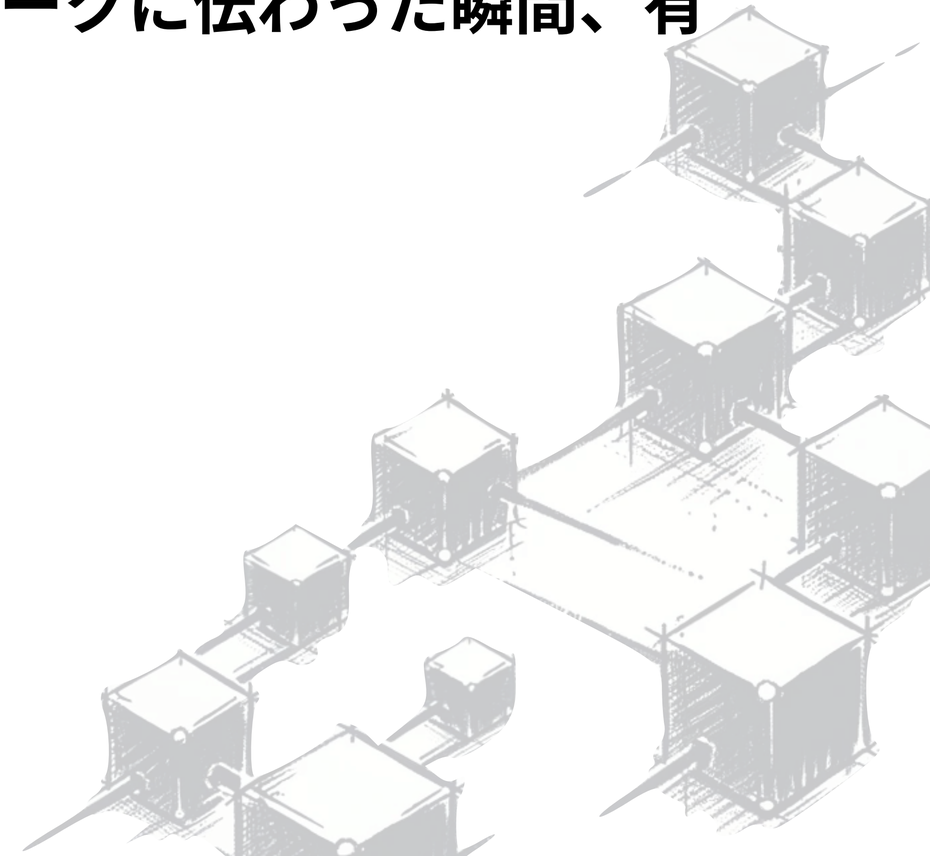
アドレス
address

- **アドレス**とは、ビットコインの送付先のこと。
- 銀行の口座番号のようなものだと思ってOK。

3CDTJnPgmUcekL6hBX
16DH8sfducSNMvzX

アドレス
address

- 銀行口座の番号とは違い、**ルールに従って作ればそれは立派なアドレス。**
- **そのアドレスを含むトランザクションがネットワークに伝わった瞬間、有効なビットコインアドレスとして認知される。**



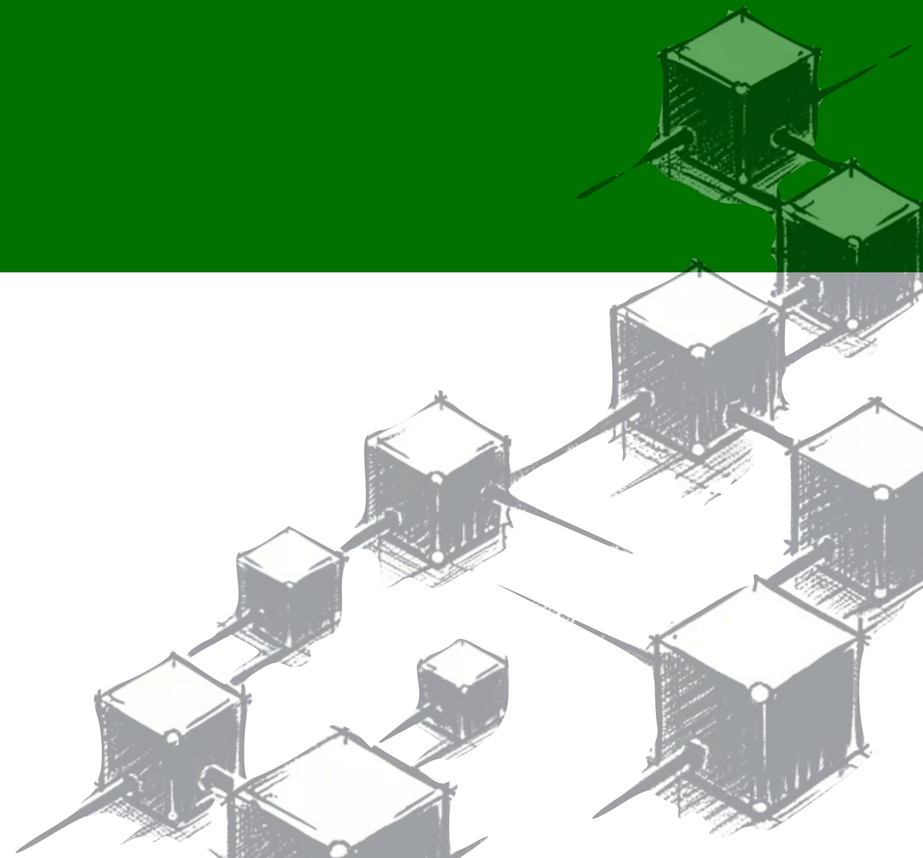
ウォレット
wallet

- **ウォレット（wallet）**とは、スマホアプリやWEBサービスで、送金、残高確認などを簡単に行えるソフトウェアのこと。

- 内部ではアドレスを持ち、そこに紐づく残高を合計したり、トランザクションをビットコインネットワークに送ったりなどなどしている。

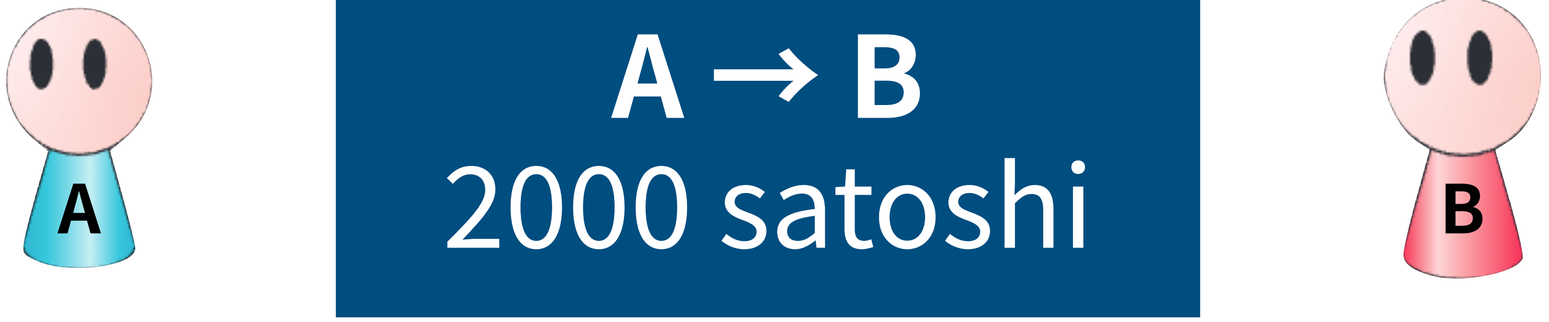
トランザクション

Transactions



トランザクション
Transactions（Tx）

- **トランザクション（transaction）**とは、取引をあらわすもの。
- 資金の移転をあらわすデータで、小切手のようなものだと思えばよい。



※ 1satoshi = 0.00000001 BTC

例を通じて納得しよう

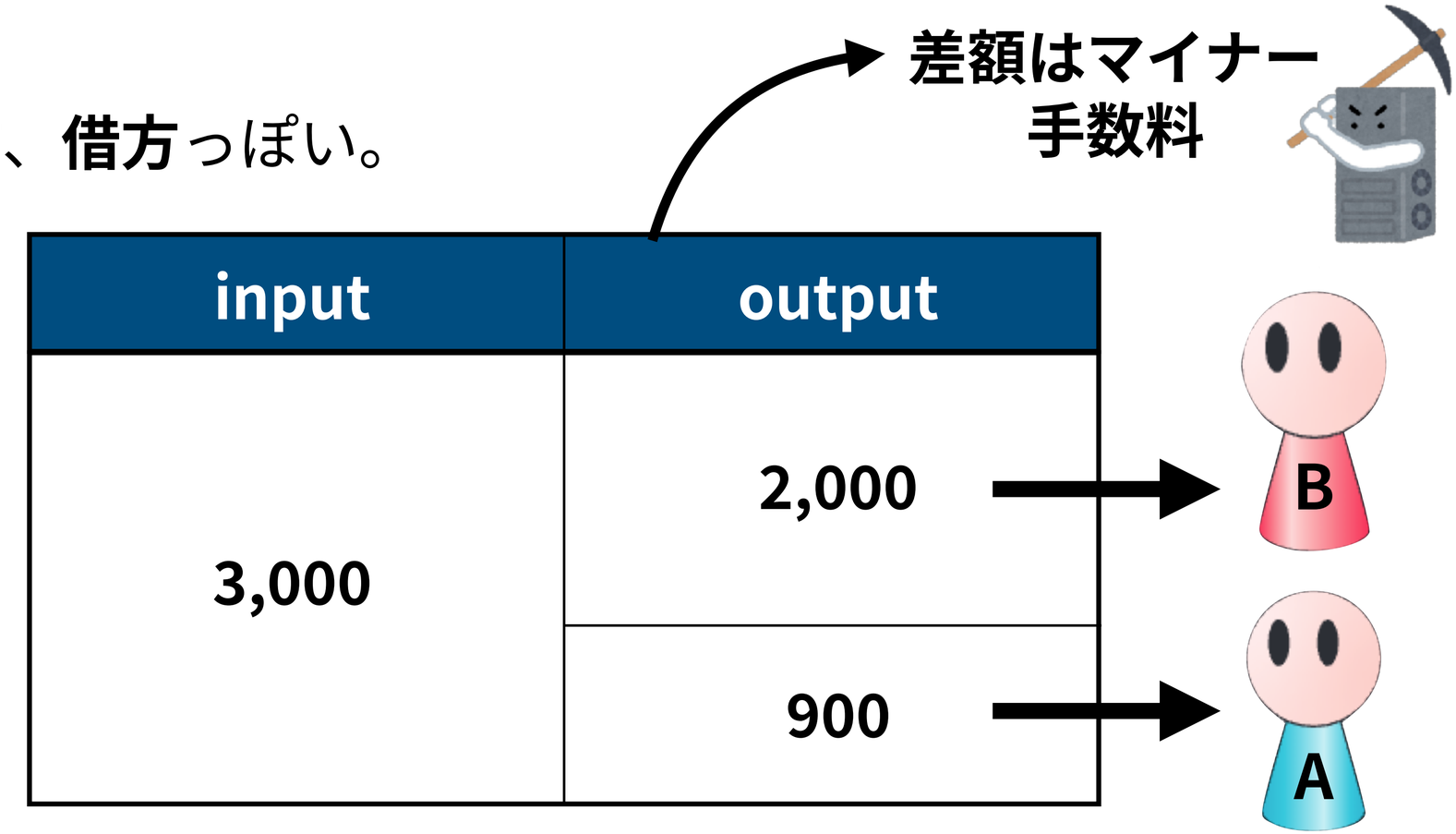
Let's think on example.

シチュエーション

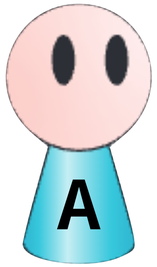
- Aは初めてウォレットアプリをインストールし、3000satoshi を友人から受け取った。
- AはBに、それをもとにして 2000satoshi を送りたい。

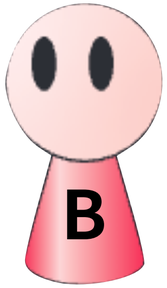
トランザクション
Transactions（Tx）

- トランザクションは、**インプット（input）**と**アウトプット（output）**からできている。
- 複式簿記の**貸方**、**借方**っぽい。

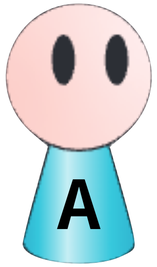


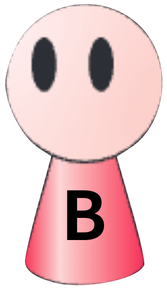
- ① AはBに2000satを送る。





- ② Aは手数料を差し引いた残額900satを自分に送る。

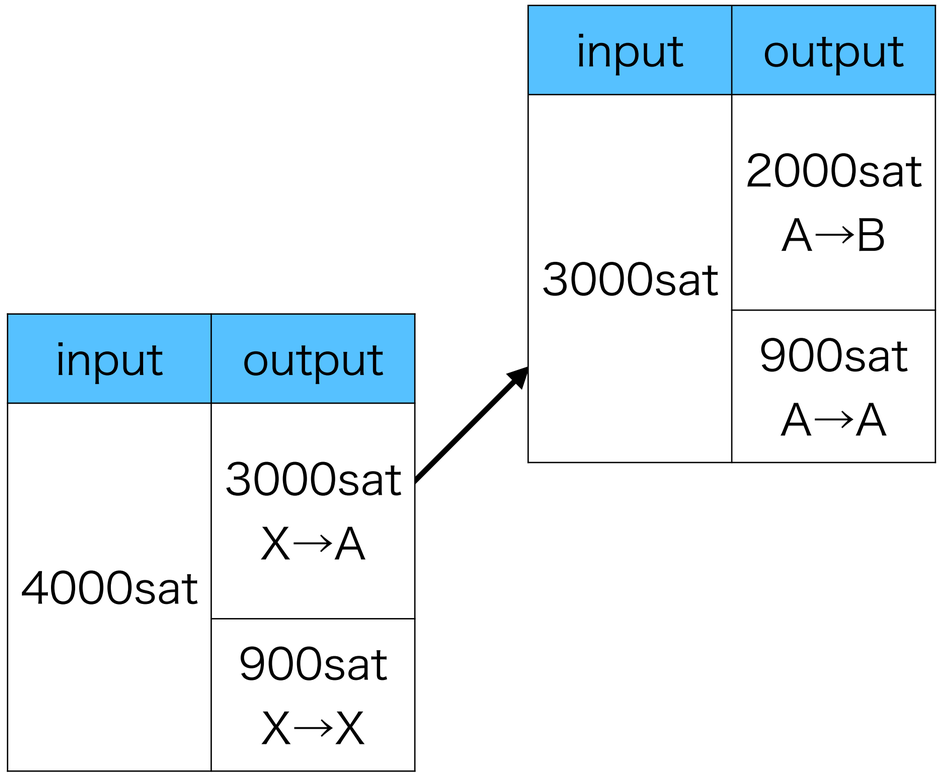




- ③ 差額は100satマイナーへ。

トランザクションのつながり

chain of transactions

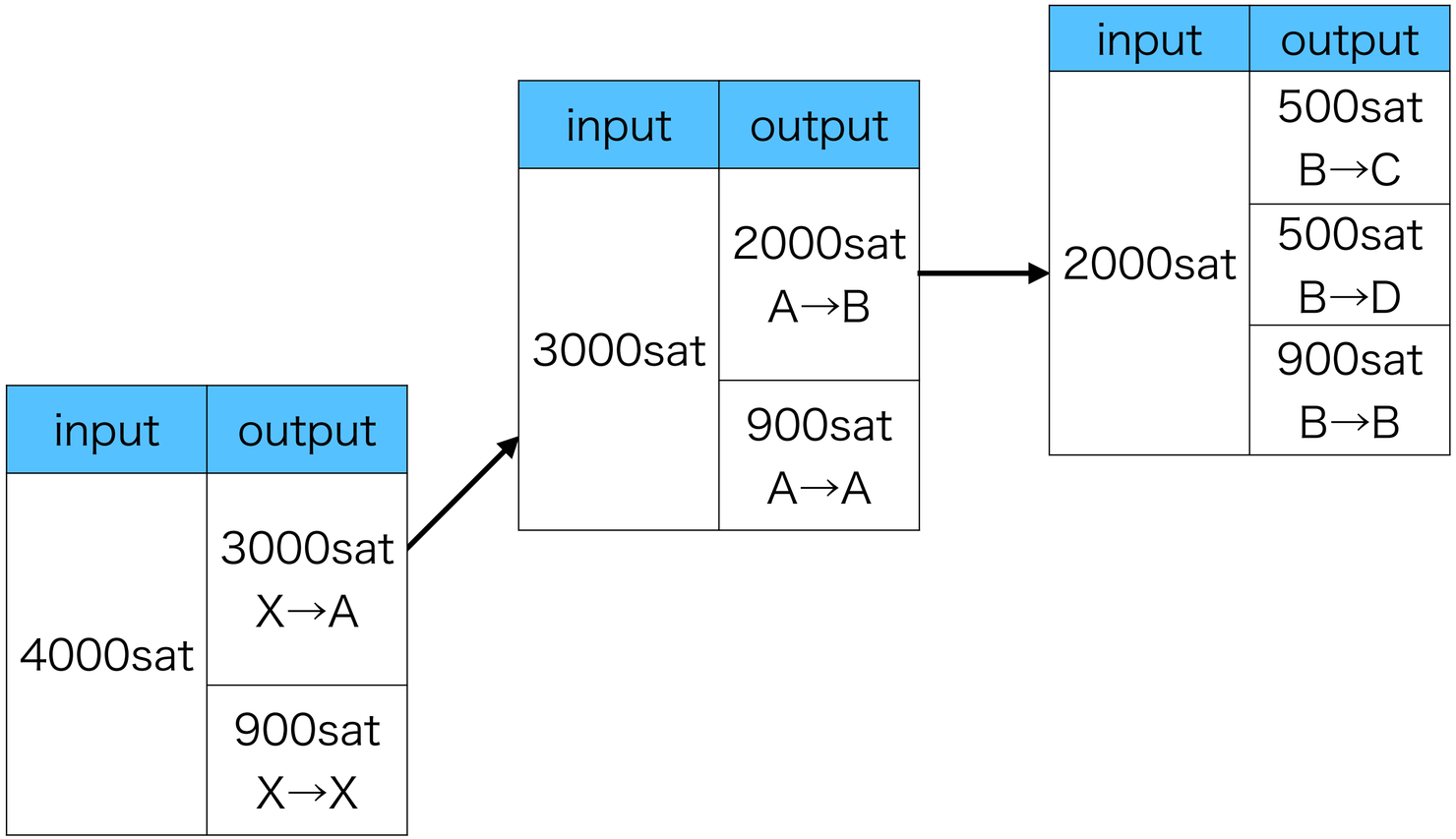


- ④ Bは手元の2000satをもとに、500satをCに、500satをDに送る。
  Aは900satのおつりを受け取る。

- ⑤ 差額の100satはマイナーに。

トランザクションのつながり

chain of transactions

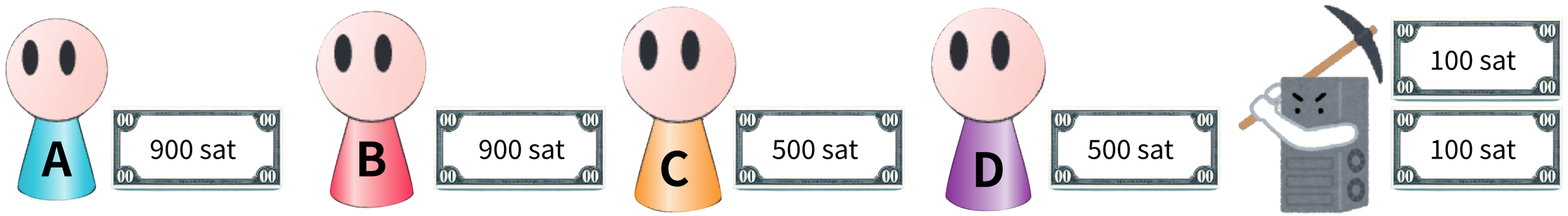


トランザクションのつながり
chain of transactions

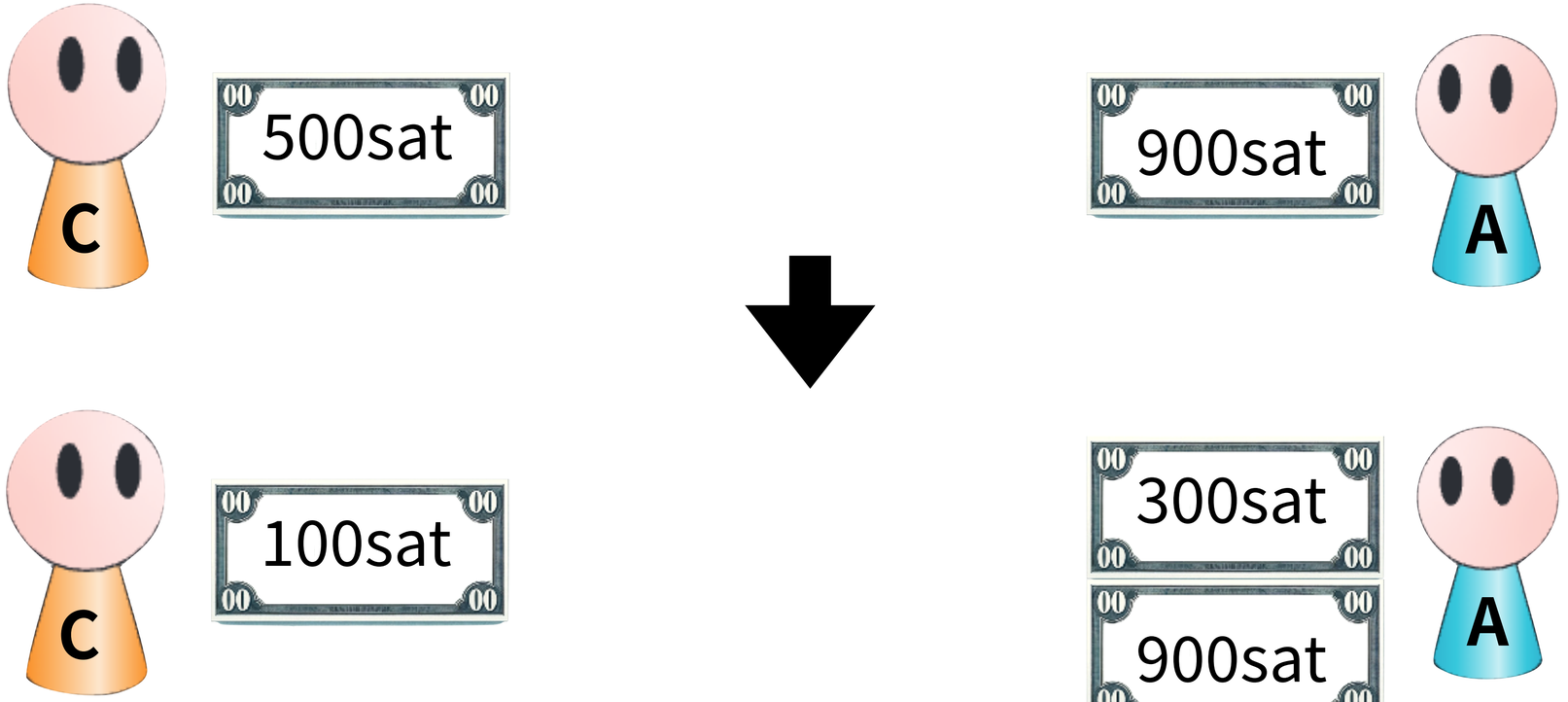
input	output
4000sat	3000sat X→A
	900sat X→X

input	output
3000sat	2000sat A→B
	900sat A→A

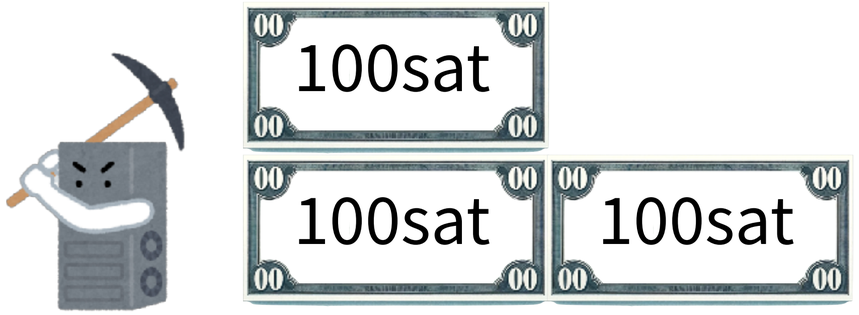
input	output
2000sat	500sat B→C
	500sat B→D
	900sat B→B



- ⑤ Cは手元の500satをもとに、300satをAに送る。おつりは受け取る。

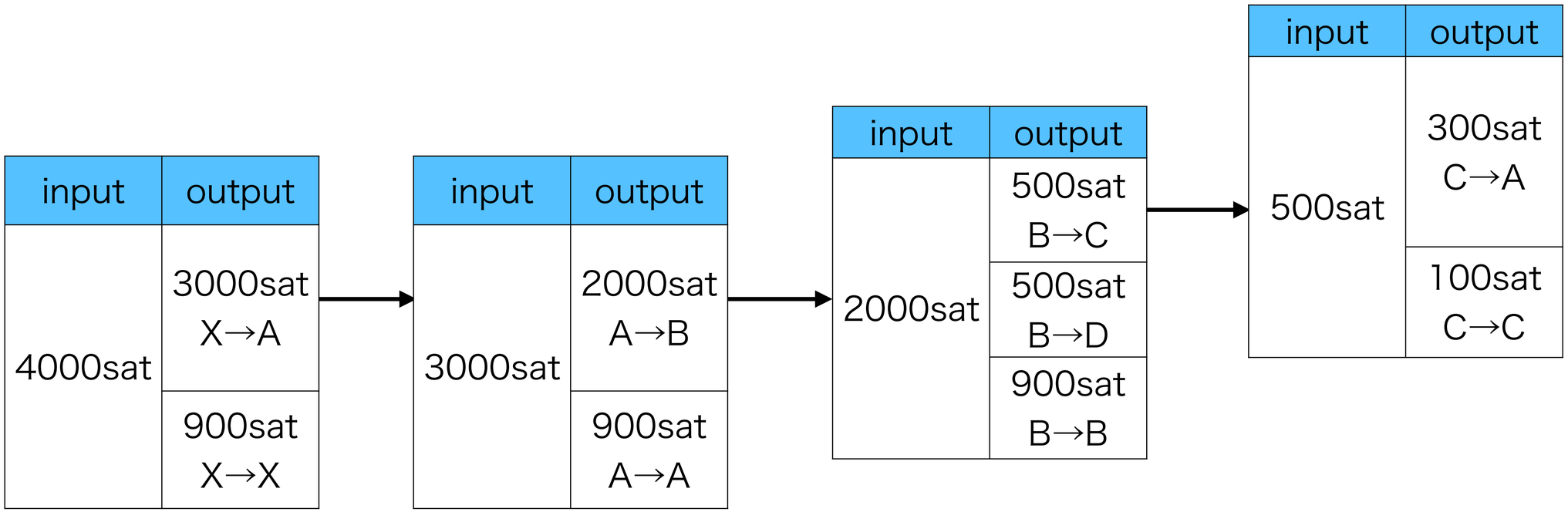


- ⑥ 手数料はマイナーに。

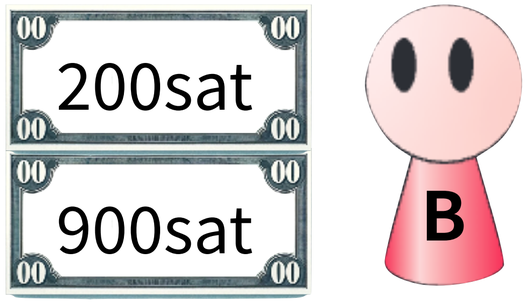


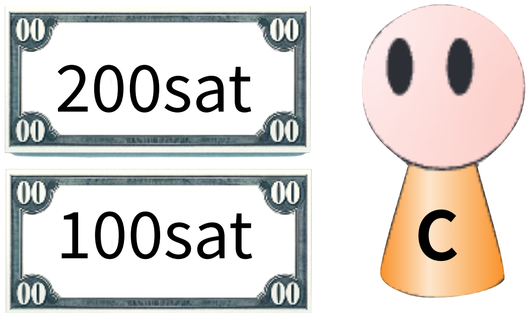
トランザクションのつながり

chain of transactions

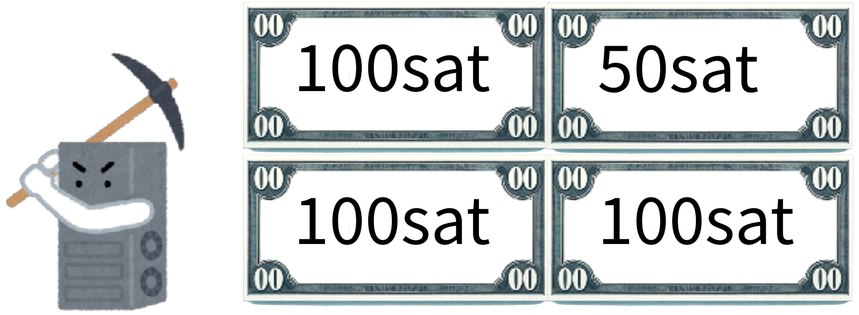


- ⑥ Dは手元の500satをもとに、200satをB, Cに送る。おつりは受け取る。



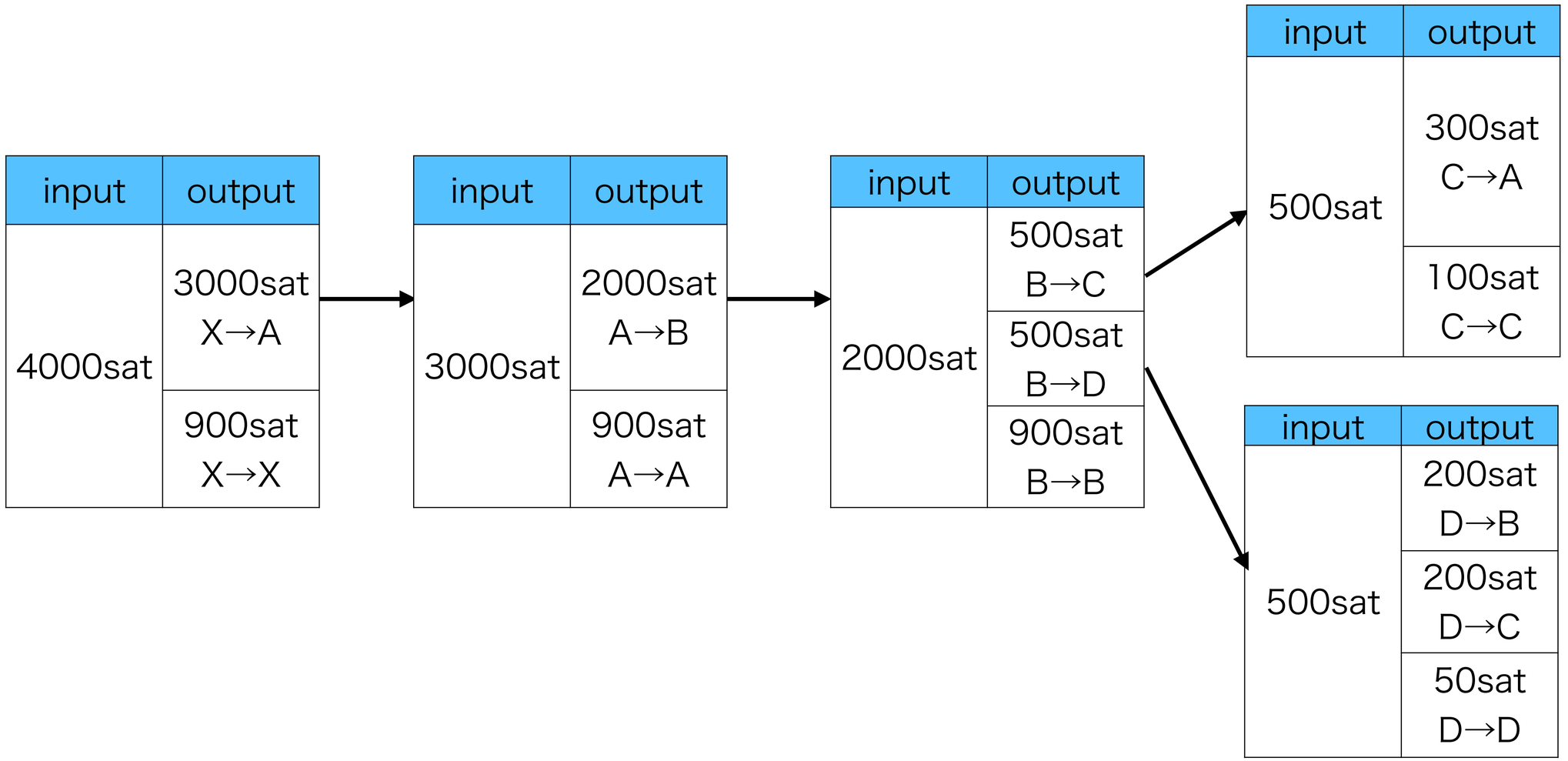


- ⑥ 手数料はマイナーに。



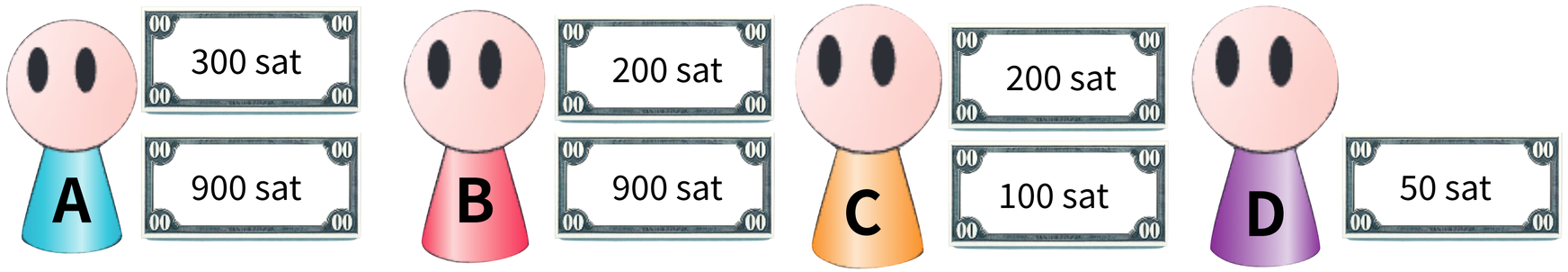
トランザクションのつながり

chain of transactions

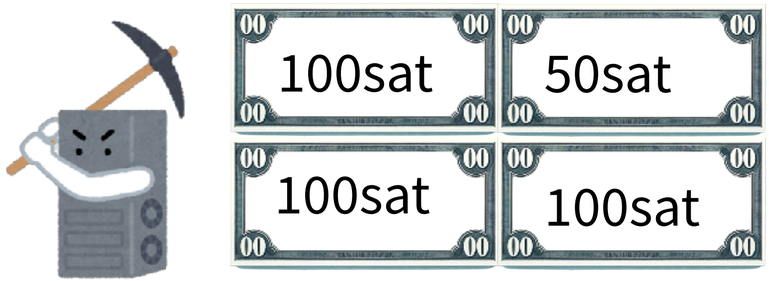


最終的な残高
balance

- 残高は以下の通り。



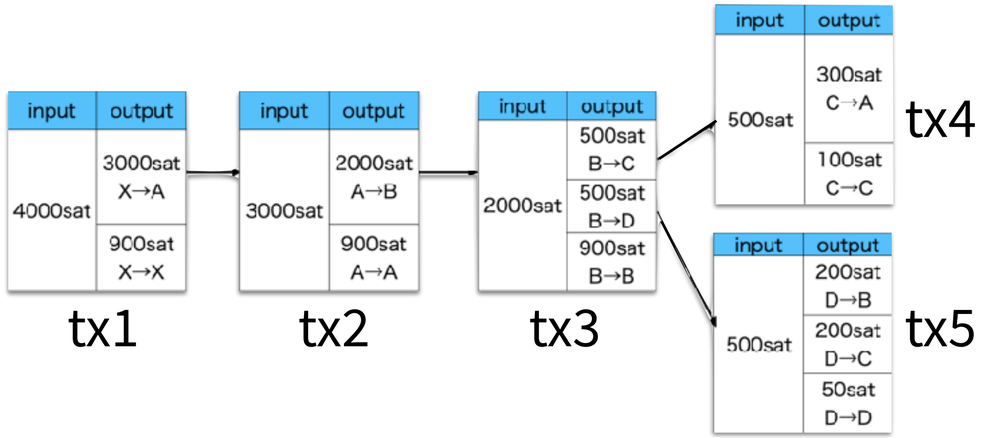
- マイナーの手数料合計は以下の通り。



UTXO

Unspent Transaction(TX) Output

- トランザクションを追跡すれば、ユーザの残高は全て計算できる。
- まだ何のinputにもなっていないアウトプットを、**UTXO（Unspent TX Output）**と呼ぶ。
- ビットコインでは、残高をUTXOの合計として管理する。



UTXOを「誰でも使える」？

UTXO can used by everyone?

- UTXOをinputにする → outputをトランザクションに書き、それが誰かのUTXOになる。
- この**「トランザクションの集まり」（そして、これが正しいという確証）**こそがビットコインの全て。
- ところで、**UTXOは「誰でも使える」**のか？ → それは当然駄目。
- よって、「受け取り手じゃないと使えなくする」仕組みがある。

トランザクションスクリプト
Transaction script

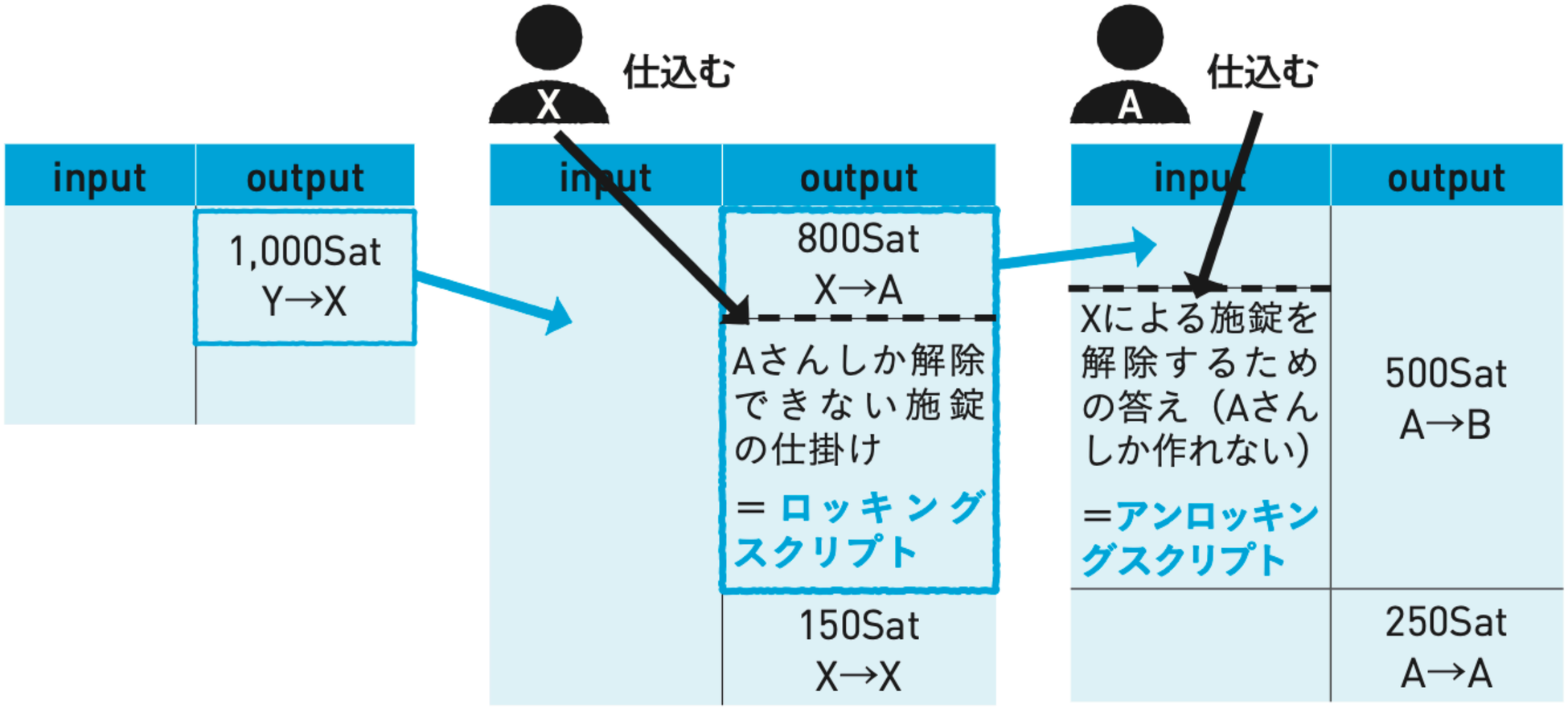
- ① UTXOの元が意図した送り手である。
  → **Locking script**

- ② それがちゃんと（なりすましでない）本人である。
  → **Unlocking script**

- あわせて**トランザクションスクリプト（Transaction script）**という。

トランザクションスクリプト
Transaction script

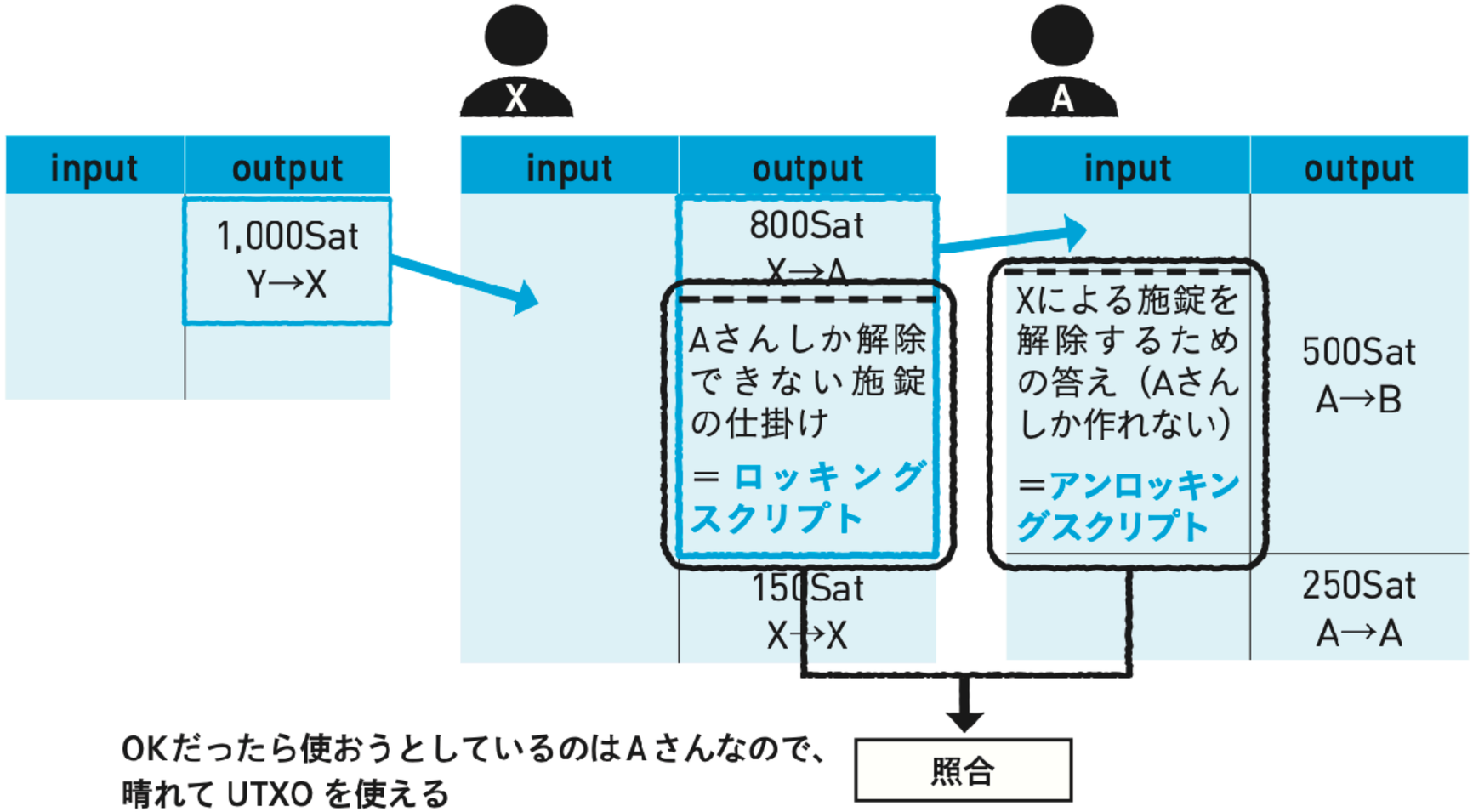
- X さんがアウトプットに仕掛けを施す



トランザクションスクリプト

Transaction script

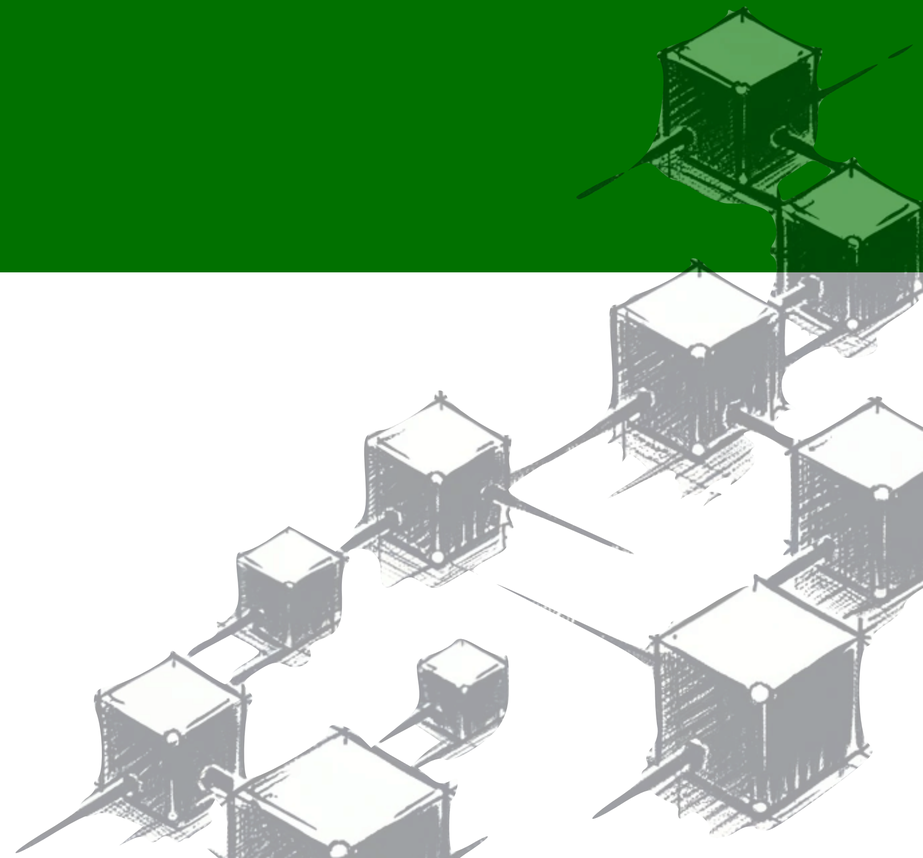
- 照合により解除を行う



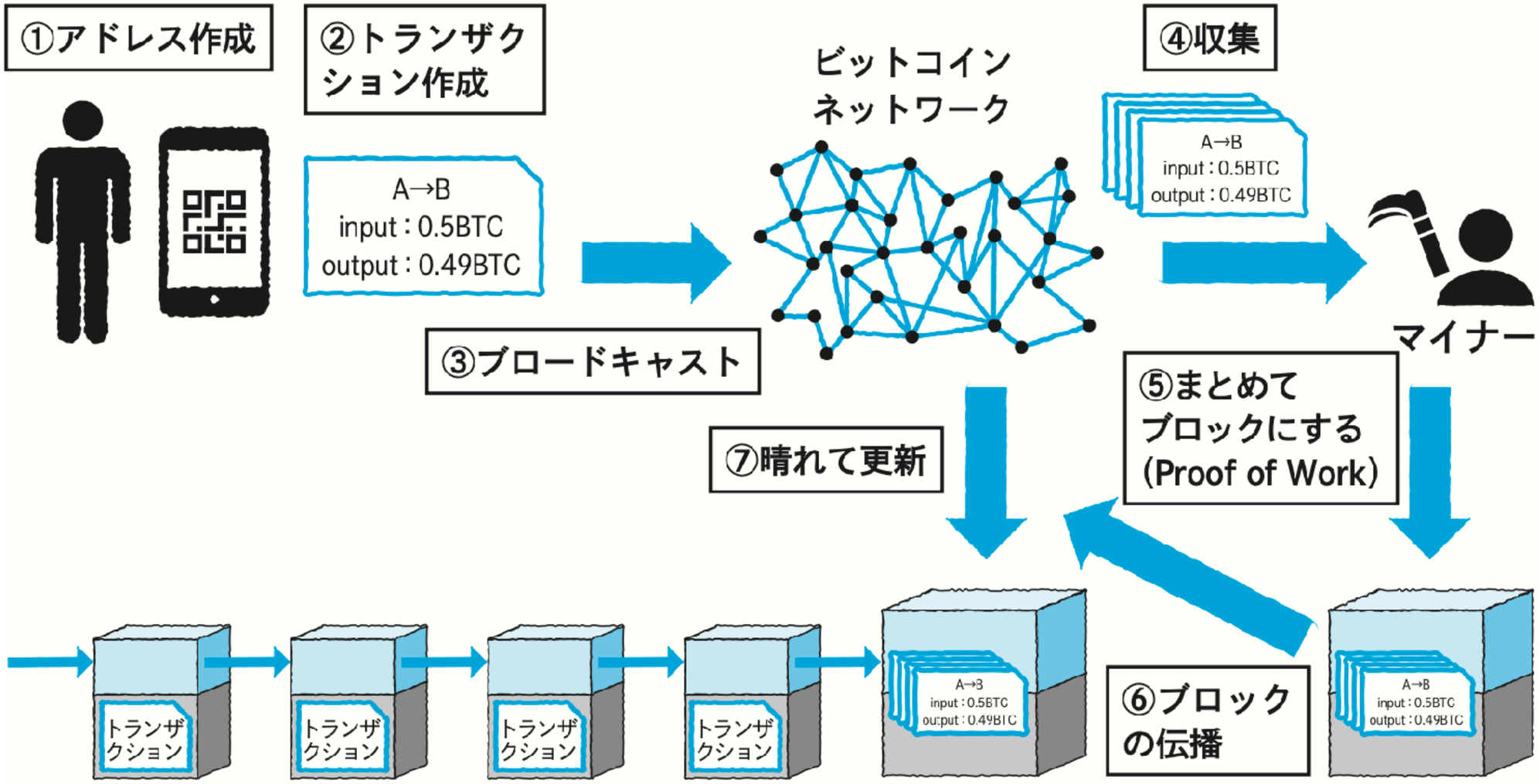
OKだったら使おうとしているのはAさんなので、
晴れて UTXO を使える

マイニング

Mining



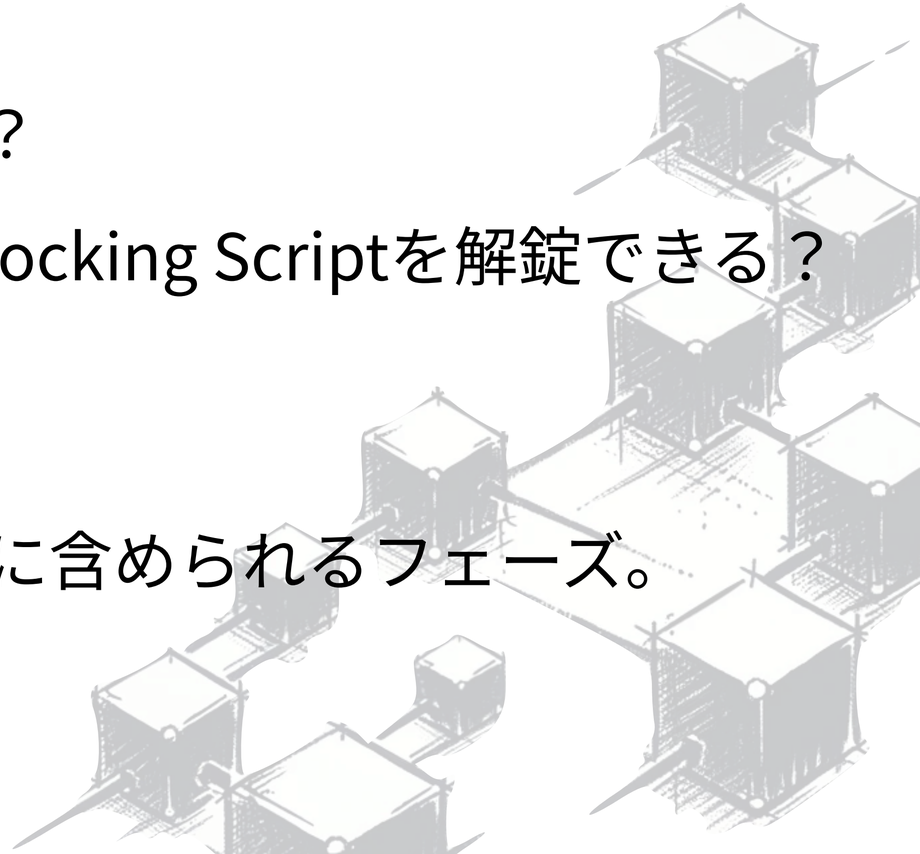
ブロックチェーンの全体像
overview of blockchain



トランザクションの検証
verification of transactions

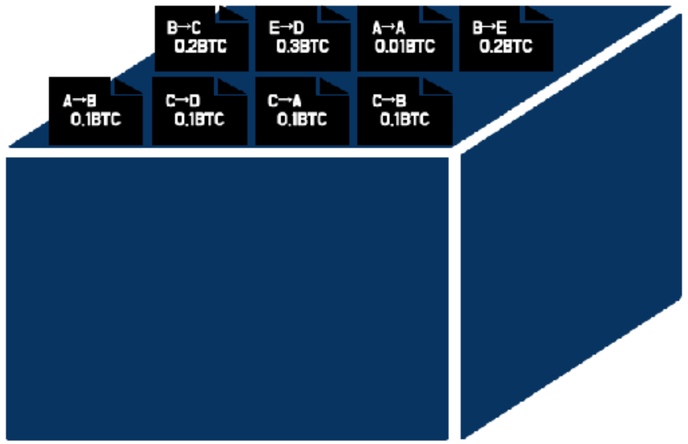
- トランザクションはネットワークにブロードキャストされ、各ノードで検証される。
  - トランザクションのデータ構造は正しい？
  - 各inputに対して、参照しているUTXOが見つかる？
  - inputにあるUnlocking Scriptは、参照元UTXOのLocking Scriptを解錠できる？
  - inputの値の総和はoutputの総和よりも大きい？

- 検証が終わったら、次はいよいよブロックチェーンに含められるフェーズ。



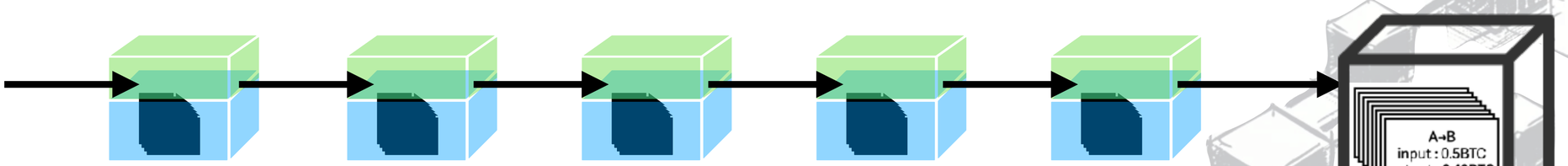
ブロック
block

- **ブロック（block）**とは、トランザクションがたくさん集まったもの。
- **ブロックチェーン（block chain）**とは、ブロックが**ハッシュチェーン（hash chain）**という形で繋がったもの（詳しくは後述）



マイニング
Mining

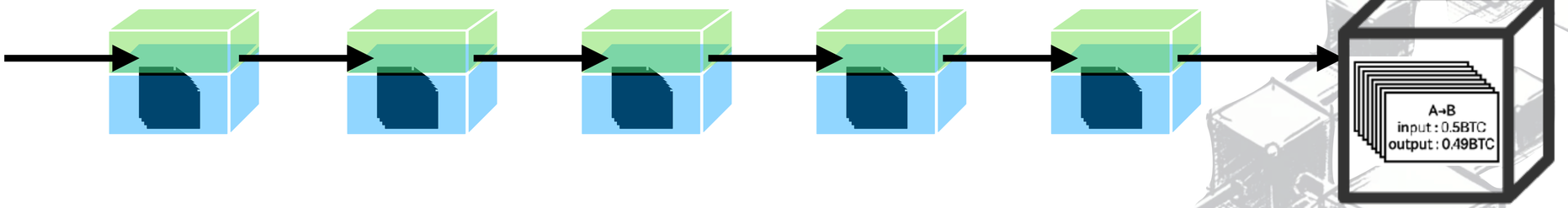
- **マイニング（Mining）**とは、トランザクションをたくさん集めて、新しいブロックを作ること。
- マイニングに成功するとお金（mining reward）がもらえる。
- その報酬を目的にマイニングを行なうノードを**マイナー（minor）**と呼ぶ。



PoW

Proof of Work

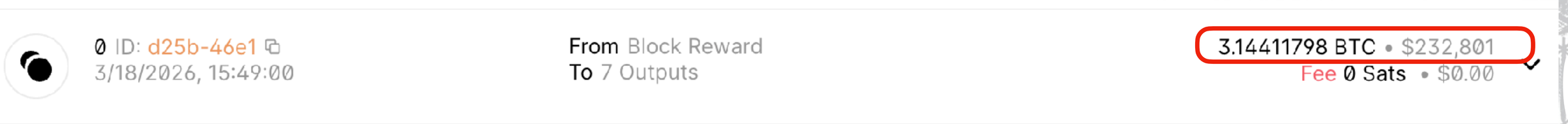
- マイニングの際にマイナーは、**Proof of Work（PoW）**という非常に大変な計算競争を行わなければならない。
- この計算競争に勝ったマイナーが、新しいブロックをブロックチェーンにつなぐことができる。



マイニングは「採掘」

What's mining

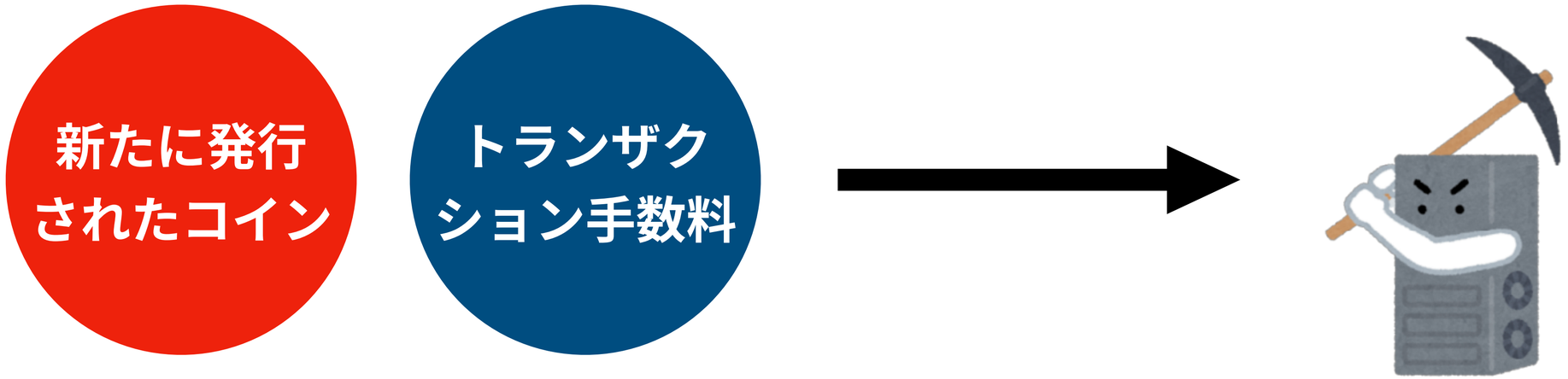
- マイニングは日本語で「採掘」という意味。
- モデルは金の採掘。ビットコインでは、マイニングに成功すると**なにもないところからビットコインが発行**され、報酬としてマイナーに渡される。



Proof of Work

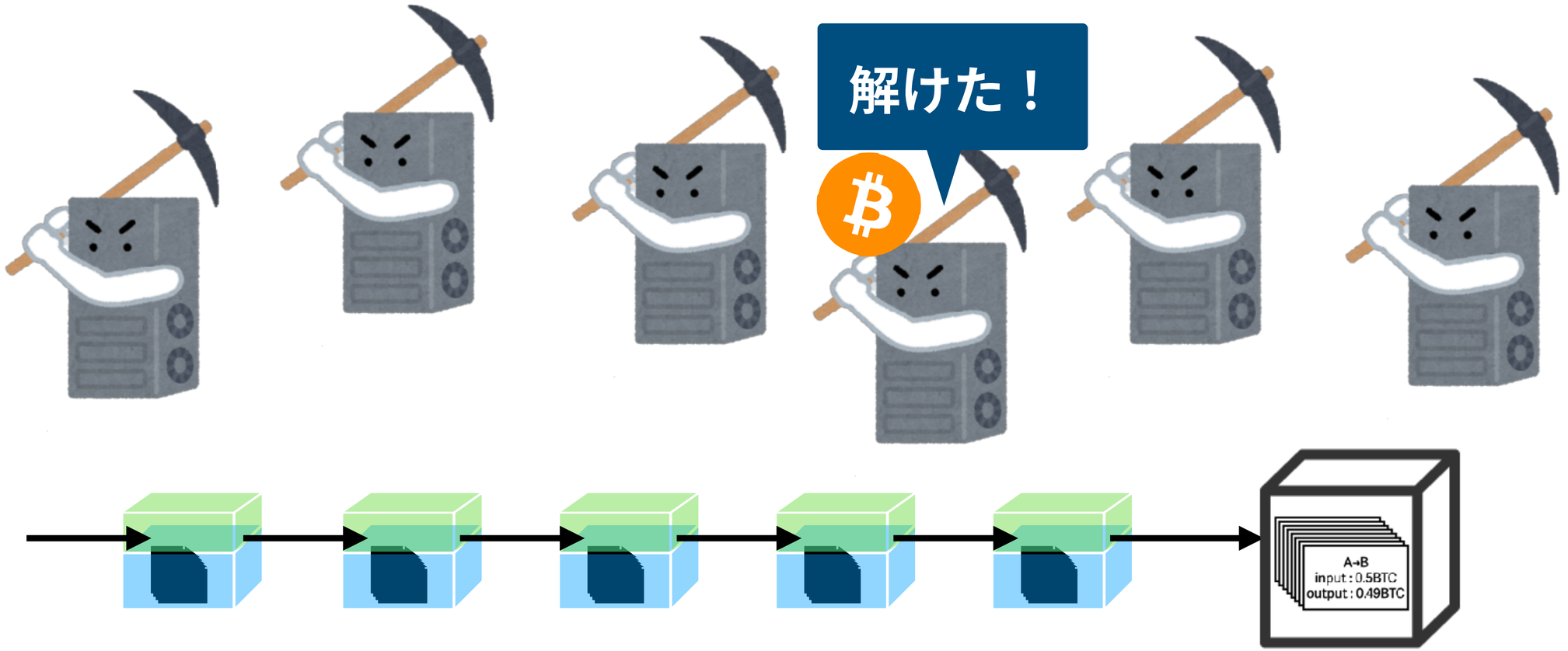
Proof of Work

- マイニングの際にマイナーは、**Proof of Work（PoW）**という非常に大変な計算競争を行わなければならない。
- この計算競争に勝ったマイナーが、新しいブロックをブロックチェーンにつなぎ、報酬を得ることができる。
- マイナーは報酬のためにマイニングを頑張る。



Proof of Work

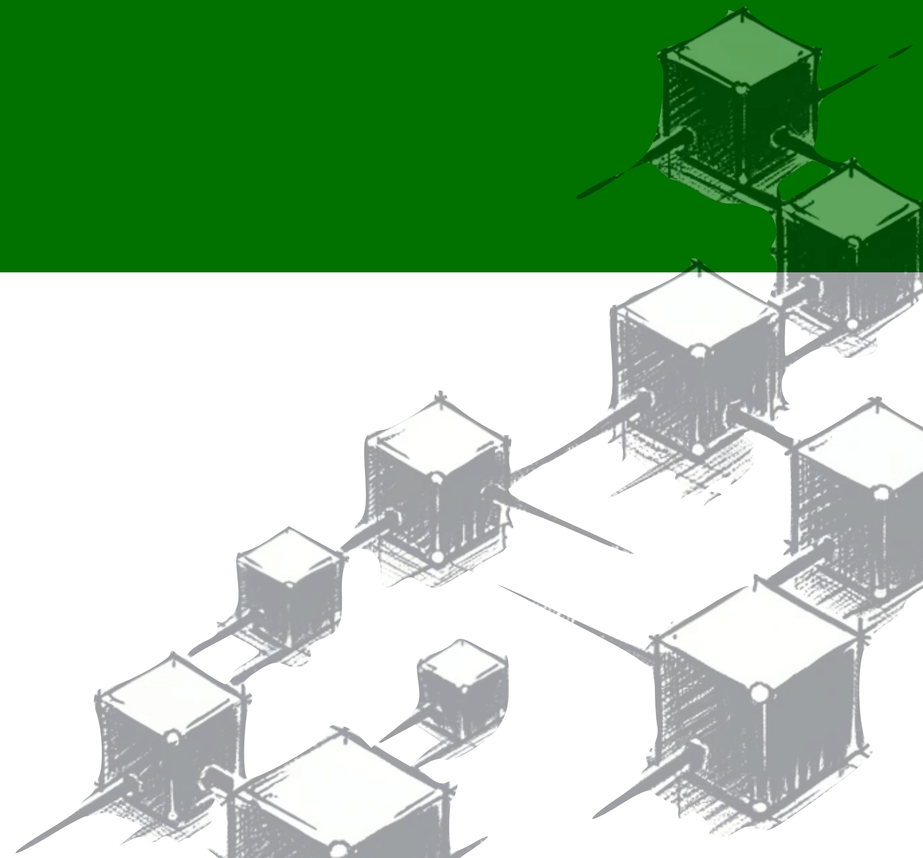
Proof of Work



とてもむずかしい計算問題

NFT

Non fundgeble token



トークン
Token

- ブロックチェーン上に任意のデータを載せ、流通させたものを**トークン**と呼ぶ
- あらゆる権利や価値、デジタルアイテムをデータ化し、管理・活用が可能
- ゲーム内アイテム、証明書、チケット、会員権、投票権など、多様な用途

代替性トークンと非代替性トークン

Token

- トークンは**代替性トークン（FT）**と**非代替性トークン（NFT）**の2種類
- 代替性とは、同じ種類のもの同士が入れ替え可能な性質
- 例：1円玉や1BTCは、どれと交換しても同じ価値を持つ
- **代替性トークン（FT）**は、量によってのみ価値が決まる

代替性トークンと非代替性トークン

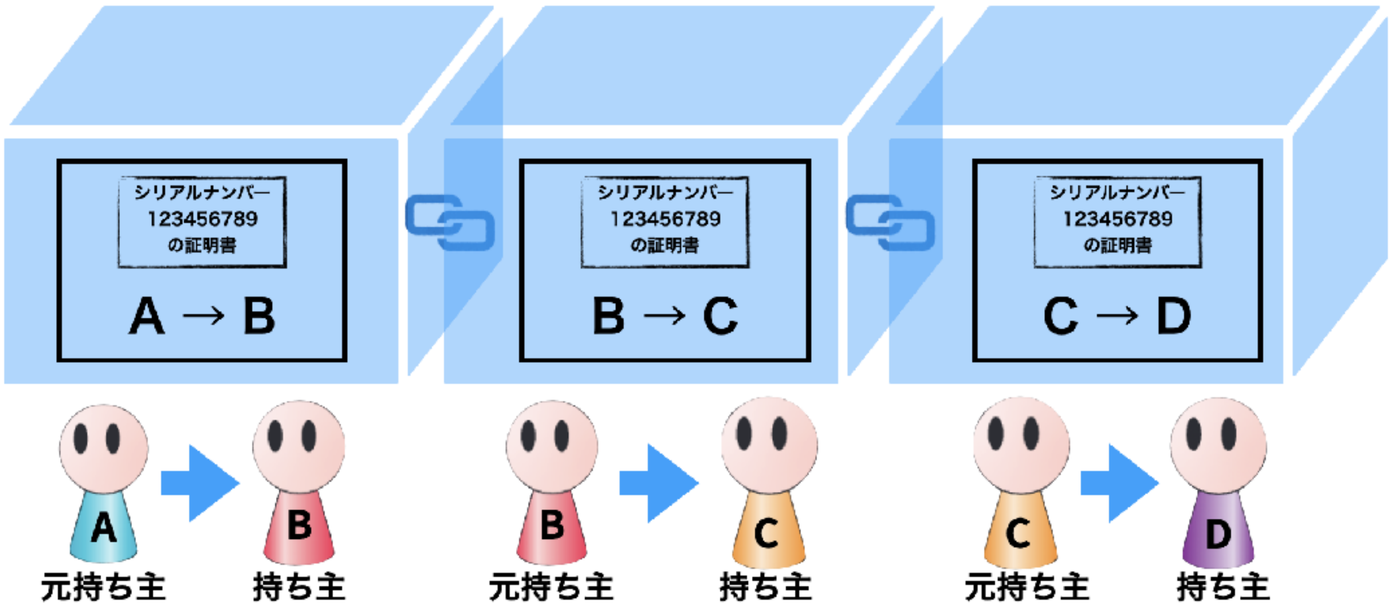
Token

- 非代替性とは、一つひとつがユニークで等価交換ができない性質
- 例：有名画家の絵画は唯一無二の価値を持つ
- 代替性を持たないトークンを**NFT**と呼ぶ。

NFTは所有者がチェーンに記録される

NFT

- NFTは、発行者と所有者がブロックチェーン上に記録される仕組み
- これにより、デジタルデータにも唯一のオリジナルと所有者の証明が可能

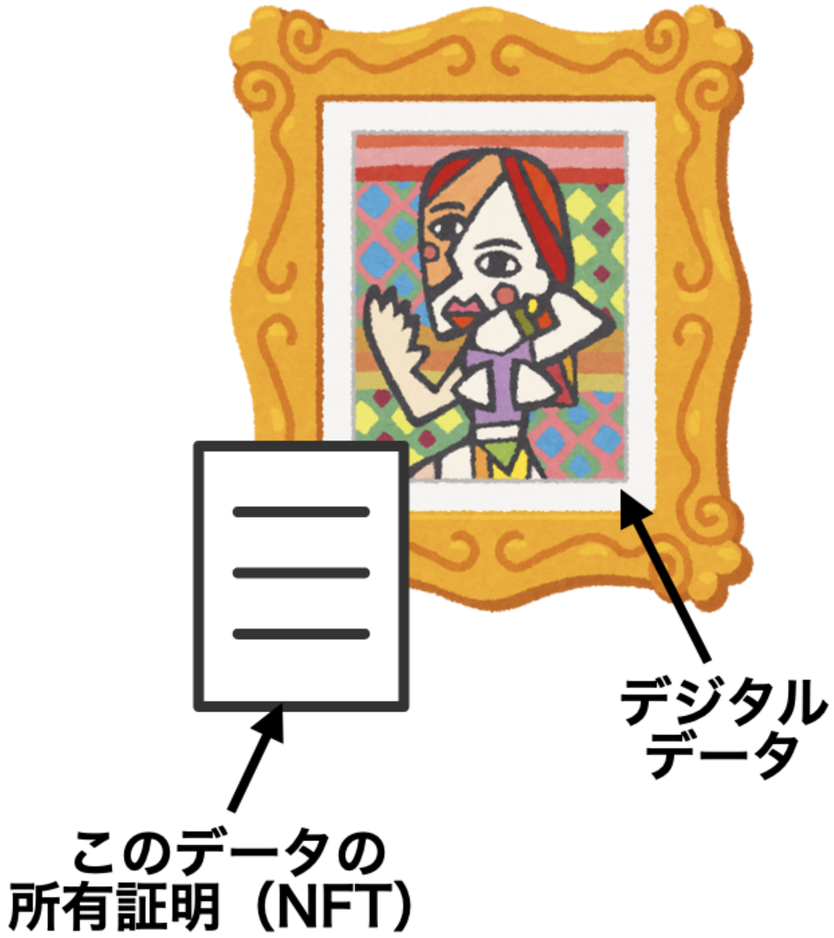


所有権
ownership

- NFTの「所有権」は、法律上の所有権とは異なる概念
- 法的な所有権は、法律が保護する物理的な権利のこと
- 一方、NFTの所有権は、ブロックチェーン上のデジタル証明のこと
- NFTを所有しても、コンテンツの法的権利が得られるわけではない！
- NFTは**「デジタル上の所有証明」**として理解することが重要

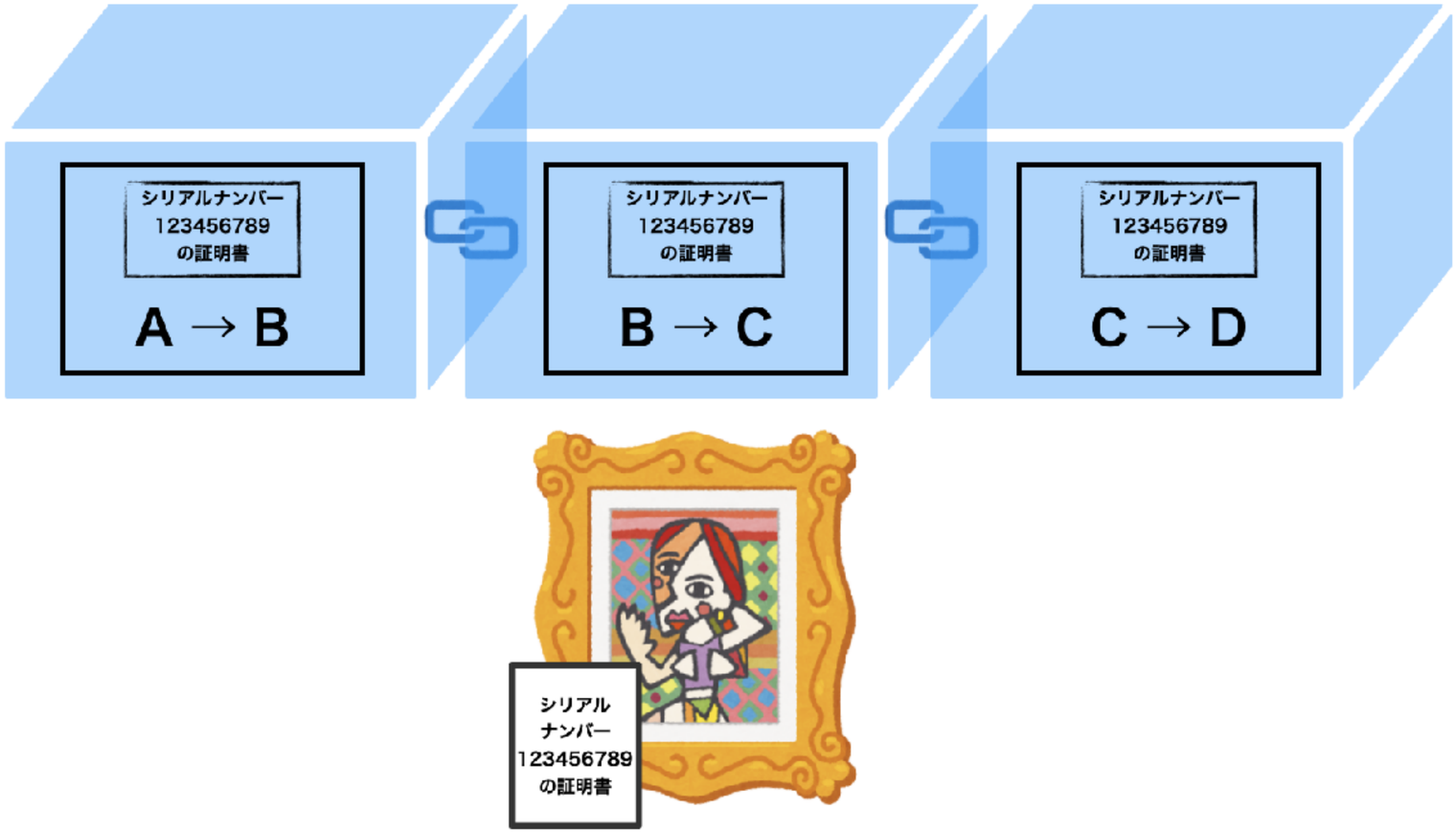
NFTのイメージ

NFT



NFTのイメージ

NFT



NFTはコピーできない？

Can you copy NFT ?

- 「NFTはコピーできない」という表現は誤解を招く場合がある
- デジタルデータ自体はコピー可能であり、保存やスクリーンショットも可能
- 唯一無二なのは、NFTとして発行される「証明書」のほう
- NFTは、ブロックチェーン上に記録された唯一のデジタル証明書
- NFTは「この人が本物を所有している」という事実を証明する役割
- 作品のコピーには正式なNFTがないため、本物とは認められない
- 現実世界の絵画の「鑑定書」と同じように、NFTが価値を証明する役割

オンチェーンとオフチェーン
On chain and Off chain

- データの保存方法には**オンチェーン**と**オフチェーン**の2種類
- オンチェーンはデータをブロックチェーン上に直接保存する方法
- オフチェーンはデータをブロックチェーン外に保存し、NFTにリンクを記録
- データの保存場所と信頼性の確保がNFTの価値に影響する重要な要素

1SatOrdinals

1SatOrdinals

- **1SatOrdinals**は、BSVの最小単位Satoshiに番号を付与してNFTを実現
- オンチェーンでデータを扱う
- 安価な手数料、高速な承認で、気軽にNFTを扱える！