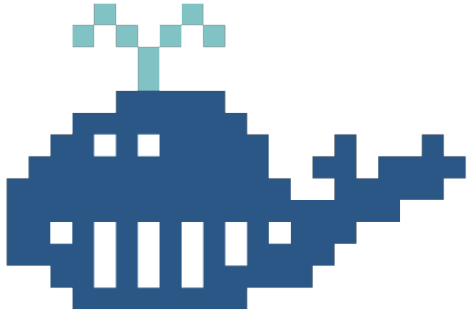


第５回：暗号通貨とは何か？

注意点

▼Not Investment Advice

資産運用はリスクが伴うものです。クジラの管理人は投資対象の展望を伝えることもありますが、投資は一切推奨しません。自己責任でお願いします。

▼Do Your Own Reserch

闇雲に情報を信頼せず、自分で学んで考える姿勢を持ちましょう。
資金を失うことも珍しくはありません。

▼No Promotion

くじらの管理人で紹介するサービスには原則プロモーションを含むことはありません。仮にプロモーションを含む場合は開示します。

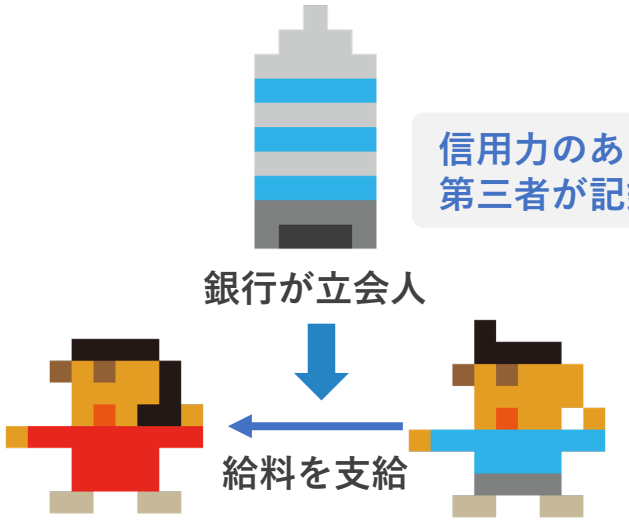
ブロックチェーンとは

ブロックチェーンとは

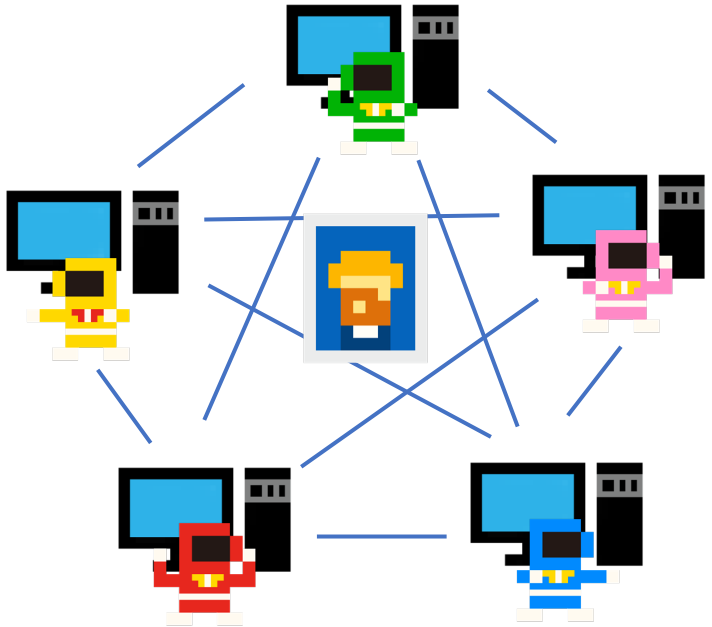
分散型台帳技術(Distributed Ledger Technology)と呼ばれる。
管理者不要かつデータの改ざんができない状態で取引履歴を維持できる台帳管理を実現させるための技術である。
ブロックチェーンの基本の考え方→その場にいる全員が同じことを知ってれば嘘をついても多数決でバレる。

分散型の意味

取引には第三者の立会いが不可欠です。
第三者が立会うことで取引は証明されます。



ある特定の機関が記録・証明を行うという点で
中央集権的と言われる。



お互いに監視し合うことで、
データの破壊や改ざんを防ぐ。

参加者みんなで記録・証明を行うという点で
非中央集権的(分散型)と言われる。

暗号通貨とは

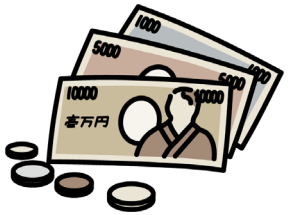
暗号通貨とは

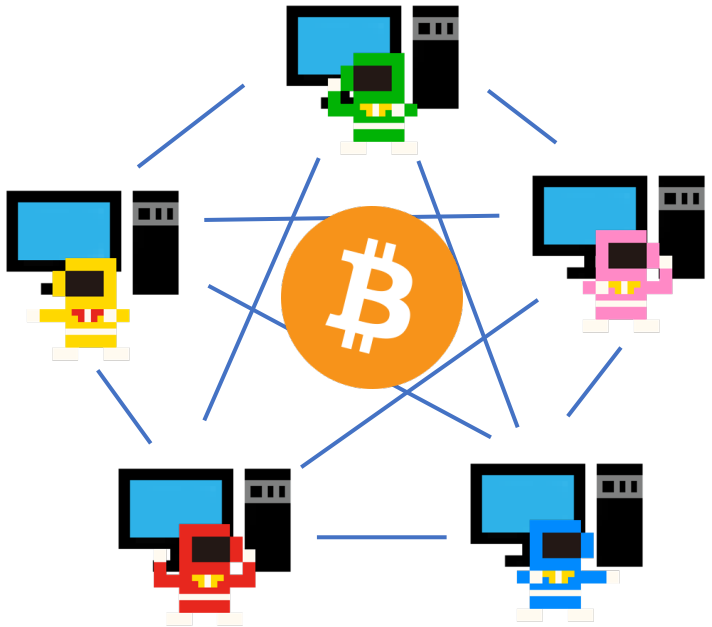
ブロックチェーンを活用したデジタルのお金。
ブロックチェーンの技術を使えば、みんなでお金が生み出せることから生まれた。

日本国

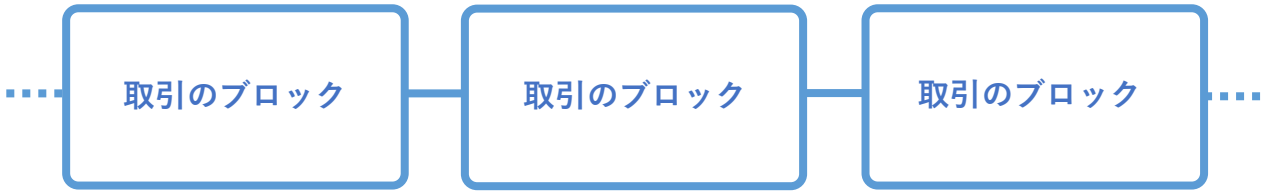
日本銀行

日本円を発行





暗号通貨を使う全ての人の間で使え、
全ての人が発行できる。

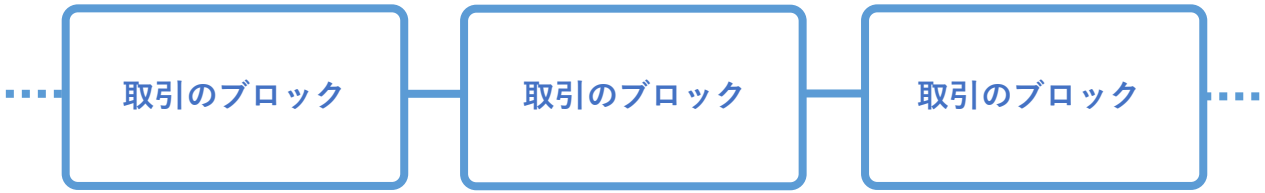


取引に立会い、記録、証明という仕事をした人に
新しい暗号通貨が発行される。

ビットコインとは

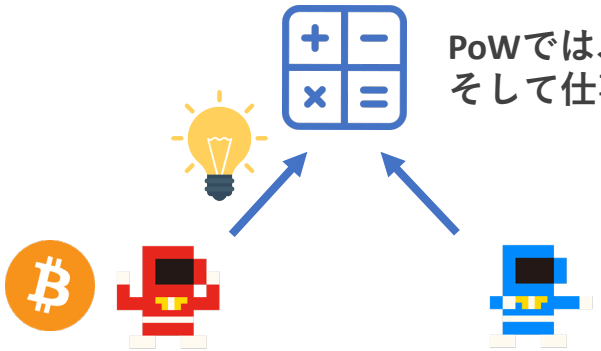
世界で初めて誕生した暗号通貨がビットコインです。
ビットコインは国や銀行などを介することなく、国境を越えて安価な手数料で送金できるデジタル通貨を作ることが開発の目的でした。

ビットコインの特徴



立会い、記録、証明の仕事を行うルールのことを
コンセンサスアルゴリズムという。

ビットコインのコンセンサスアルゴリズムは
プルーフオブワーク(PoW)が使われている。



PoWでは、ある計算問題が出題され、一番早く解いた人が一連の仕事ができる。
そして仕事の対価として新しく発行されたビットコインがもらえる。

この工程をマイニングという。
マイニングする人をマイナーという。

ビットコインの概要

ティッカー	BTC
発行開始年月	2009年1月
コンセンサス アルゴリズム	PoW
上限発行量	約2100万枚
ノード数	約14705(2022年5月時点)
送金時間	約10分

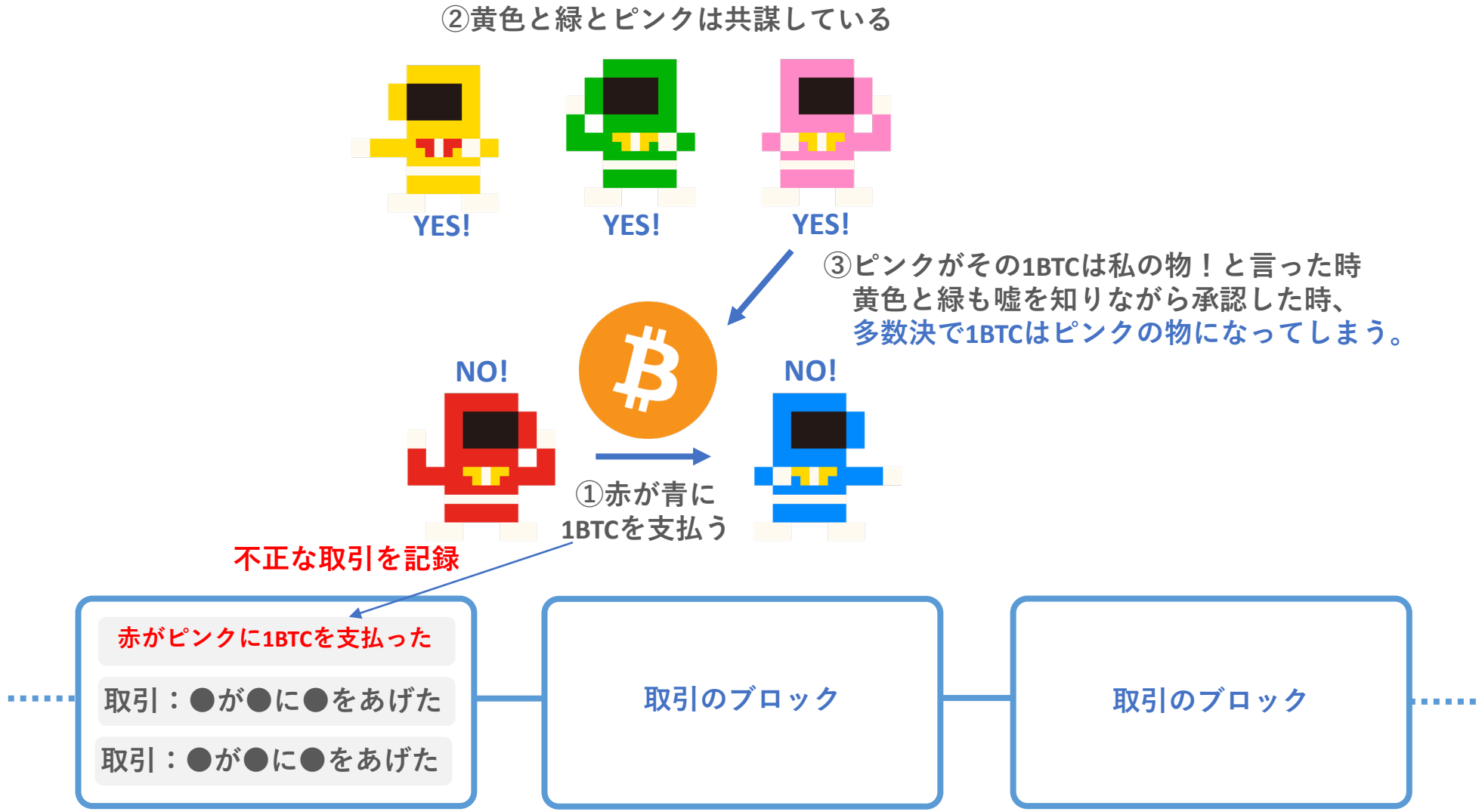
発行量の上限があるため、金と同様に希少性が高いと考えられ「デジタルゴールド」と呼ばれる。
インフレヘッジとして投資されることが多い。

ノード数は取引の検証をするパソコンの数。
多ければ多いほど分散されているということであり、セキュリティが高い。

取引を承認する間隔が10分に1回になるように自動調節されている。取引量が増えるほど処理に時間がかかり、取引手数料も高くなる。

51%攻撃とは

暗号通貨の脅威の1つに51%攻撃があります。ブロックチェーンの基本の考え方に「その場にいる全員が同じことを知ってれば嘘をついても多数決でバレる。」とありましたが、多数が共謀して嘘をついたらどうなるでしょう？



51%攻撃は防げるか？

現在51%攻撃に対する決定的な対処法は存在しません。
しかし、そもそも51%攻撃を行うためには非常に多くの費用がかかることや、仮に成功したとしても、攻撃された通貨の価値は急落して価値がなくなることから、51%攻撃を行うメリットが小さいと言えます。

Bitcoin (BTC)

Cost for a 51% attack

Market cap	$654.88 B
Mining algorithm	SHA-256
Network hash rate	226,489 PH/s
Nicehash cost	0.004 BTC / PH / day
Nicehash cost / hr	$6.01 / PH / hour
Estimated cost of 1 hour 51% attack	*$1,361,613*
Nicehash capacity	369 PH/s
Nicehash percentage of network	0%

51%攻撃を１時間行うことにかかるコスト