Bitcoin 完全に理解した

About me

Kan Ueno(https://scrapbox.io/kanna/about_me)

Software Engineer @Belong Inc
Bitcoin が大好きな人

今日話すこと

Bitcoin は今までのデジタルマネーとなにが違うのか
Bitcoin でなにができるのか

Bitcoin は新しいデジタルマネー

Photo by Vadim Artyukhin on unsplash

Photo by steve pancrate on unsplash

Photo by Markus Winkler on unsplash

Photo by Nathan Dumlao on unsplash

古いデジタルマネーの課題

なんでも銀行の許可が必要

口座を作るのも許可制

送金するのも許可制

アプリを作るのも許可制

Photo by Daniel Lloyd Blunk-Fernández on unsplash

なぜ許可が必要なのか

お金がコピーできると困る

デジタルデータは簡単にコピーできることが特徴

お金の場合はコピーできてはいけない

銀行が管理する必要がある

Photo by Colin Watts on unsplash

Bitcoin のアプローチ

みんなで仲良く管理する🥳
でもそれは難しい🤔
持ち回りで管理しよう

競争して勝った人が管理者になる🚴

Photo by Duy Pham on unsplash

マイニング

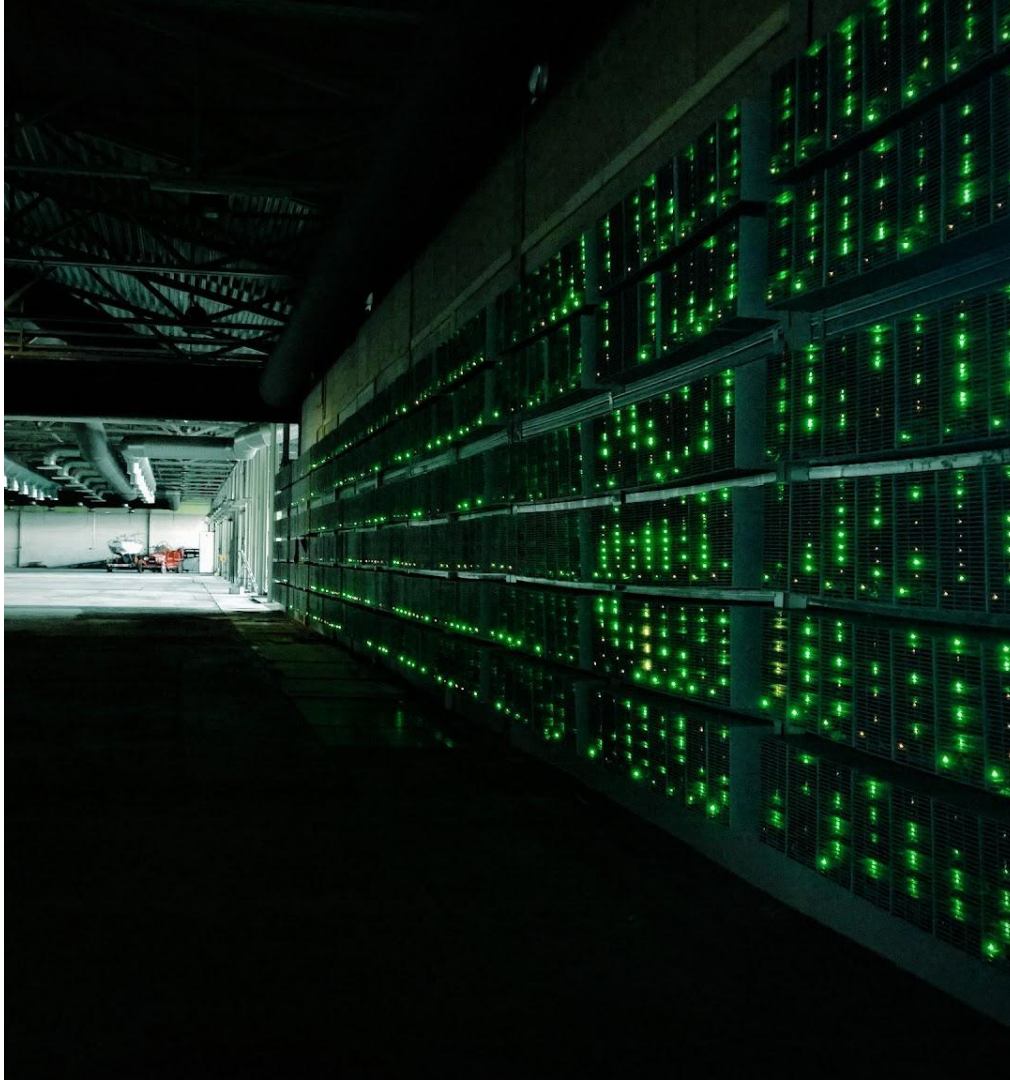
管理者を決めるための競争

計算をして最初に答えを見つけた人が管理者になる

管理者は Bitcoin の取引を決めることができる

報酬がもらえる

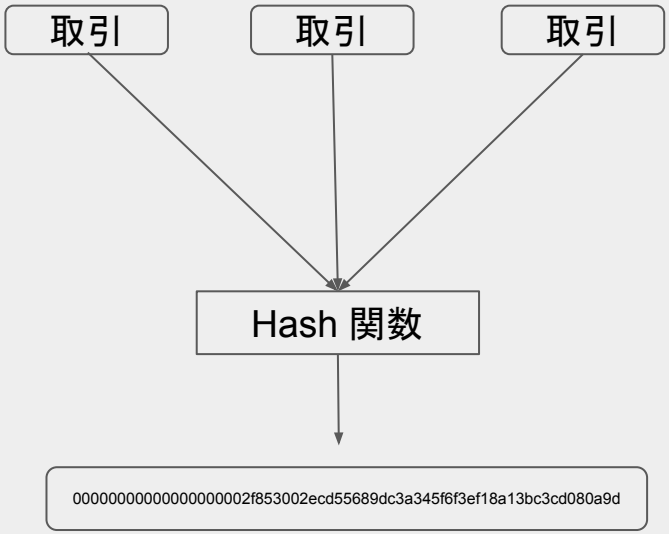
誰でもマイニングできる



Marko Ahtisaari, CC BY 2.0, via Wikimedia Commons

ちょっと詳しいマイニング

1. 承認したい取引をまとめる
2. 取引を Input に Hash 値を計算する
3. Hash 値が条件を満たすまで繰り返す



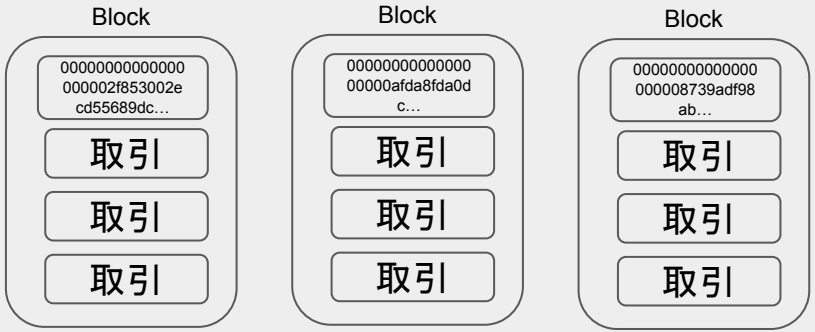
(Block 720585の Hash 値)

Hash 関数とはなんだったか

同じ Input に対しての Output は必ず同じ
Input が少しでも変わると Output は全く異なる値
Output から Input を逆算できない

マイニングの役割

1. 管理者を決める
2. 取引が承認される
3. bitcoin が新規に発行される



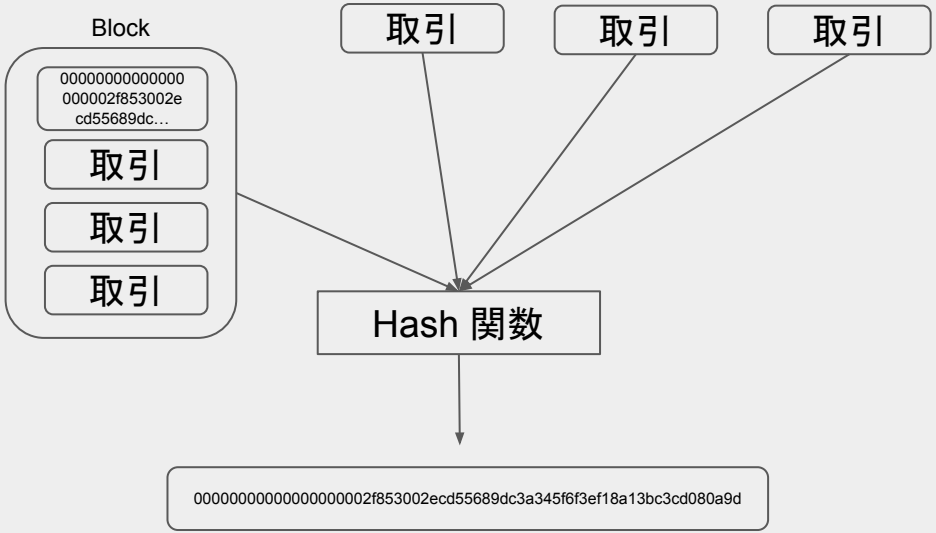
Hash 関数とはなんだったか

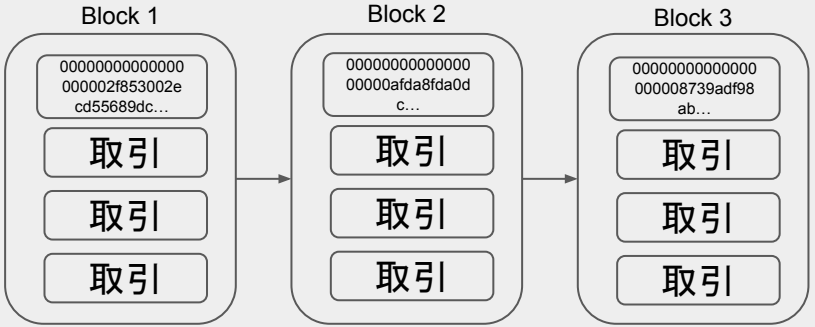
同じ Input に対しての Output は必ず同じ
Input が少しでも変わると Output は全く異なる値
Output から Input を逆算できない

マイニングをもうひと工夫

ブロックの順番が決まる

あとから変更することが難しい





Hash 関数とはなんだったか

同じ Input に対しての Output は必ず同じ
Input が少しでも変わると Output は全く異なる値
Output から Input を逆算できない

Blockchain

Blockchain は Bitcoin のためにつくられたデータ構造

変更が難しいデータ構造である

Photo by Shubham Dhage on unsplash

Bitcoin の新規性

銀行という管理者をなくした

銀行がなくてもお金を発行している
銀行がなくてもお金が流通している

誰の許可も受けずにお金を送れる 🎉
誰の許可も受けずにアプリが作れる 🎉

Photo by NASA on unsplash

Bitcoin のある世界

お金に無限の可能性がある

誰でも Bitcoin をよいものにしていくことができる

誰でも Bitcoin を使ってアプリケーションが作れる

誰でもお金をデザインできる

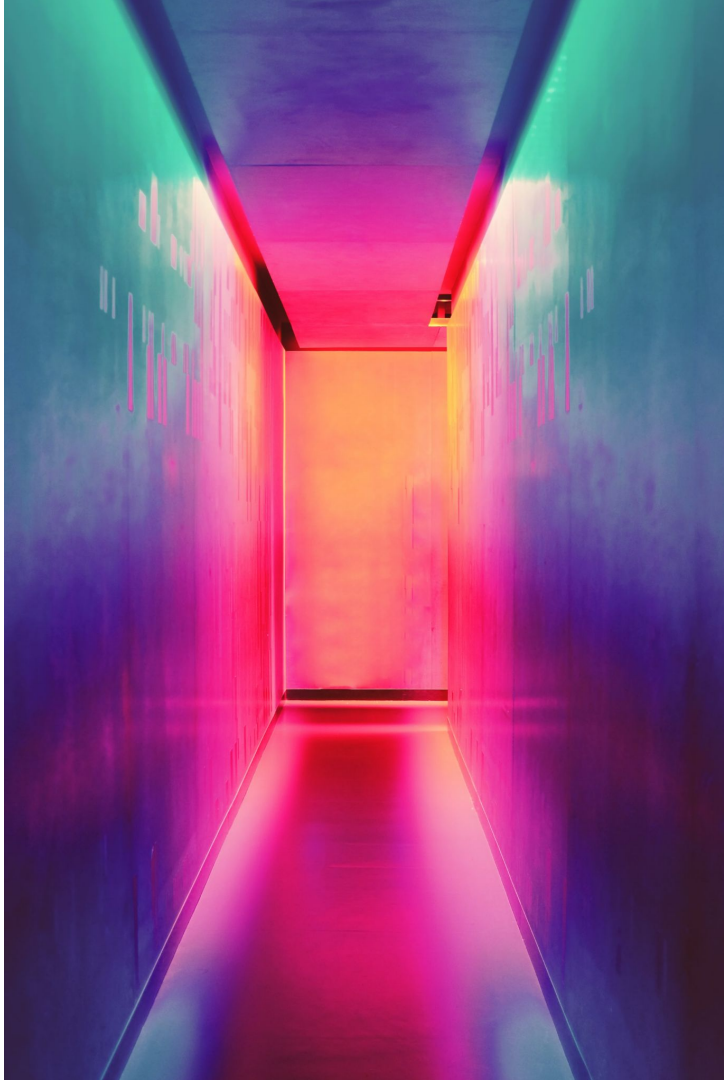


Photo by Efe Kurnaz on unsplash