Orchestrating a brighter world

NEC

サイエンスアゴラ2019

暗号技術が支えるビットコインのしくみ

セキュリティ研究所
佐古和恵
日本学術会議　連携会員
一般社団法人　MyDataJapan 副理事長
2019.11.16

\Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

自己紹介

佐古和恵　博士（工学）

ＮＥＣ　中央研究所　セキュリティ研究所　特別技術主幹

Sovrin Foundation 理事／日本応用数理学会　前会長

- 入社以来、電子投票システム、電子抽選システム、匿名認証技術など、セキュリティとプライバシを両立させる暗号プロトコル技術の研究開発に従事。
- 日本学術会議連携会員、H29-30 電子情報通信学会副会長, MyDataJapan 副理事長
- 金融分野のセキュリティを扱う国際会議Financial Cryptographyの実行委員長(2013)　プログラム共同委員長(2018)
- 公開鍵暗号国際会議PKC(2019) 欧州セキュリティ国際会議ESORICS(2019) プログラム共同委員長
- ISO TC307「ブロックチェーンと分散台帳技術」国際エキスパート
- 情報処理学会学会誌 2016年9月号

「透明性と公平性を実現するブロックチェーン技術」

大注意

本講座では暗号資産ビットコインの技術の紹介をしますが、

決して暗号資産の購入を勧めるものではありません。

暗号資産の価値は必ずあがる、とか、必ずもうかる、ということはありません。

壮大な「社会実験」みたいなものです。

買うなら、お小遣いの範囲で！

ご参考：チューリップ・バブル(1630年代)

- Wikipediaより：

　オランダ黄金時代（略）において、当時オスマン帝国からもたらされたばかりであったチューリップ球根の価格が異常に高騰し、突然に下降した期間を指す。

- 一説によると、1637年には、「1個当たり、熟練した職人の年収の10倍以上の価格で販売される球根もあった」

- 英国ジャーナリスト、チャールズ・マッケイ著（1841年）

『Extraordinary Popular Delusions and the Madness of Crowds

　直訳：異常にはやった妄想と人々の狂気

（邦題：狂気とバブル　―　なぜ人は集団になると愚行に走るのか）』

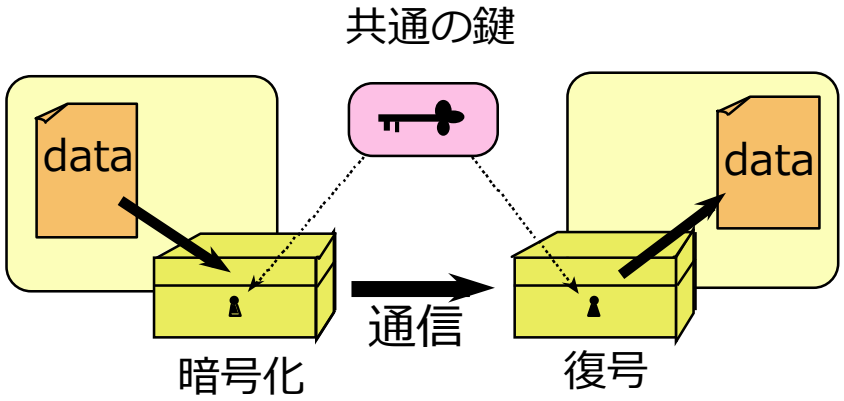
目次

1. 暗号技術について
   公開鍵暗号・デジタル署名
2. ビットコインの動作概要（イメージ）
3. ビットコインにおけるその他の暗号技術
   ハッシュ関数・ハッシュチェーン
4. Q&A

1. 暗号技術について

共通鍵暗号

共通鍵暗号

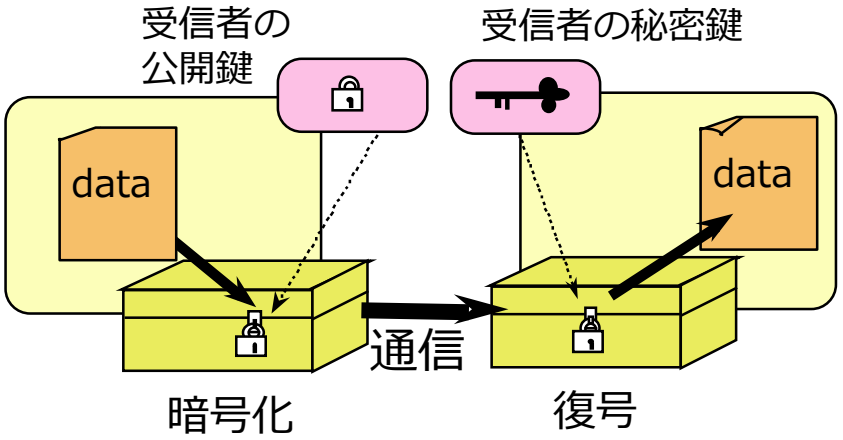


- データと「鍵」を「暗号化アルゴリズム」に入力すると、「暗号文」が計算される。
- 「暗号化アルゴリズム」を知っていても、「鍵」を知らないと、「暗号文」から元の「データ」がわからない！
- 「暗号文」と「鍵」を「復号アルゴリズム」に入力すると元の「データ」が得られる。

公開鍵暗号（１９７０年代）

- データと「暗号化鍵」を「暗号化アルゴリズム」に入力すると、「暗号文」が計算される。
- 「暗号化アルゴリズム」を知っていても、**暗号化鍵を知っていても**「**復号**鍵」を知らないと、「暗号文」から元の「データ」がわからない！
- 「暗号文」と「**復号**鍵」を「復号アルゴリズム」に入力すると元の「データ」が得られる。
- 暗号鍵→公開鍵
- 復号鍵→秘密鍵

- 公開鍵暗号



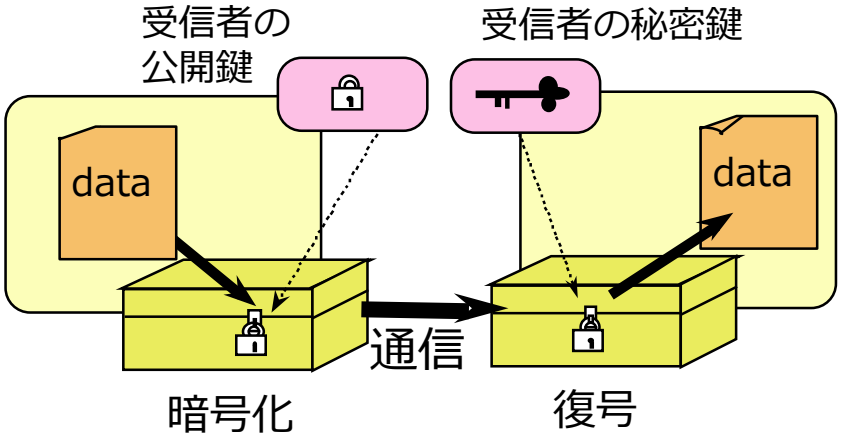
公開鍵暗号どうつくるの？

- 「暗号化鍵（公開鍵）」がわかっても「**復号**鍵」がわからないようにしたい。
- RSA暗号のアイディア：

　素因数分解が難しいことを利用して、公開鍵を２素数の積（掛け算）に、秘密鍵を素因数にする！

- 公開鍵：１５
  秘密鍵：３と５
- 公開鍵：10進数で300桁
  秘密鍵：150桁

- 公開鍵暗号



公開鍵暗号どうつくるの？（その２）

- ちゃんと復号できるようにしたい
- RSA暗号のアイディア：

フェルマーの小定理を使うと、素数pに対して、p-1以下の数はすべてp乗してpで割った余りが元の数になる！

- 試してみよう！

p=5

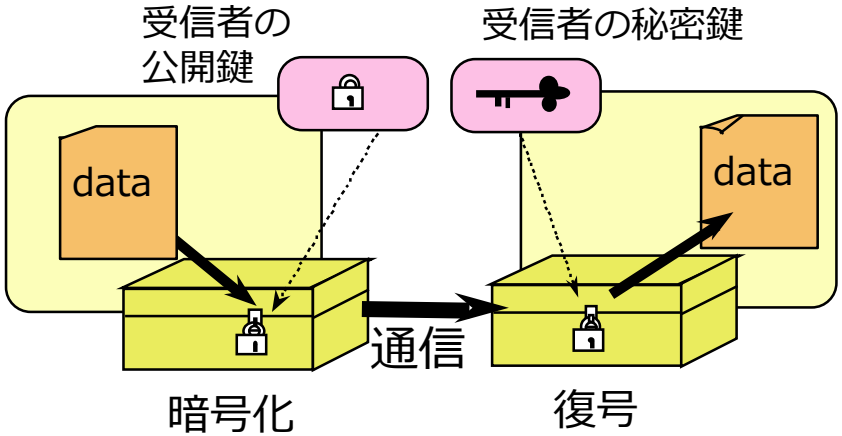
2を5乗すると、32　pで割って？

3を5乗すると 243

p=7 2を7乗すると？

- データをｘ乗してもらって、のこりのp-x乗すれば、元のデータになる！

- 公開鍵暗号



RSA暗号
(Rivest-Shamir-Adleman)

準備

すべてのMに対して

$M^{ed}=M(\mathrm{mod}\ N)$

になるようなe, d, Nの組を作る。

e,nは公開し、dは秘密に保管する。

暗号化

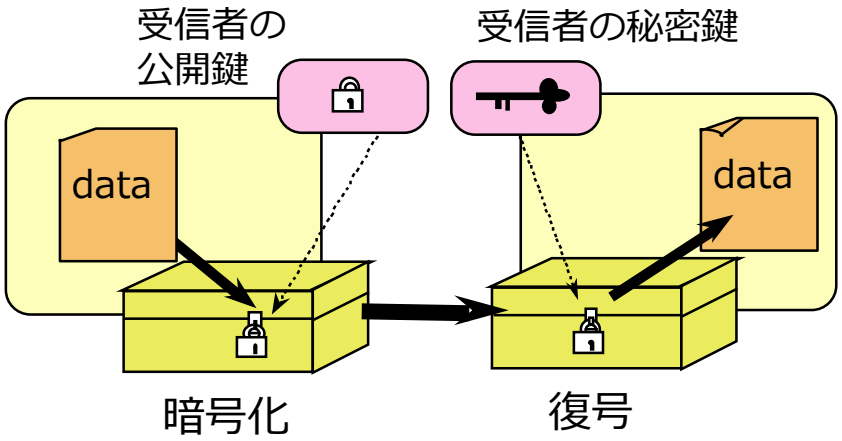
$C = M^{e}\ (\mathrm{mod}\ N)$　　誰でもできる

復号

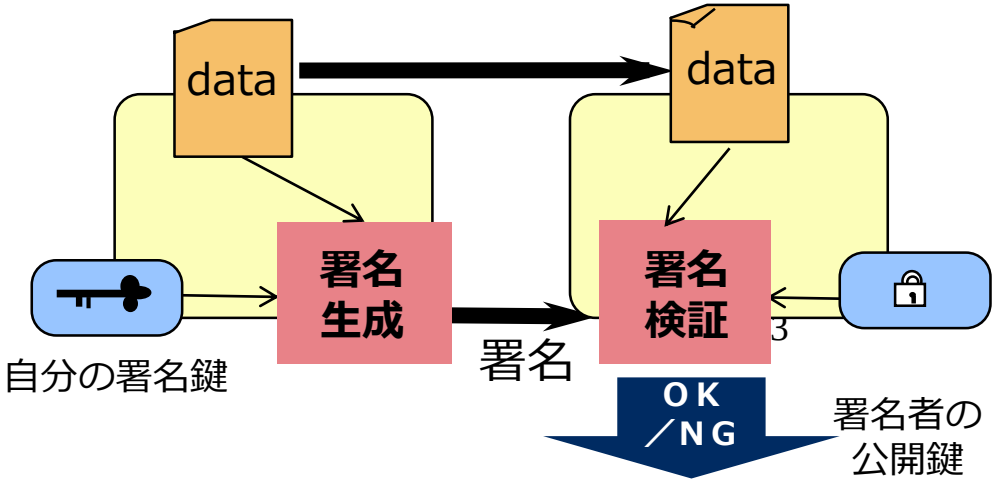
$M = C^{d}\ (\mathrm{mod}\ N)$　　dを知る人だけが可能

公開鍵暗号とデジタル署名

公開鍵暗号



デジタル署名



「暗号」という日本語

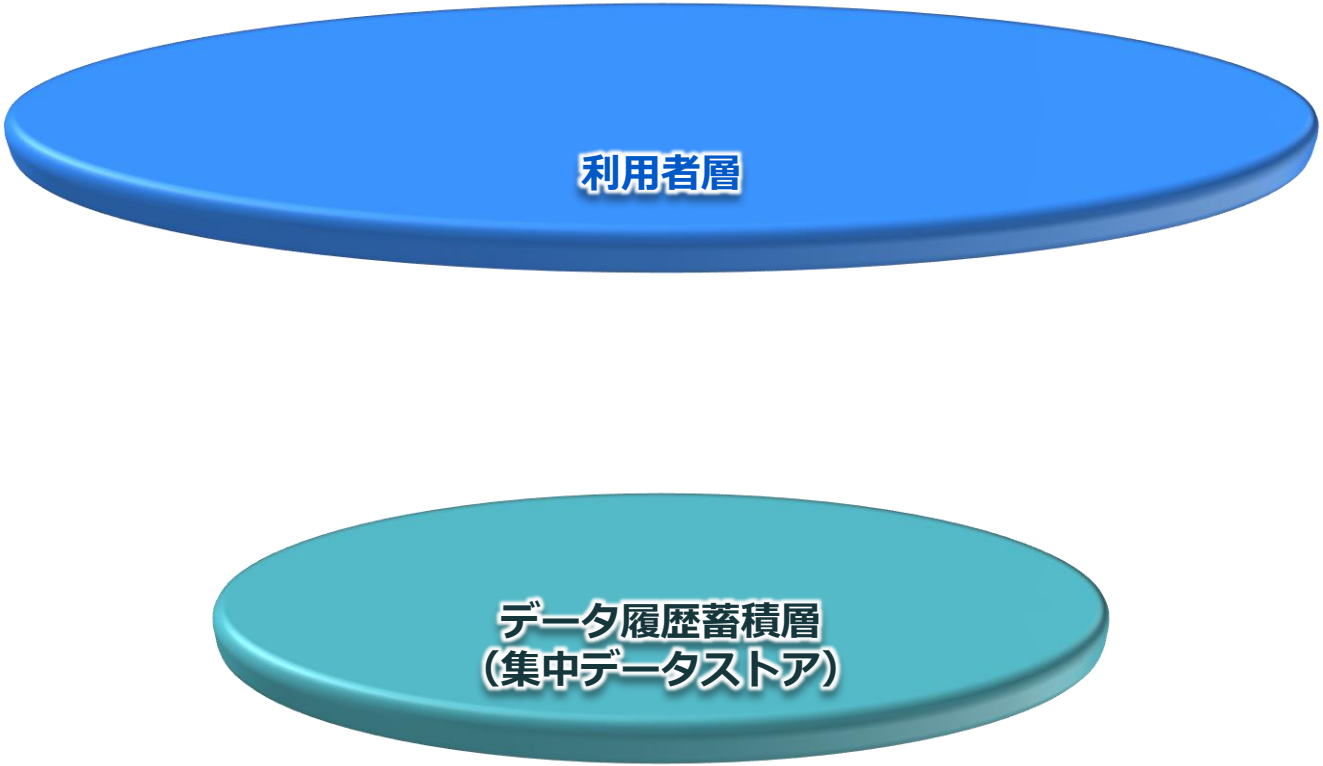
- 英語ではEncryption(データを暗号化する）とCryptography（秘匿に関する学問）という言葉がある
- デジタル署名は「署名鍵」を秘匿するのでCryptographyだけど、データは暗号化しない。
- 日本語になったときにどちらも「暗号」になってしまった！！

- ビットコインはデータは暗号化せず、デジタル署名のみを使う！

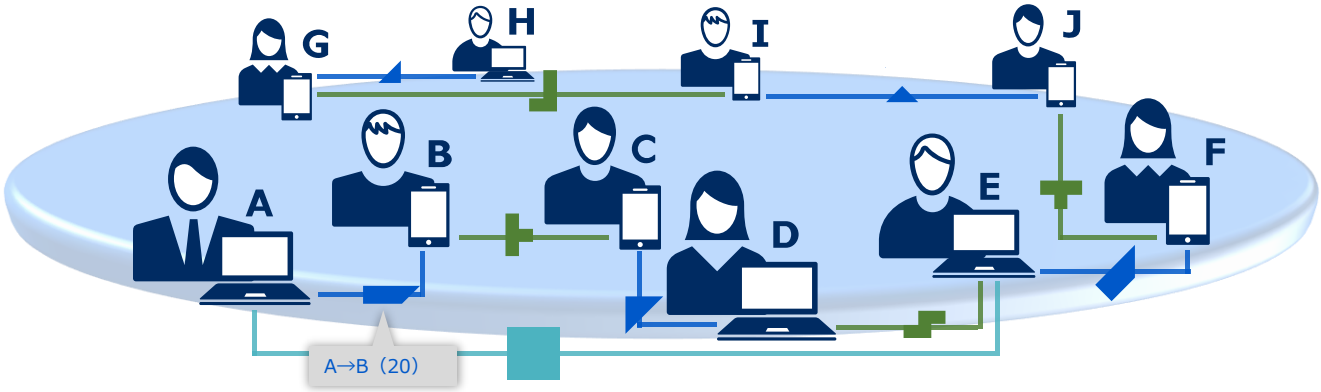
2.ビットコインの動作概要（イメージ）

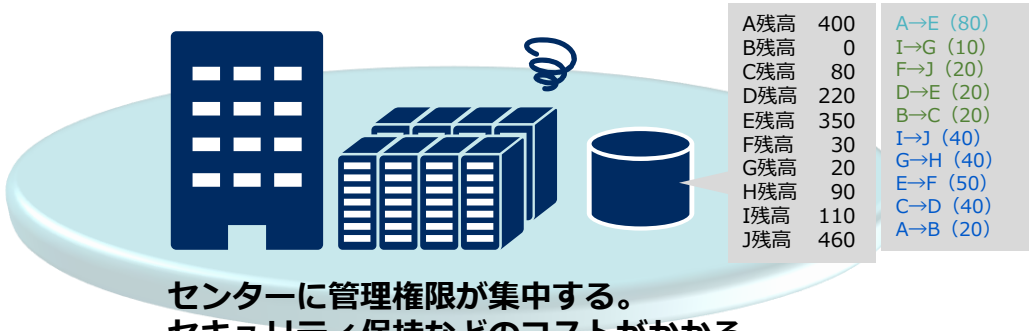
ビットコインで使われているデータ管理技術である
「ブロックチェーン」を紹介します

従来型：センターサーバで集中管理（集中データストア）



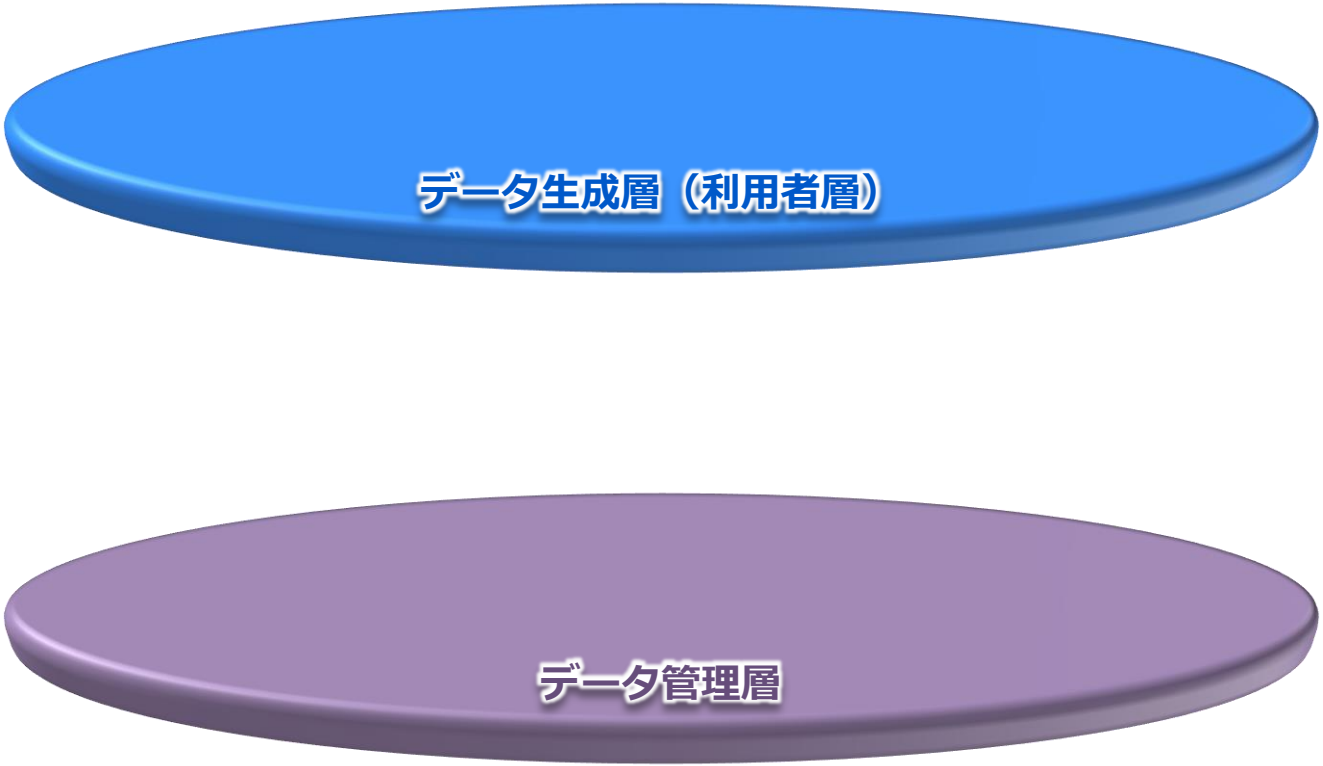
従来型：センターサーバで集中管理（集中データストア）



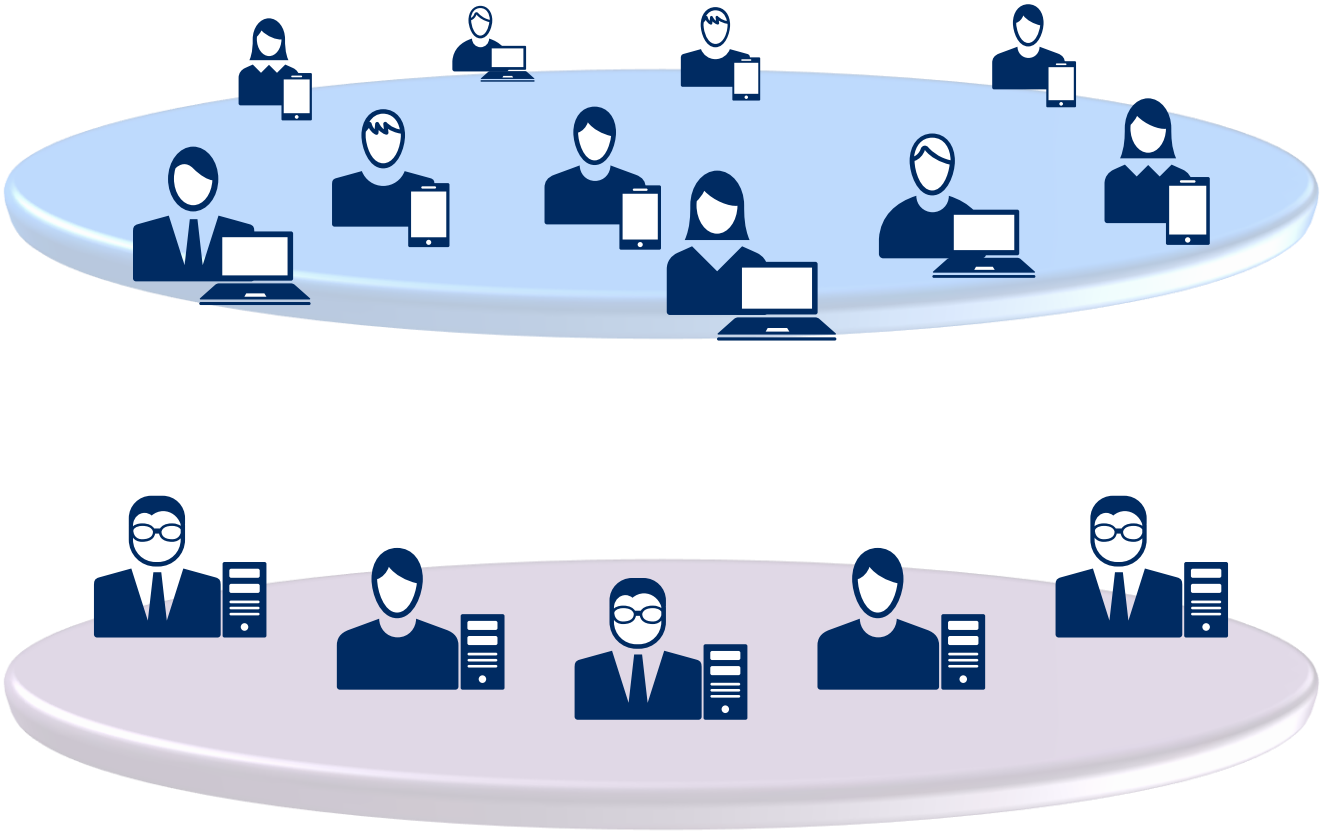


センターに管理権限が集中する。
セキュリティ保持などのコストがかかる。

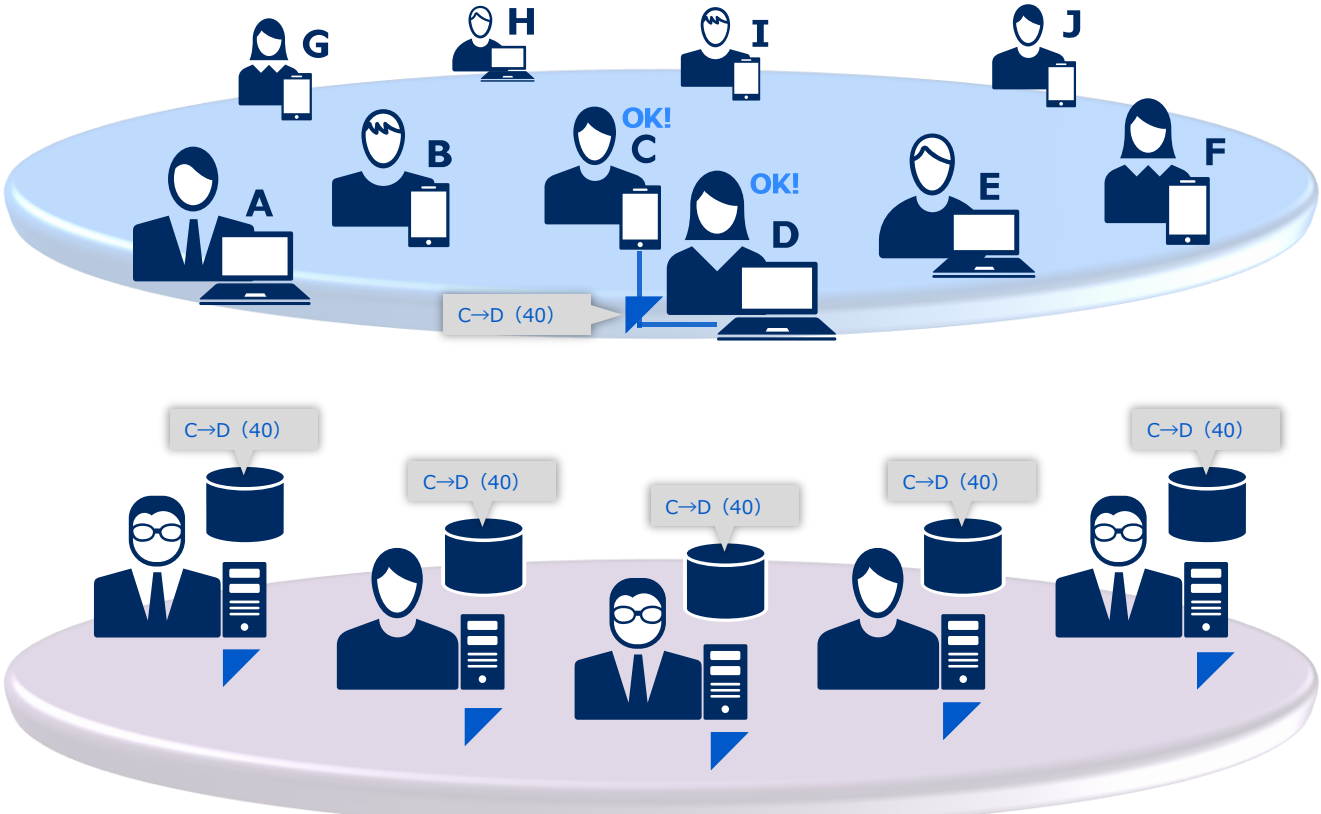
ブロックチェーン ｜ 利用者と管理者



ブロックチェーン ｜ 複数の管理者が存在

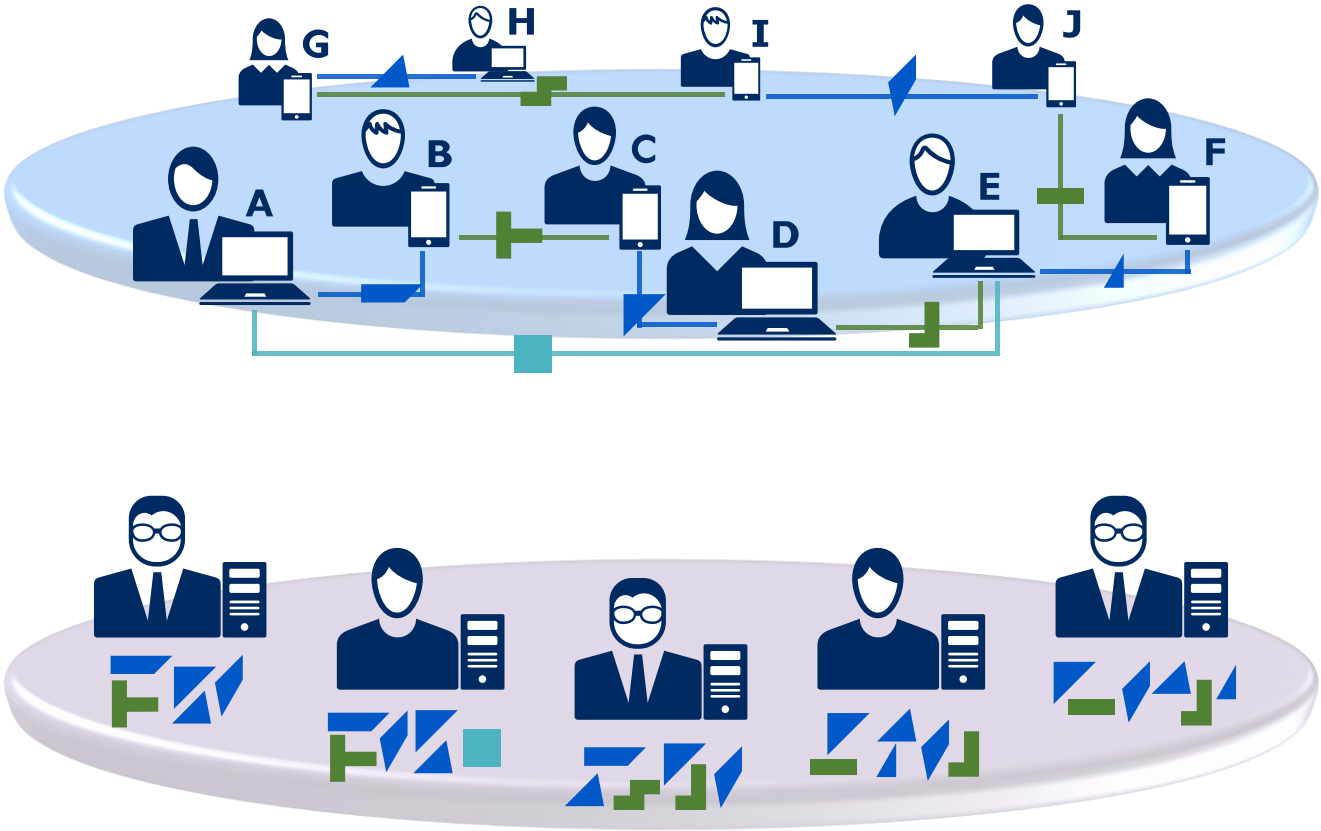


ブロックチェーン ｜ 管理層でデータが広まる



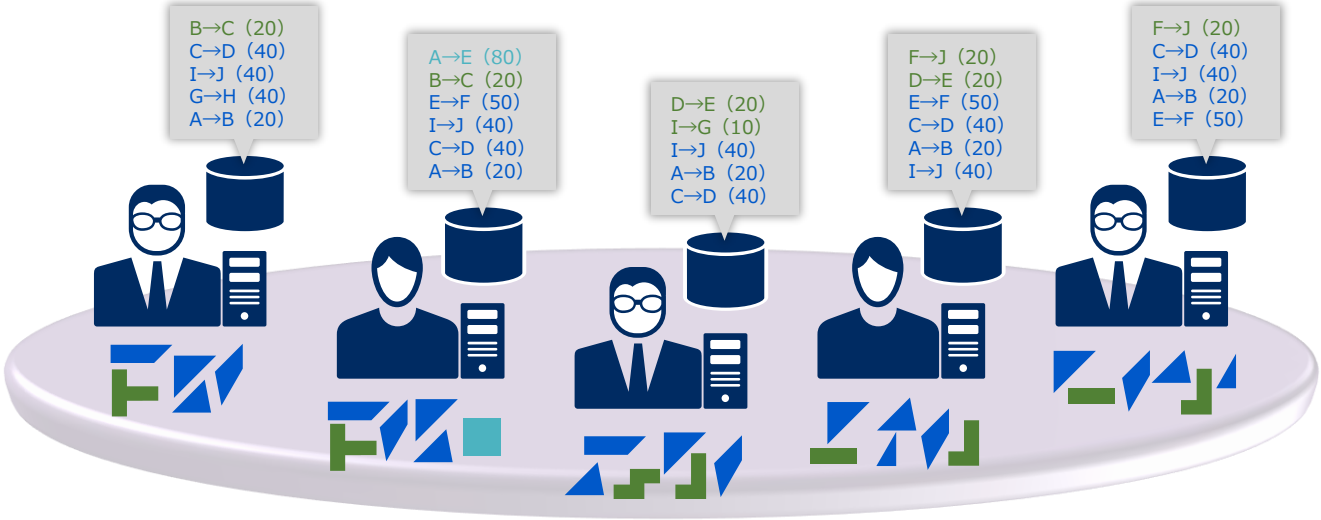
正当なデータであれば、P2P通信でデータ管理層内に同報する。

ブロックチェーン ｜ あちこちで絶え間なくデータが発生



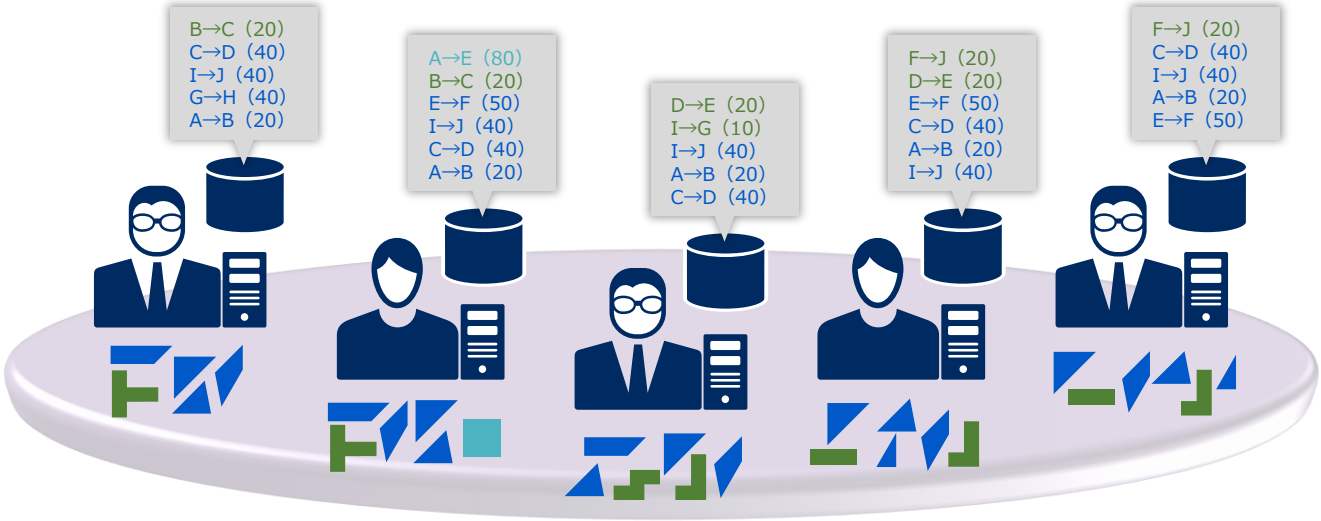
ブロックチェーン ｜ 管理層のデータに差異が出る

データ個数も順番も不一致



ビットコインが解きたい問題

どうしたら、一致させられるか？



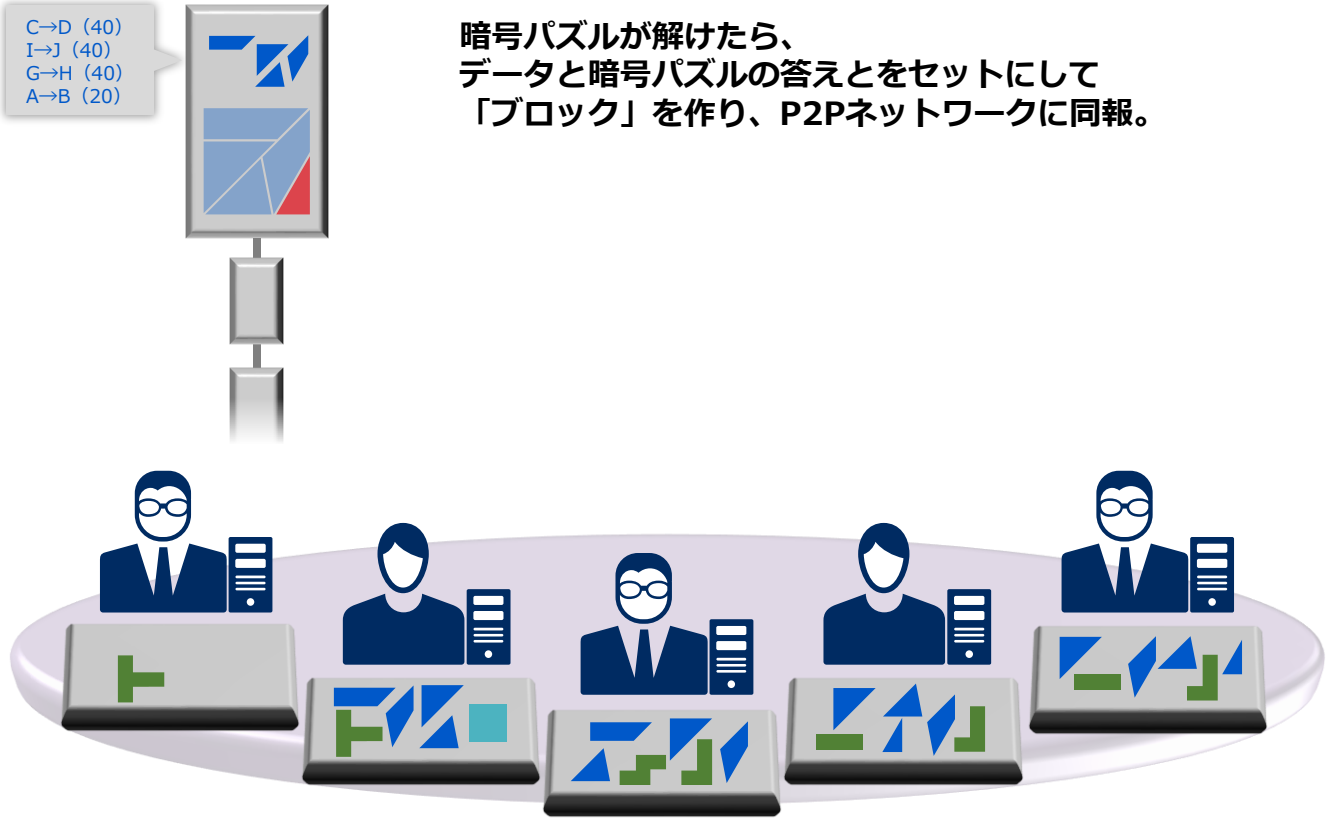
ブロックチェーン ｜ ブロック作り＝暗号パズルの早解き

データや順番を同期させる時間稼ぎために、
早い者勝ちの暗号パズルを解く。（マイニング）

正方形を作るために、
足りないピースのかたちは？

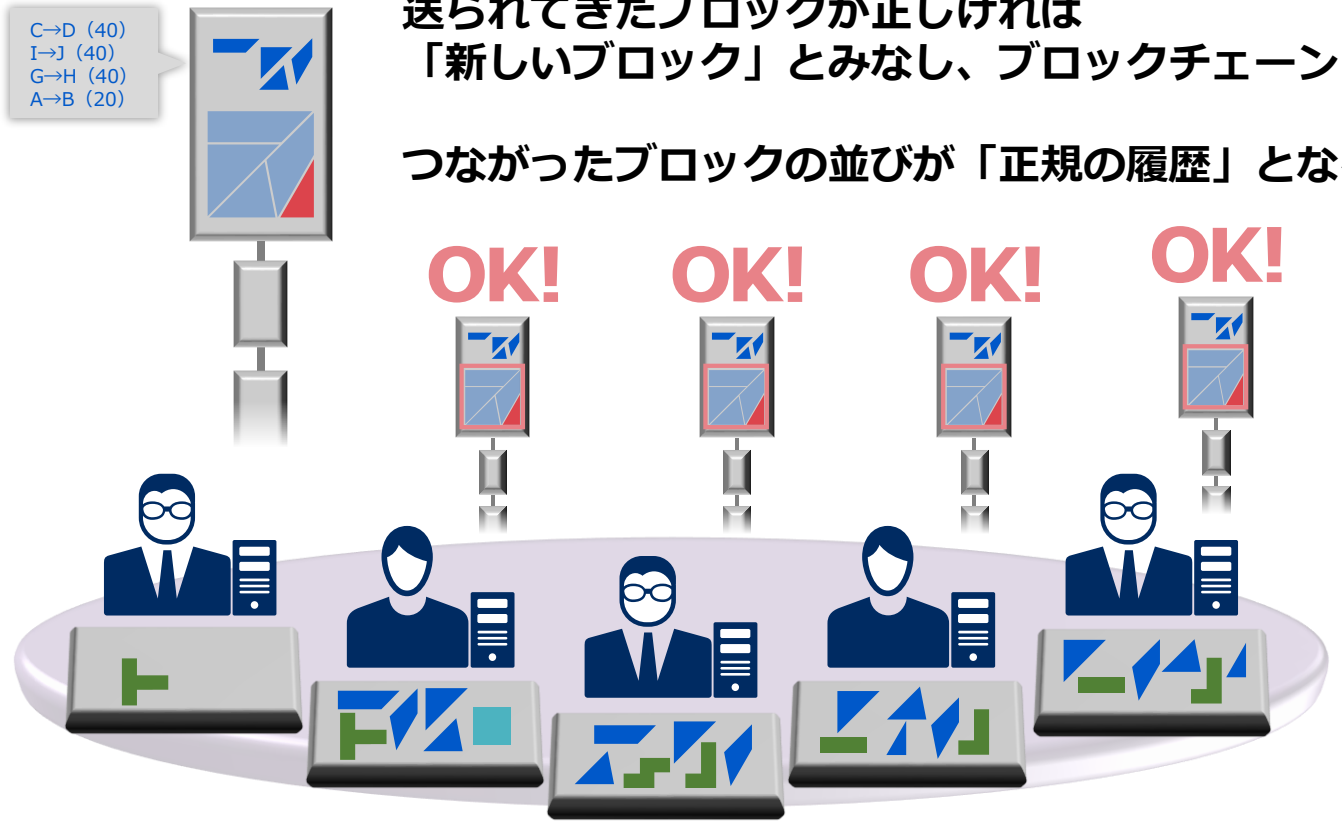
※暗号パズルは、どのユーザーも、手元のデータで必ず解ける。

ブロックチェーン ｜ ブロック候補の同報



暗号パズルが解けたら、
データと暗号パズルの答えとをセットにして
「ブロック」を作り、P2Pネットワークに同報。

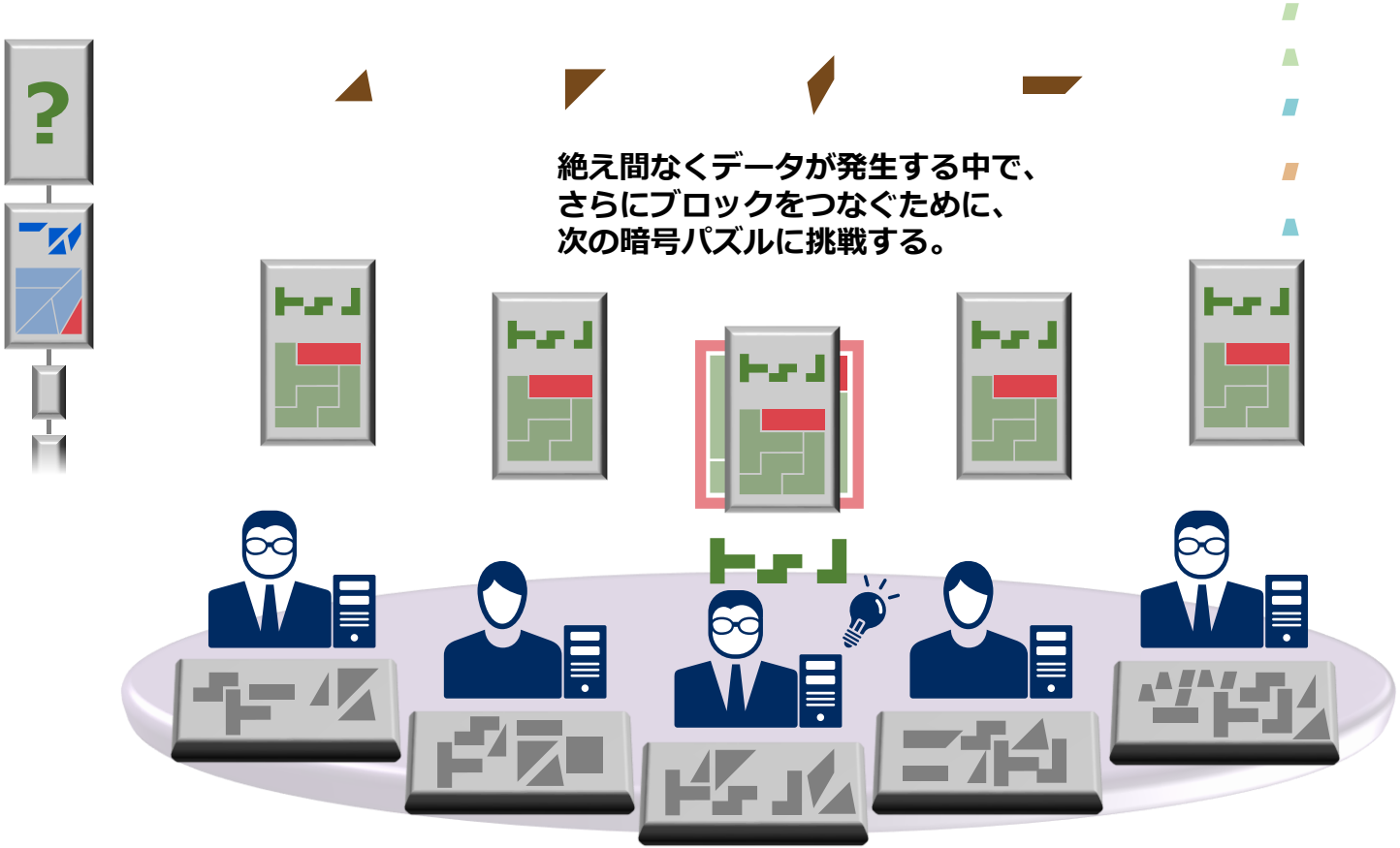
ブロックチェーン ｜ ブロックの承認＝履歴登録



送られてきたブロックが正しければ
「新しいブロック」とみなし、ブロックチェーンにつなぐ。

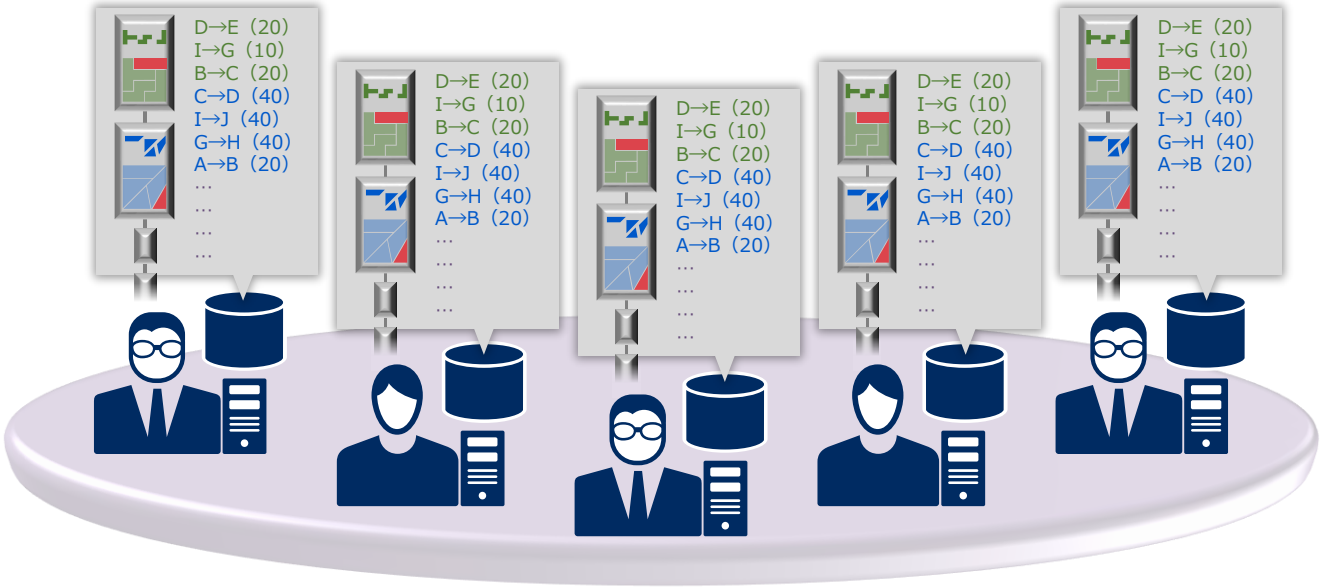
つながったブロックの並びが「正規の履歴」となる。

ブロックチェーン ｜ すぐに次のブロック作りへ

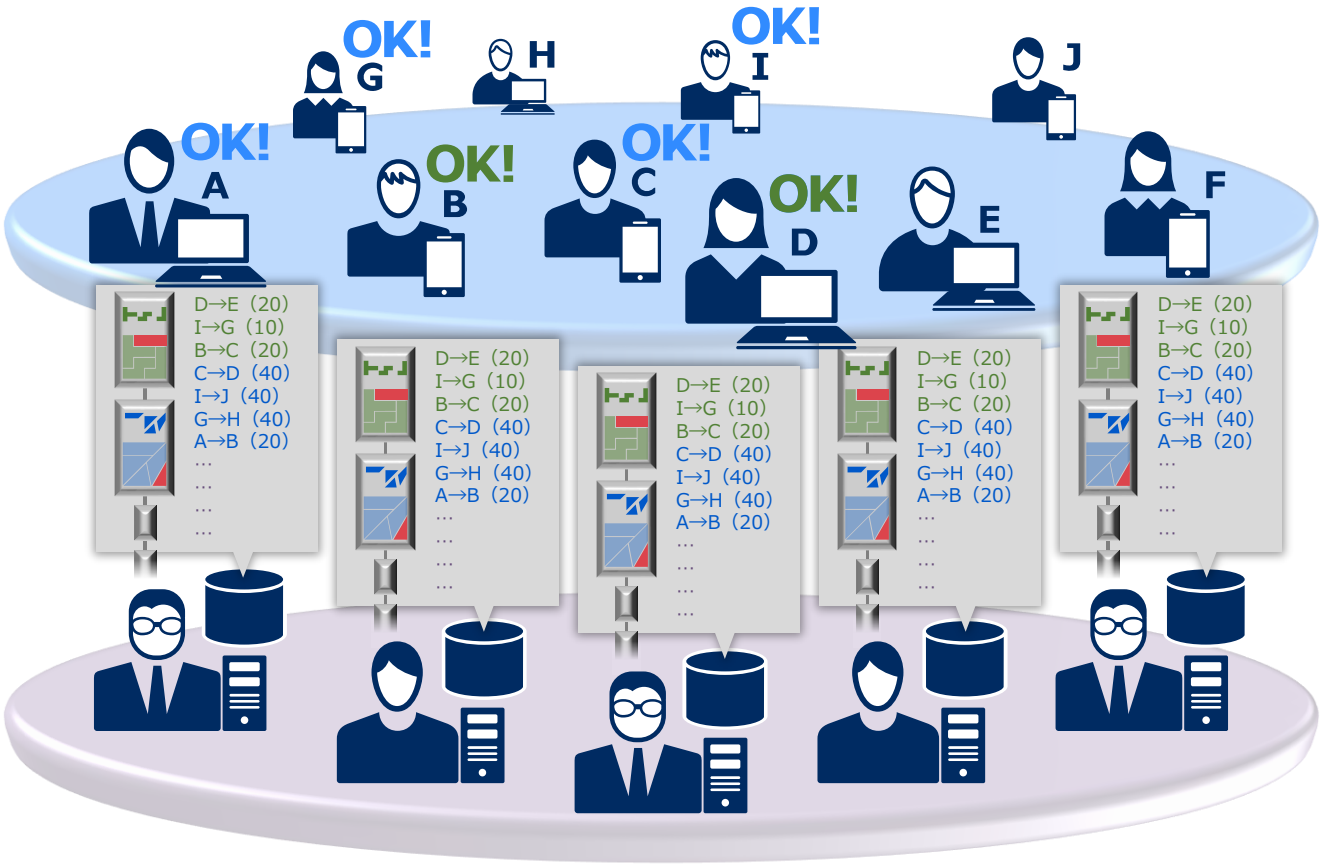


ブロックチェーン ｜ 履歴管理システムのしくみ

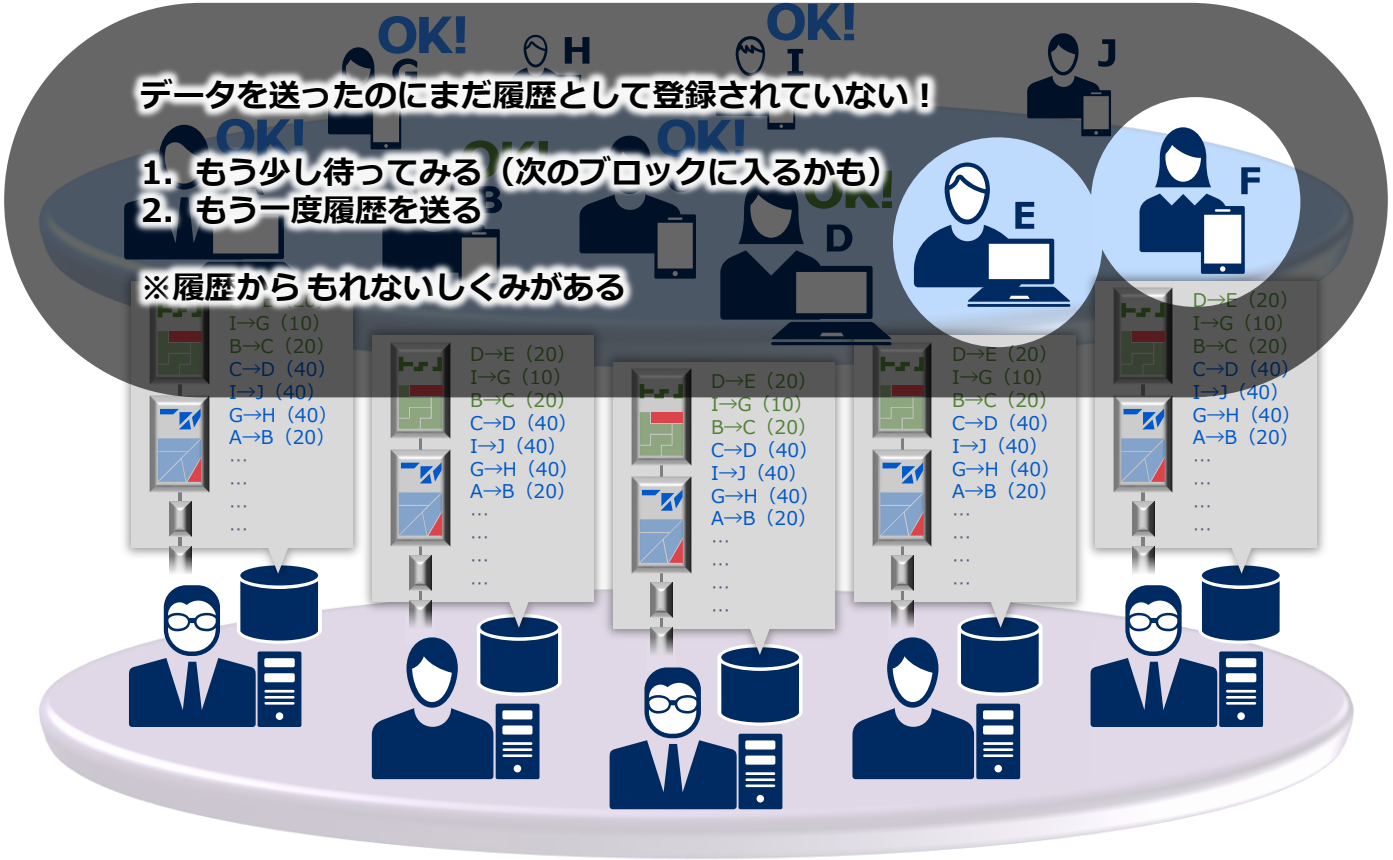
これを繰り返すと、データ管理層の全員が同じ履歴を管理できる。



ブロックチェーン ｜ 履歴管理システムのしくみ

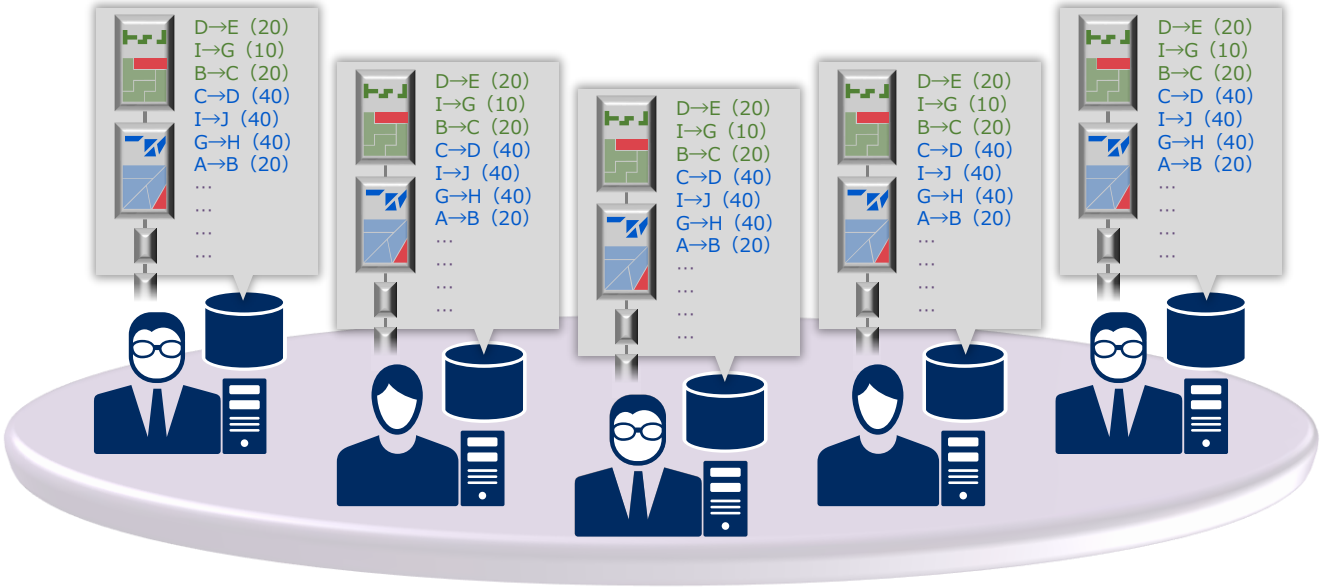


ブロックチェーン ｜ 履歴管理システムのしくみ

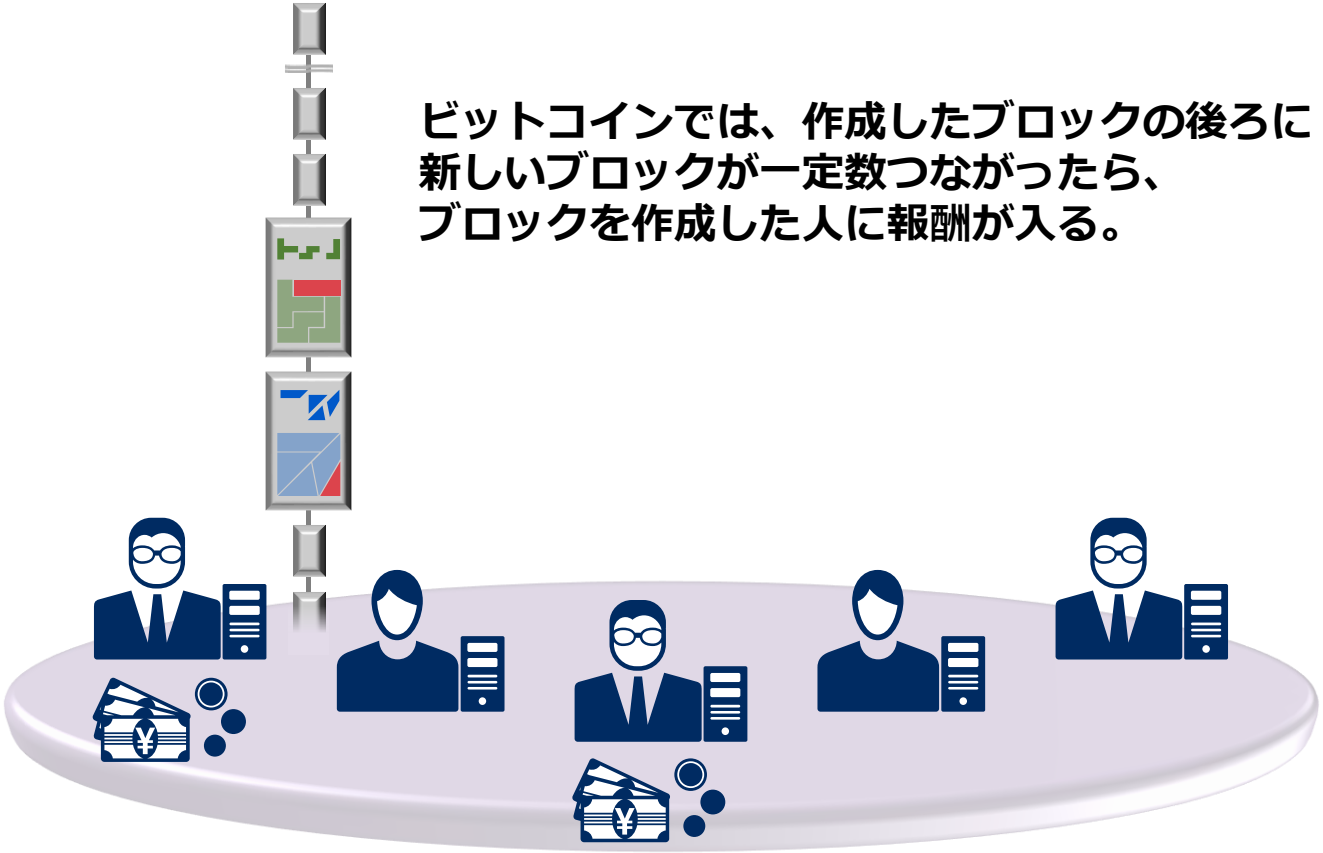


ブロックチェーン ｜ 履歴管理システムのしくみ

どこかに障害が起きても、
ほかが生き残っていれば、情報は消滅しない。



ブロックチェーン ｜ ちなみに…（なぜ暗号パズルを解くか？）

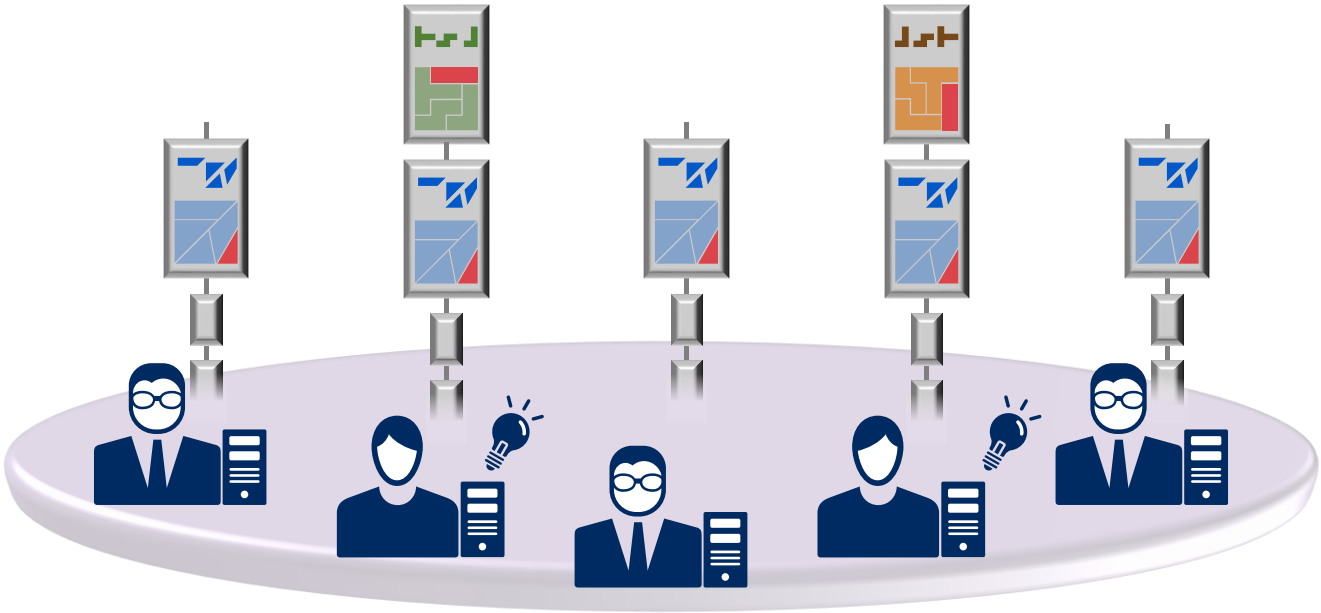


ビットコインでは、作成したブロックの後ろに
新しいブロックが一定数つながったら、
ブロックを作成した人に報酬が入る。

Q. 同時にパズルが解かれた場合はどうなるのか？

早い者勝ち、かつ多数派に収束

パズルの答えは、1つではない。
そのため、2つ以上の答え（ブロックチェーン）がほぼ同時に
P2Pネットワークに送信されることがある。



早い者勝ち、かつ多数派に収束

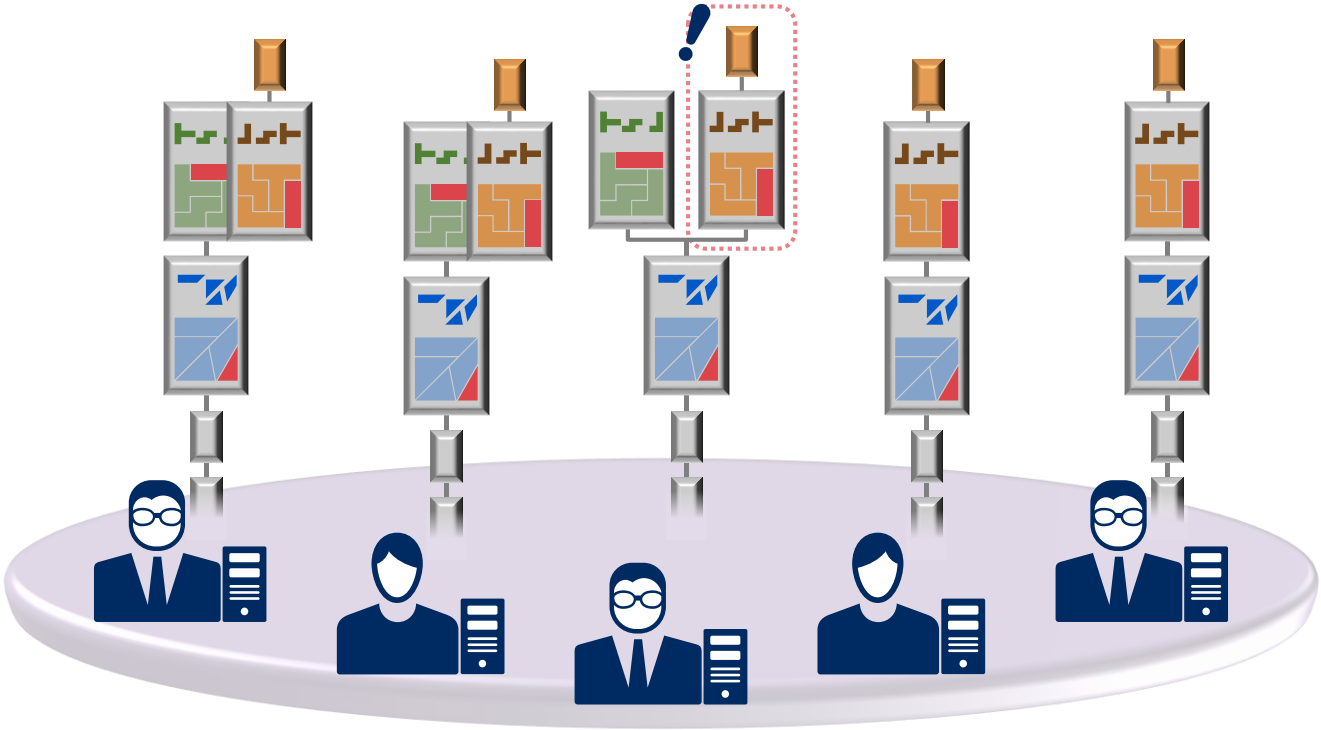
パズルの答えは、1つではない。
そのため、2つ以上の答え（ブロックチェーン）がほぼ同時に
P2Pネットワークに送信されることがある。

早い者勝ち、かつ多数派に収束

先に長くなったほうがメインのブロックチェーンになる。
採用されなかったチェーンは消え、先端につながれていたブロックは未承認となる。

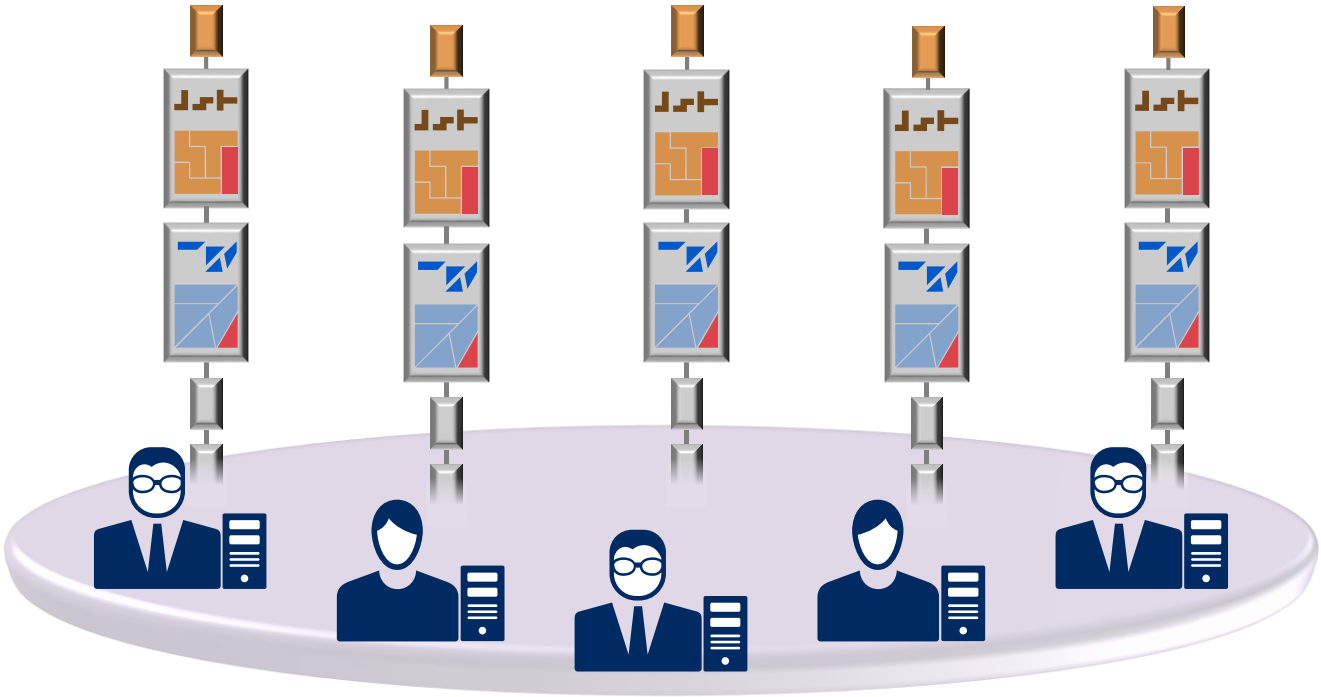
早い者勝ち、かつ多数派に収束

先に長くなったほうがメインのブロックチェーンになる。
採用されなかったチェーンは消え、先端につながれていたブロックは未承認となる。

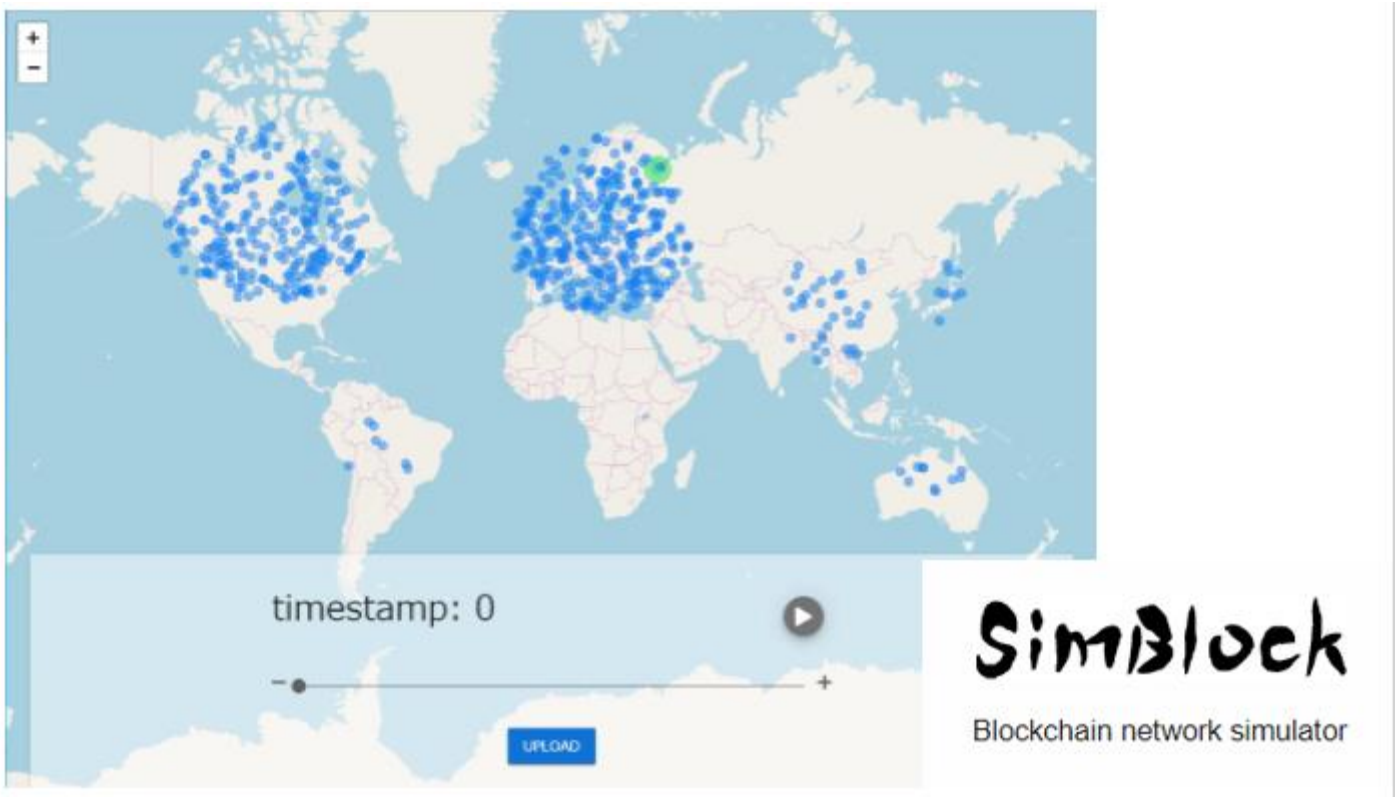


早い者勝ち、かつ多数派に収束

無効になったブロックは、
数ブロック以内にブロックチェーンに取り込まれるので、
取引履歴がなくなることはない。



東工大首藤先生 https://dsg-titech.github.io/simblock-visualizer/

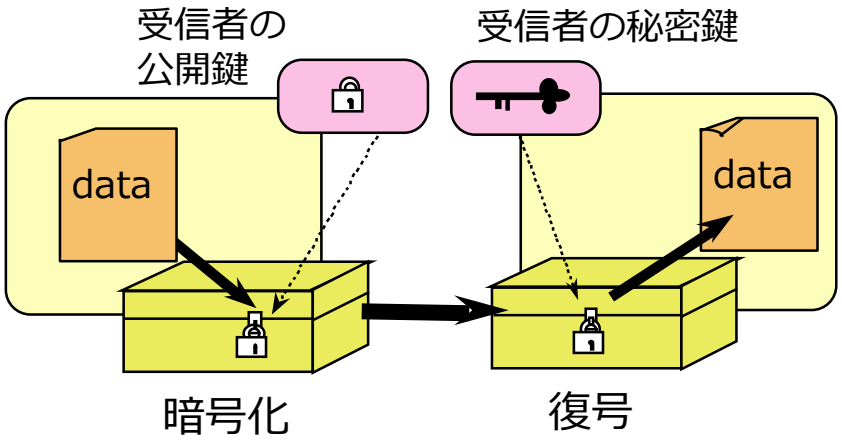


目次

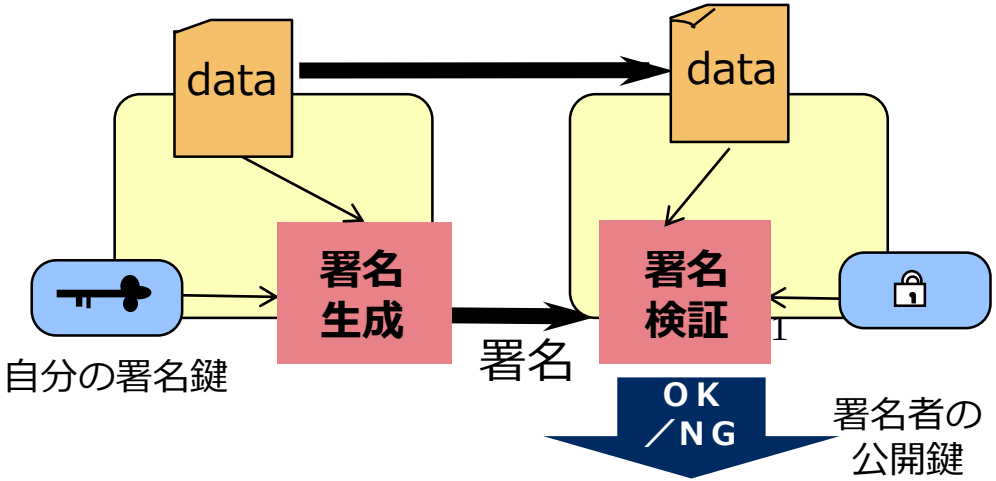
1. 暗号技術について
   公開鍵暗号・デジタル署名
2. ビットコインの動作概要（イメージ）
3. ビットコインにおけるその他の暗号技術
   ハッシュ関数・ハッシュチェーン
4. Q&A

公開鍵暗号とデジタル署名

公開鍵暗号



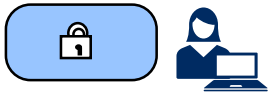
デジタル署名

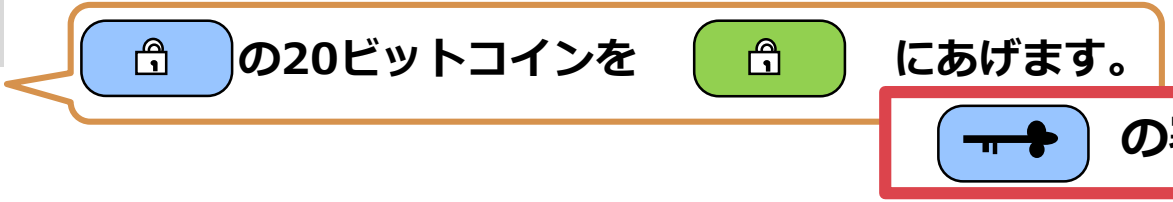


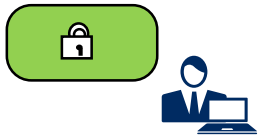
ビットコインとデジタル署名

公開鍵：アドレス

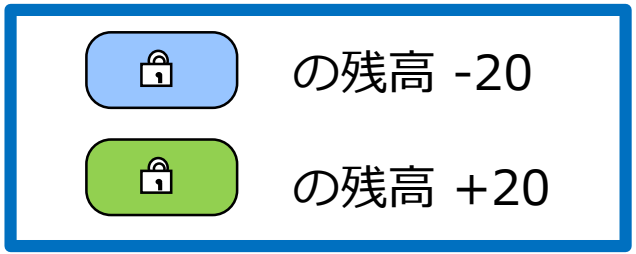
A→B（20）

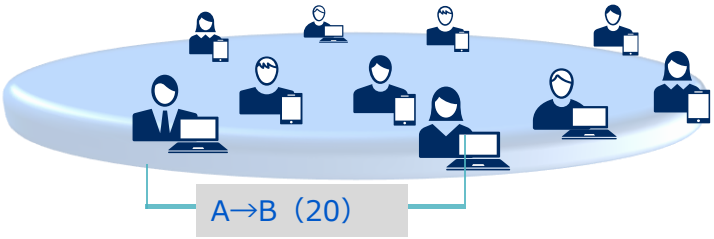




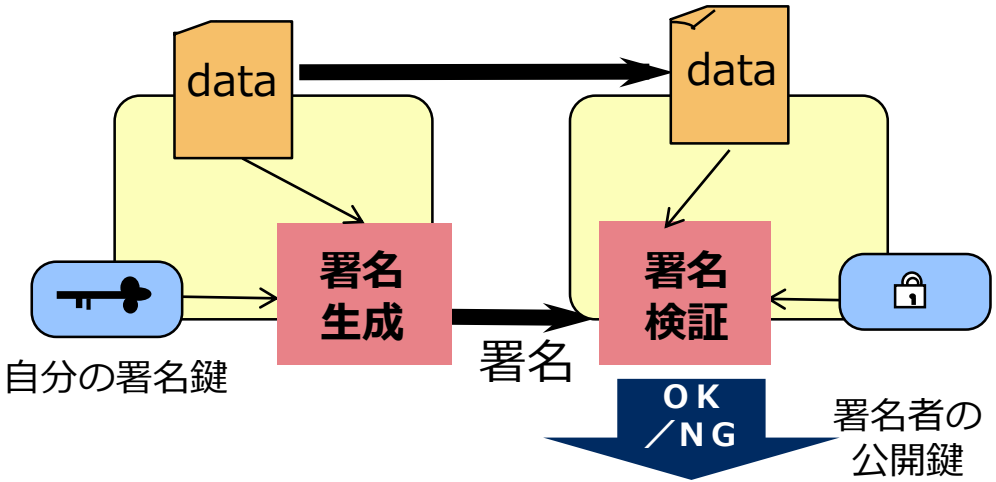


A残高400
B残高　0
C残高 80





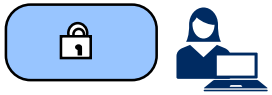
デジタル署名



ビットコインとデジタル署名

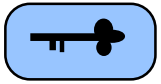
公開鍵：アドレス

A→B（20）



の20ビットコインを

にあげます。

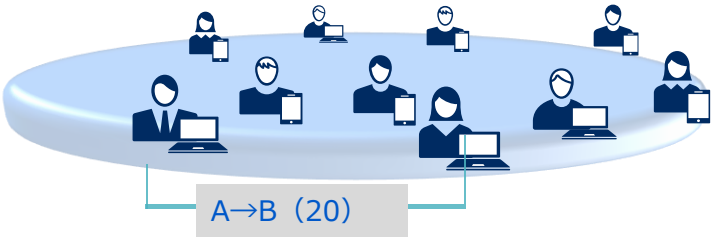


の署名

A残高400
B残高　0
C残高 80

の残高 -20

の残高 +20



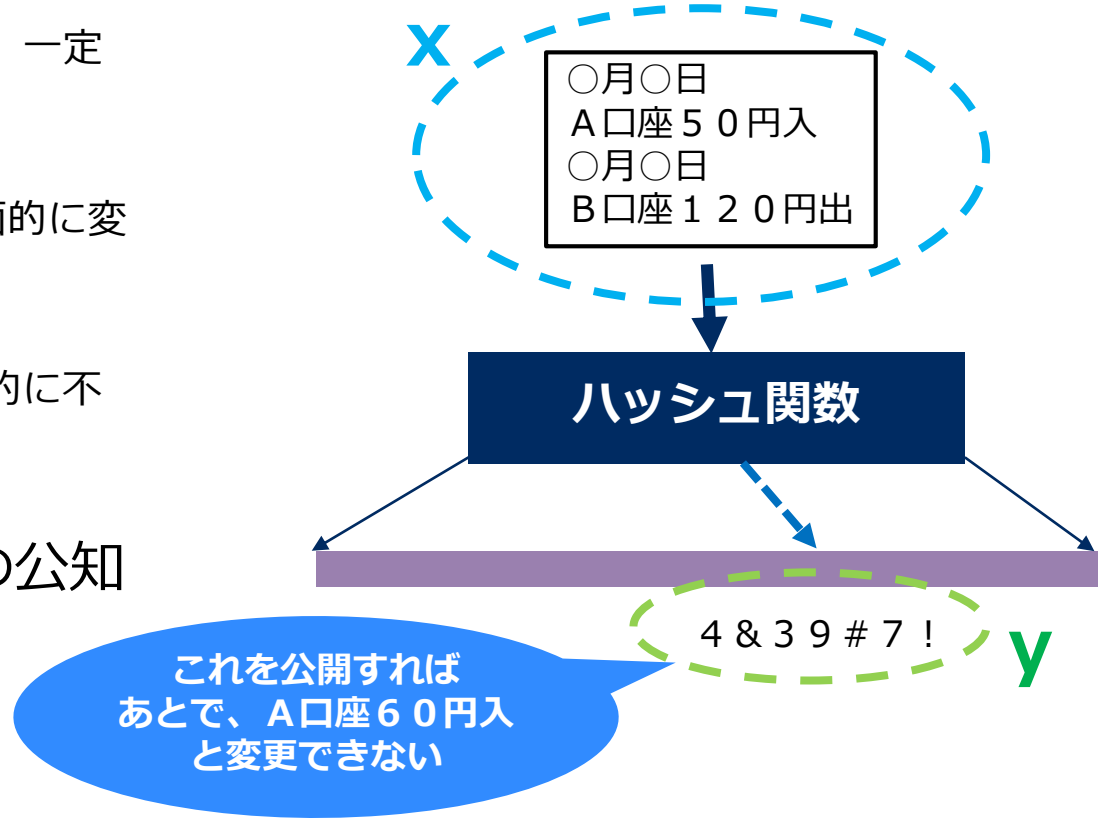
ビットコインというコインがあるわけではない！
ビットコインは単位。

一方向性ハッシュ関数

Hash(x)=y

- 任意の長さの文字列xを入力として、一定長の文字列 y を出力
- y をxの**ハッシュ値**という
- x が１ビットでも変わると y は全面的に変化
- 出力y から入力x は推測できない
- 同じ出力になる2入力の探索は現実的に不可能

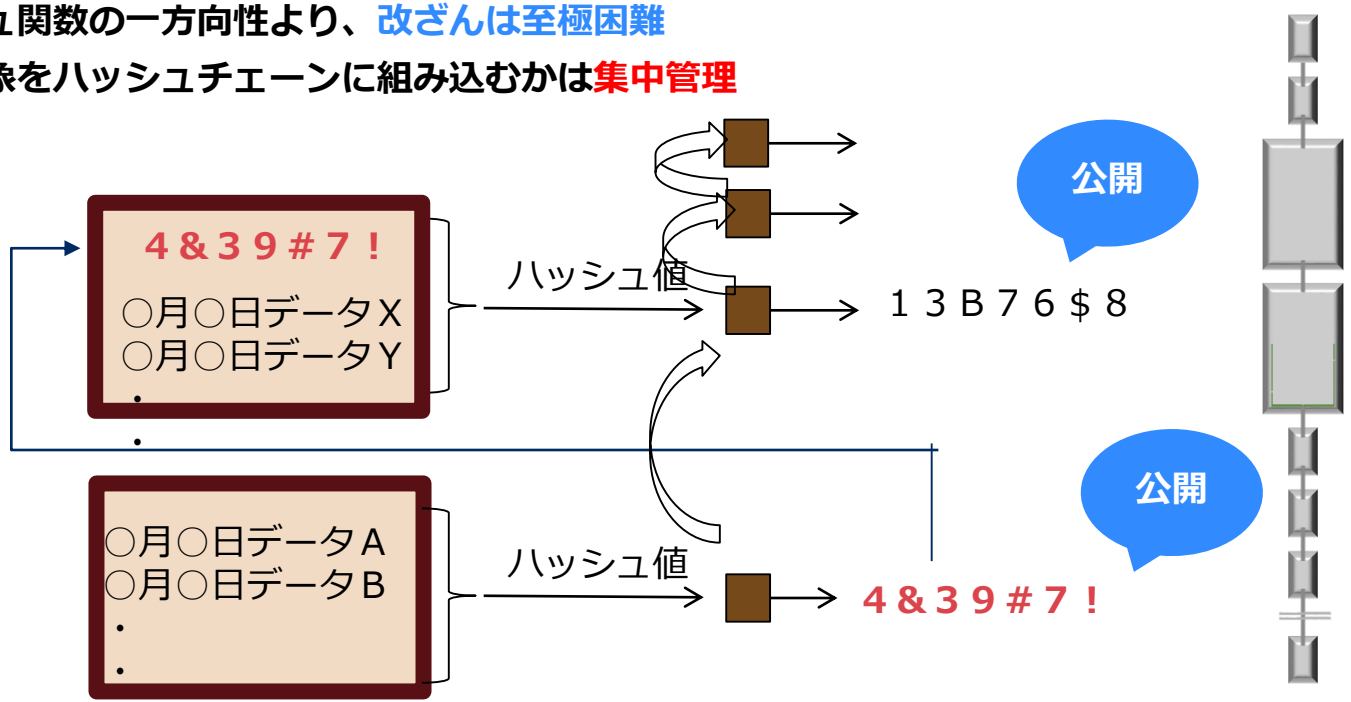
SHA-256, RIPE-MDなどの公知アルゴリズムで実績。



既存技術：ハッシュチェーン（タイムスタンプ技術）

あるデータが特定の時点までに存在したことを保証する技術

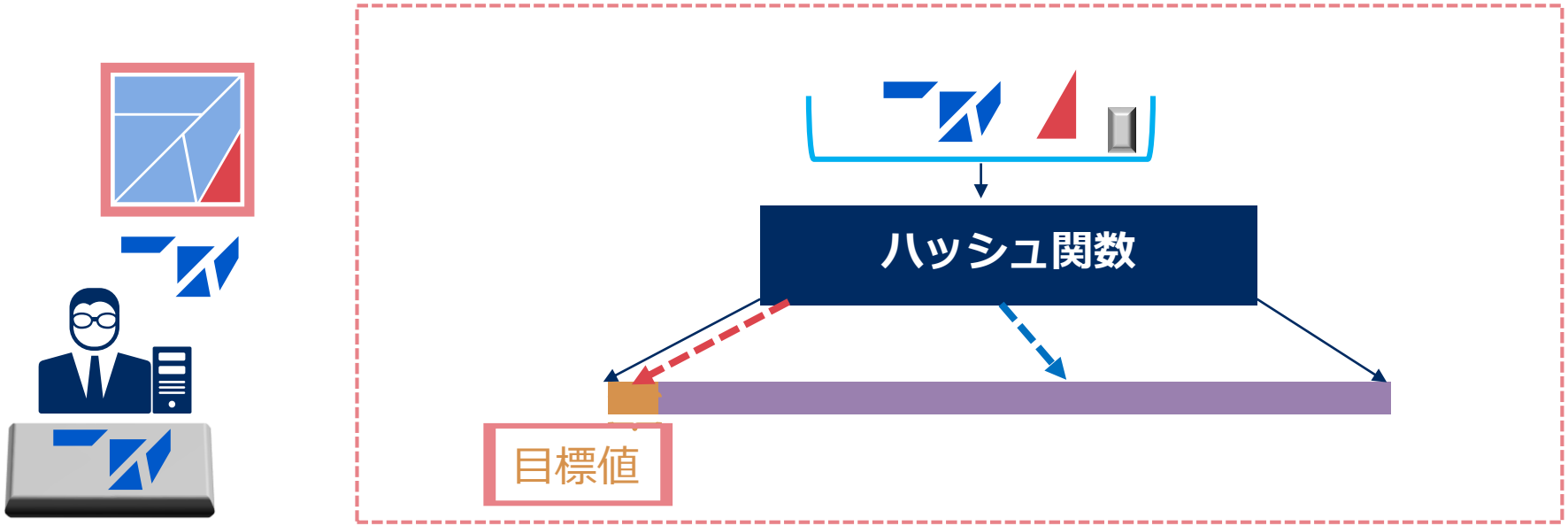
- **ハッシュ値を連鎖的に公開することで、莫大な数のデータの存在を簡単に証明可能（ハッシュチェーン）**
  - **公開手段の例：Financial Times誌**
- **ハッシュ関数の一方向性より、改ざんは至極困難**
- **どの事象をハッシュチェーンに組み込むかは集中管理**



チェーンを同期させるための暗号パズル

データや順番を同期させる時間稼ぎために、早い者勝ちの暗号パズルを解く。（マイニング）

※暗号パズルは、どのユーザーも、手元のデータで必ず解ける。



目次

1. 暗号技術について
   公開鍵暗号・デジタル署名
2. ビットコインの動作概要（イメージ）
3. ビットコインにおけるその他の暗号技術
   ハッシュ関数・ハッシュチェーン
4. Q&A


Orchestrating a brighter world
NEC