

ブロックチェーンの仕組み

疑問：技術的な仕組みはどうなっているの？

どうやって、ブロックチェーンは「信頼できる第三者を
必要としない」オンライン送金を実現できたのか？

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.



ブロックチェーンを理解する上で必要な知識

ハッシュ値：ハッシュ関数から出力された値

30382283da9836e16279dcb833e4aab4bdf6d86e9a3e6b502cf711d04029fd7

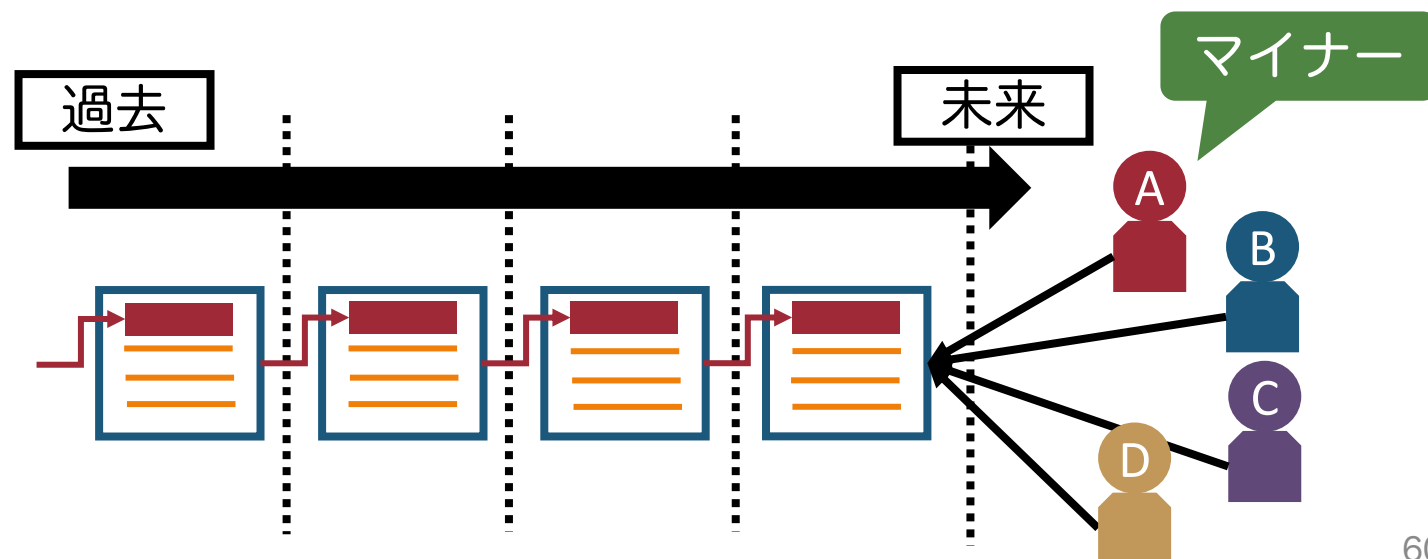
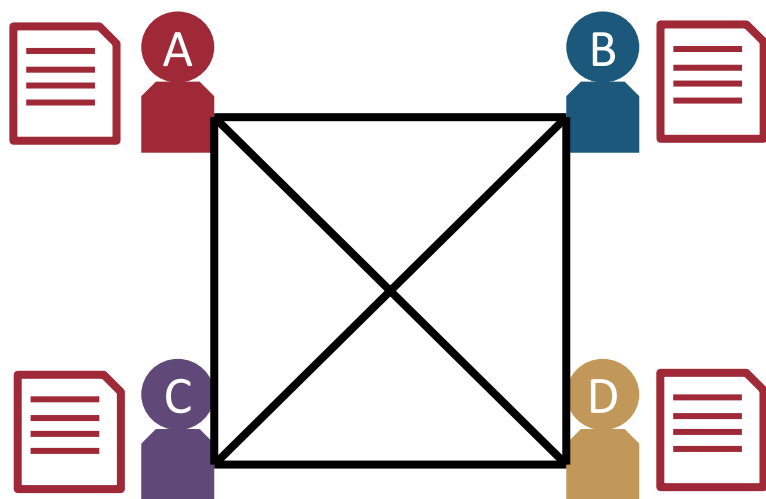
入力値を改ざんした場合、
出力値が変わるので改ざん
検知に使われる



- 特徴1: ハッシュ関数から出力されたハッシュ値は、入力値によって一意に決まる。
- 特徴2: ハッシュ値から、元の入力値を推測することはできない（不可逆変換）。

ブロックチェーンの仕組みざっくり解説編

- 分散台帳技術
 - みんなで、取引の正当性を検証できるようにしましょう
- ブロックとチェーン（改ざん耐性）
 - 一定期間の取引記録をブロックにまとめましょう
 - ブロック同士をハッシュ値を使ったチェーンでつなぎましょう
- 合意形成（コンセンサスアルゴリズム）
 - ブロックの正当性を保証するために、ブロックはみんなの合意の下で作成しましょう



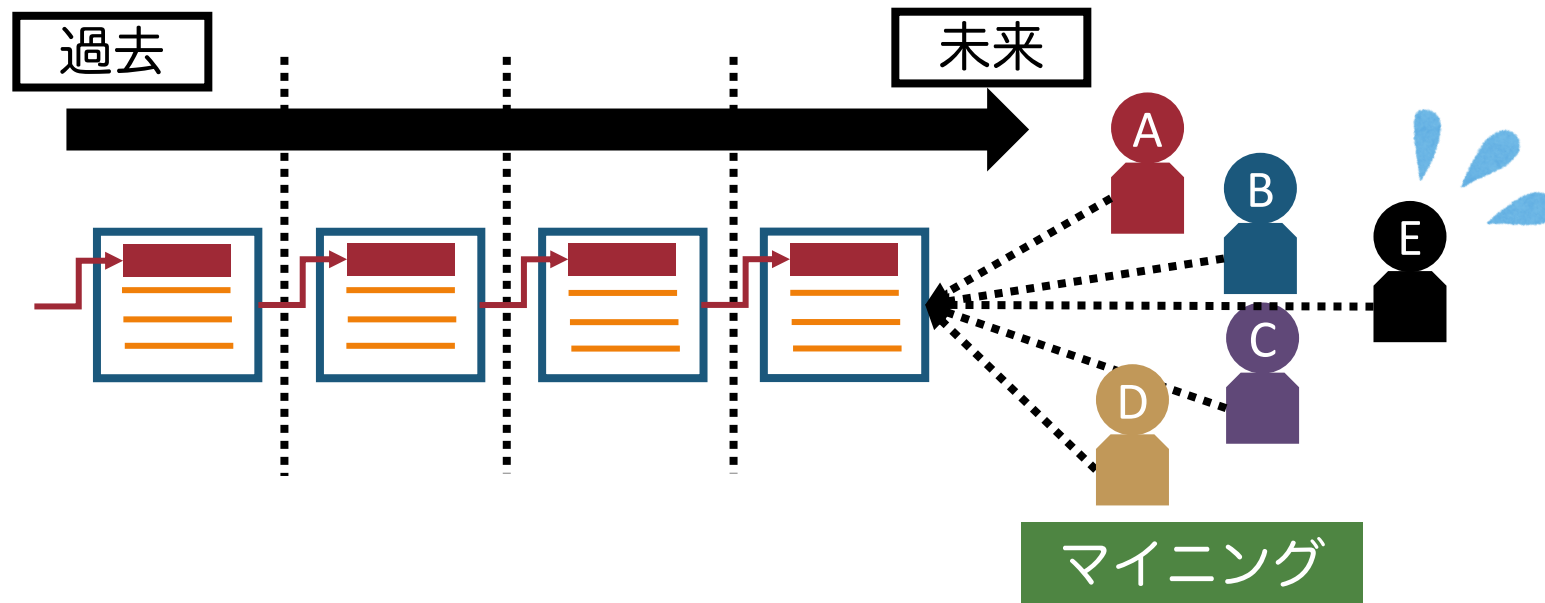
非中央集権型での合意形成

分散したノードの環境下で、ノード同士の合意を取るのは難しい（ビザンチン将軍問題）

-> みんなが納得のいく合意を取る必要がある

- **Proof-of-work**（ビットコインの合意形成で利用されている方法）：

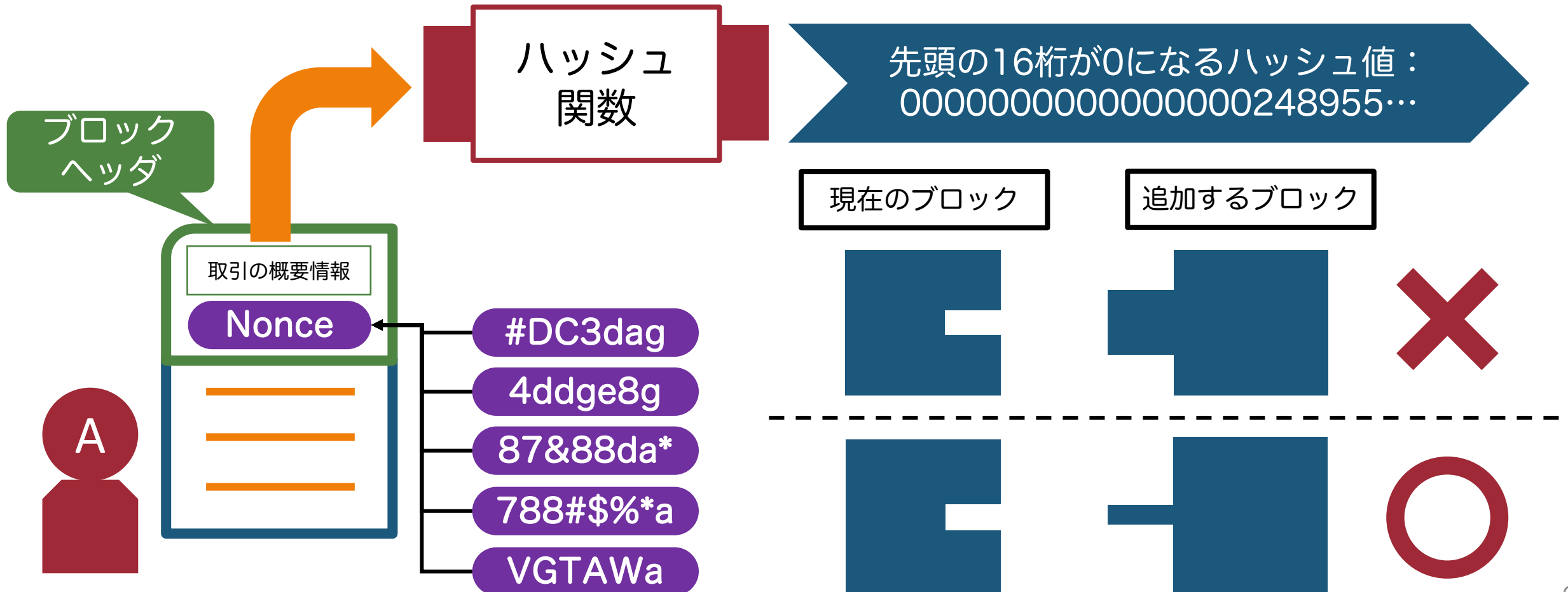
計算処理能力が必要な計算を解く「競争」をさせて、勝者にインセンティブ（新規ビットコインとその期間の取引手数料の総額）を与えることで不正が起きないようにする。



どんな競争をするの？（ブロックをつなぐための競争）

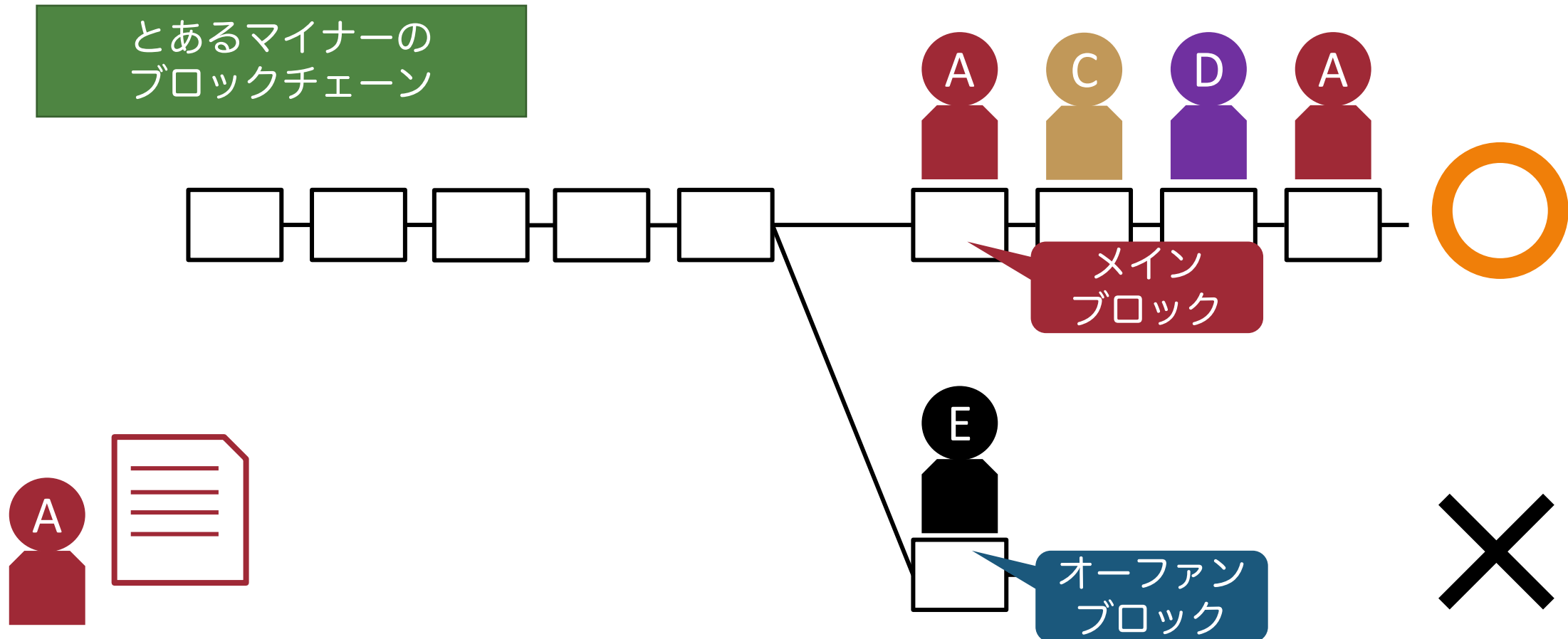
ある値よりも小さくなるハッシュ値の入力値を探す（ブロックがつながる条件）

（ハッシュ値って不可逆変換で元の値がわからないんじゃないかなかったですかね？）



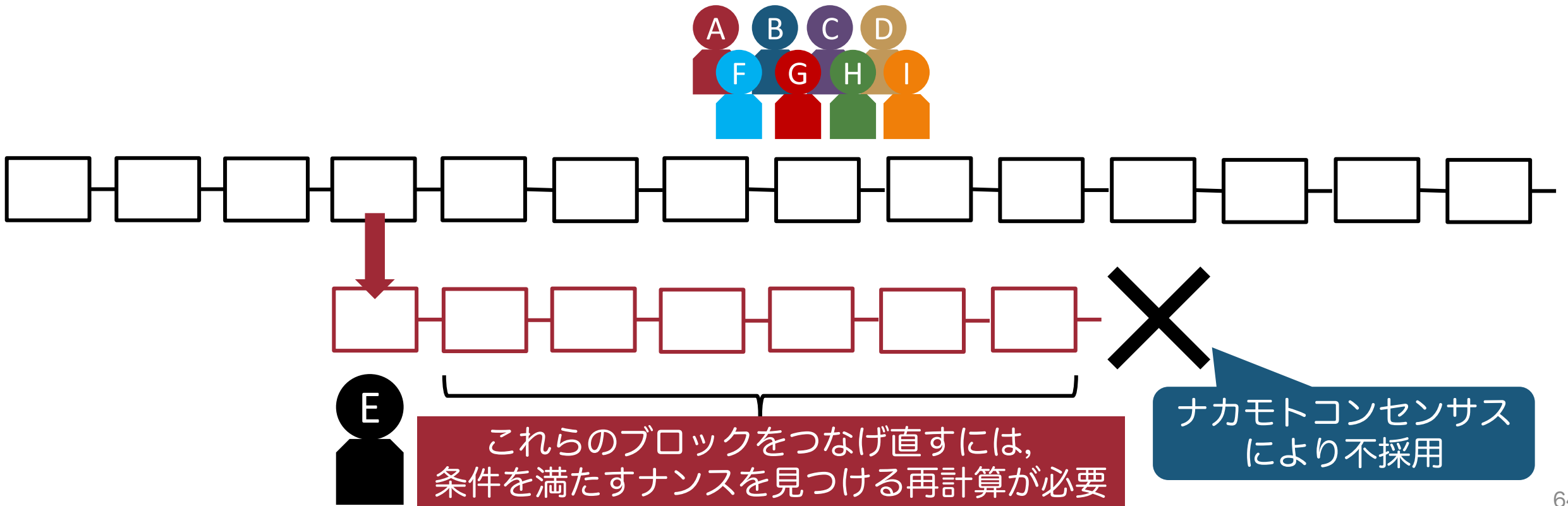
ナカモトコンセンサス

ブロックチェーンの分岐した場合，ある程度長くなった方のブロックを採用する
(インセンティブは，ある程度ブロックが繋がってからもらえるようになっている)



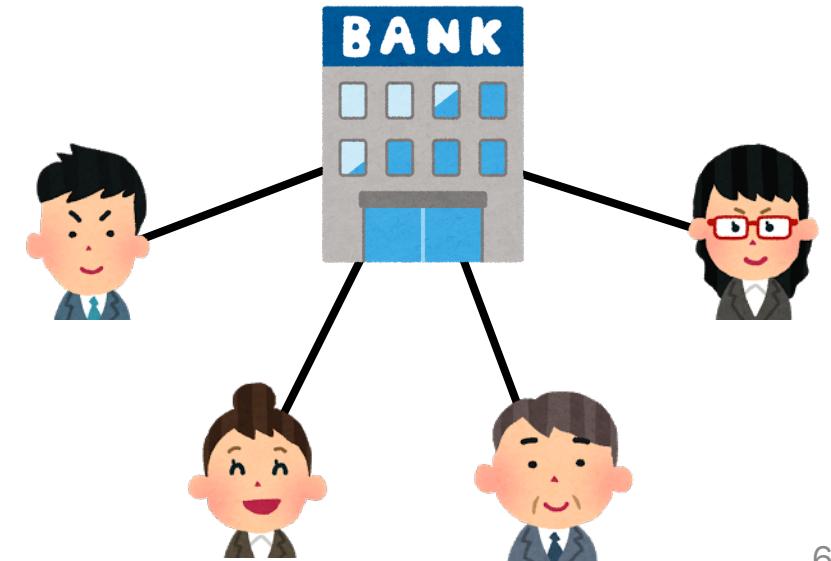
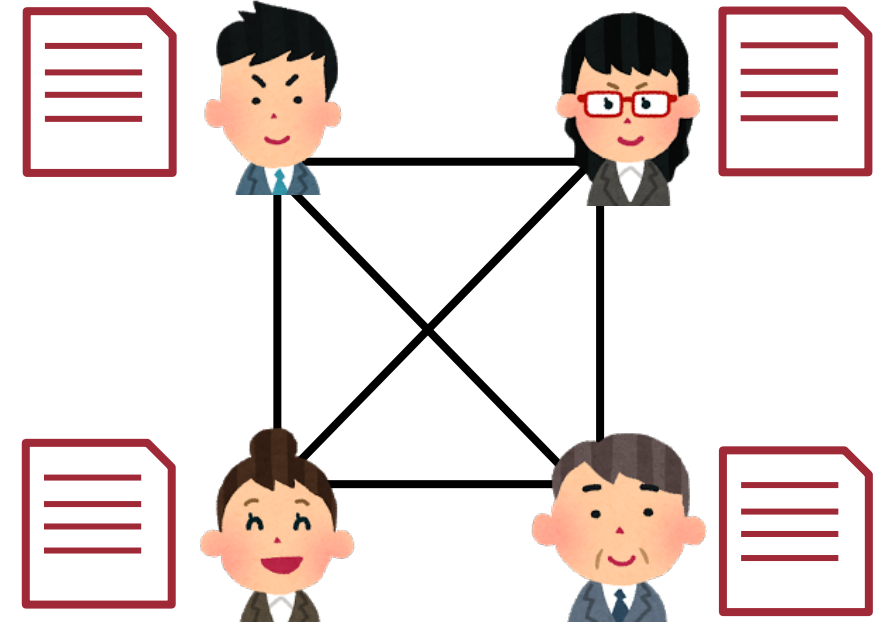
過去の取引の改ざんは困難

過去の取引を改ざんするとそれ以降のブロックも修正する必要がある（ハッシュ値のチェーン）。
それ以降のブロックを作るということは、世界中の人が、計算力をかけて作ったブロックを自分でもう一度作り直すということ。



ブロックチェーンが実現した技術的利点

- 信頼性を担保した当事者間の直接取引
 - P2Pの弱点の克服
- 単一障害点問題の解消（CIAのA）
- データの改ざん耐性
- データの効率的な共有
 - 他人の取引データも共有
- 透明性（全ての取引データが閲覧可能）
- 公平性（みんなが平等）
 - 誰か1人がデータを掌握して、データの改ざんやコントロールとかできない



課題3

- ブロックチェーン技術の**問題点**について調べてみてください。
ださい。
- キーワード：
 - ブロックチェーン 役に立たない
 - ブロックチェーン デメリット
 - ブロックチェーン 課題

