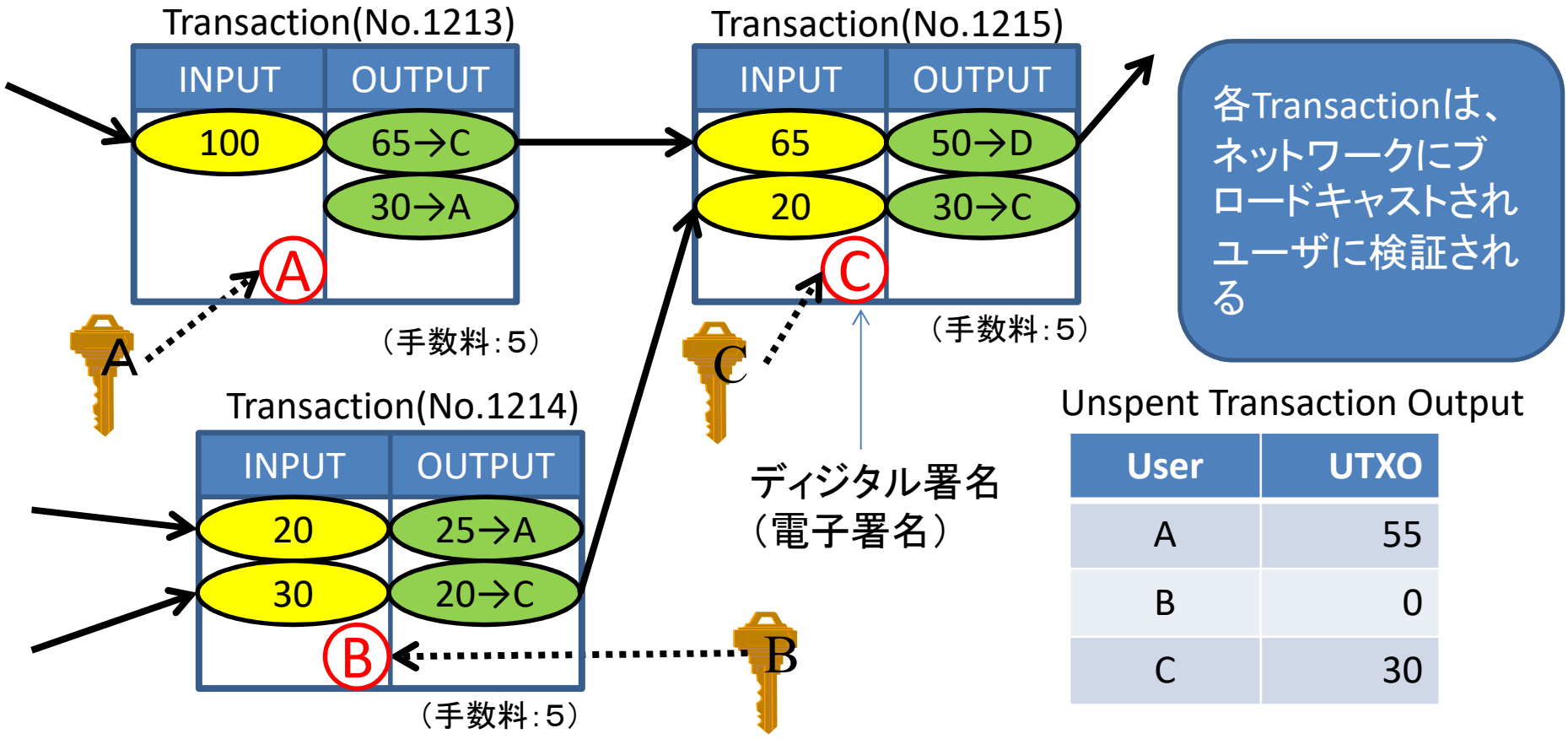
BitCoinのしくみ

BitCoinとは

- Satoshi Nakamoto（を名乗る人物）により2009年に提案、運用されるようになった仮想通貨システム
- BitCoinのやり取り（Transaction）は全てP2Pネットワークで公開され管理される
- 特別な管理主体（銀行等）は存在せず、取引の承認は、マイナー（採掘者）と呼ばれる利用者が行う
- Proof-of-Workと呼ばれる問題を最初に解いたマイナーが取引承認を行うことができ、その際に報酬としてBitCoinを得ることができる
- Proof-of-Workは計算速度の上昇に応じて難易度が自動調整される

取引履歴(Transactions)

- 「Coin」そのものを表す電子データはない
- BitCoinでは取引（Transaction）の履歴で価値(Coin)を表す

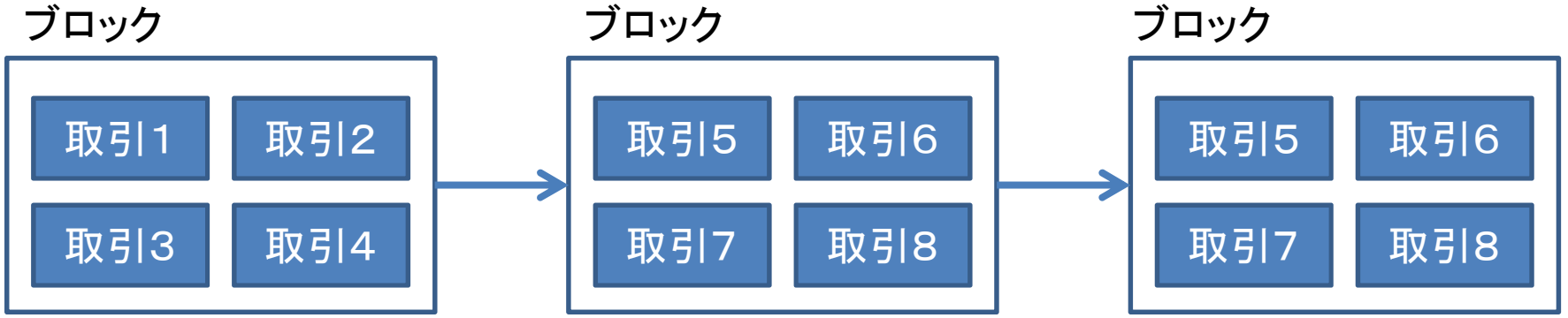


Unspent Transaction Output

User	UTXO
A	55
B	0
C	30

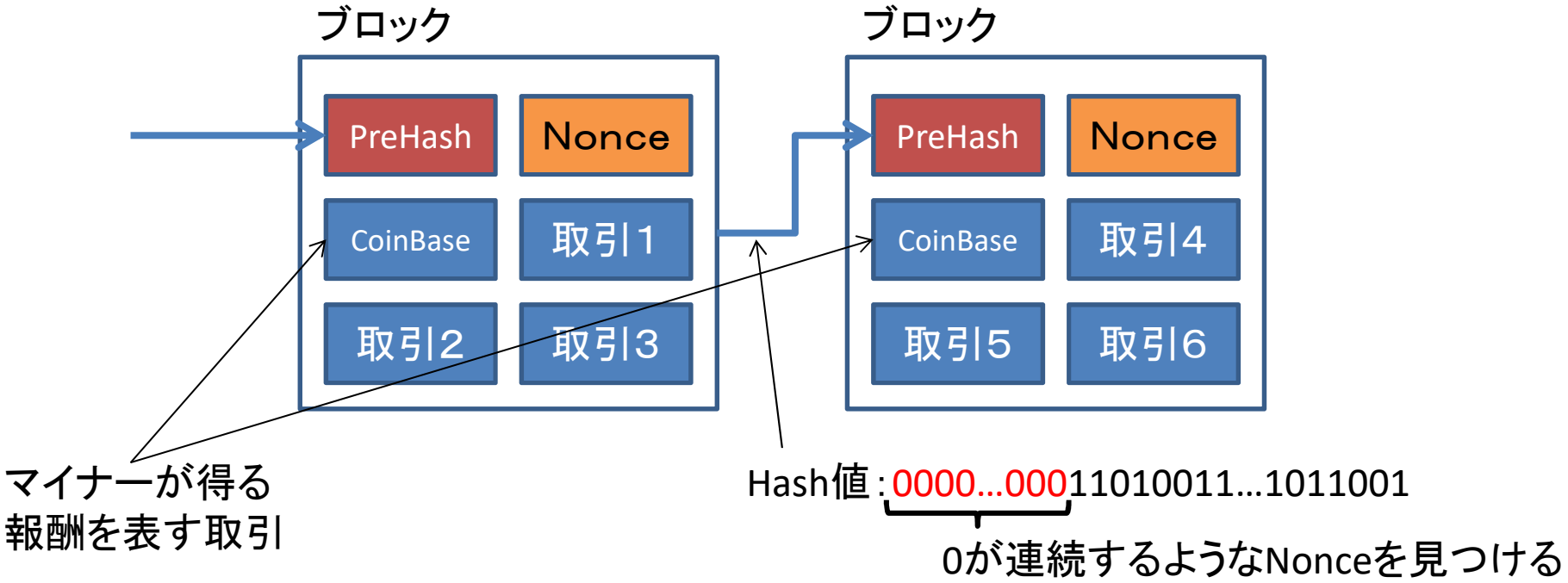
ブロックチェーンとP2Pネットワーク

- 全ての取引履歴はP2Pネットワークで公開、全ユーザで共有される
- 複数の取引履歴が一つのブロックにまとめられる
- 新しいブロックは以前のブロックの末尾に連結される→ブロックチェーン
- 誰がブロックの連結作業を行うか？

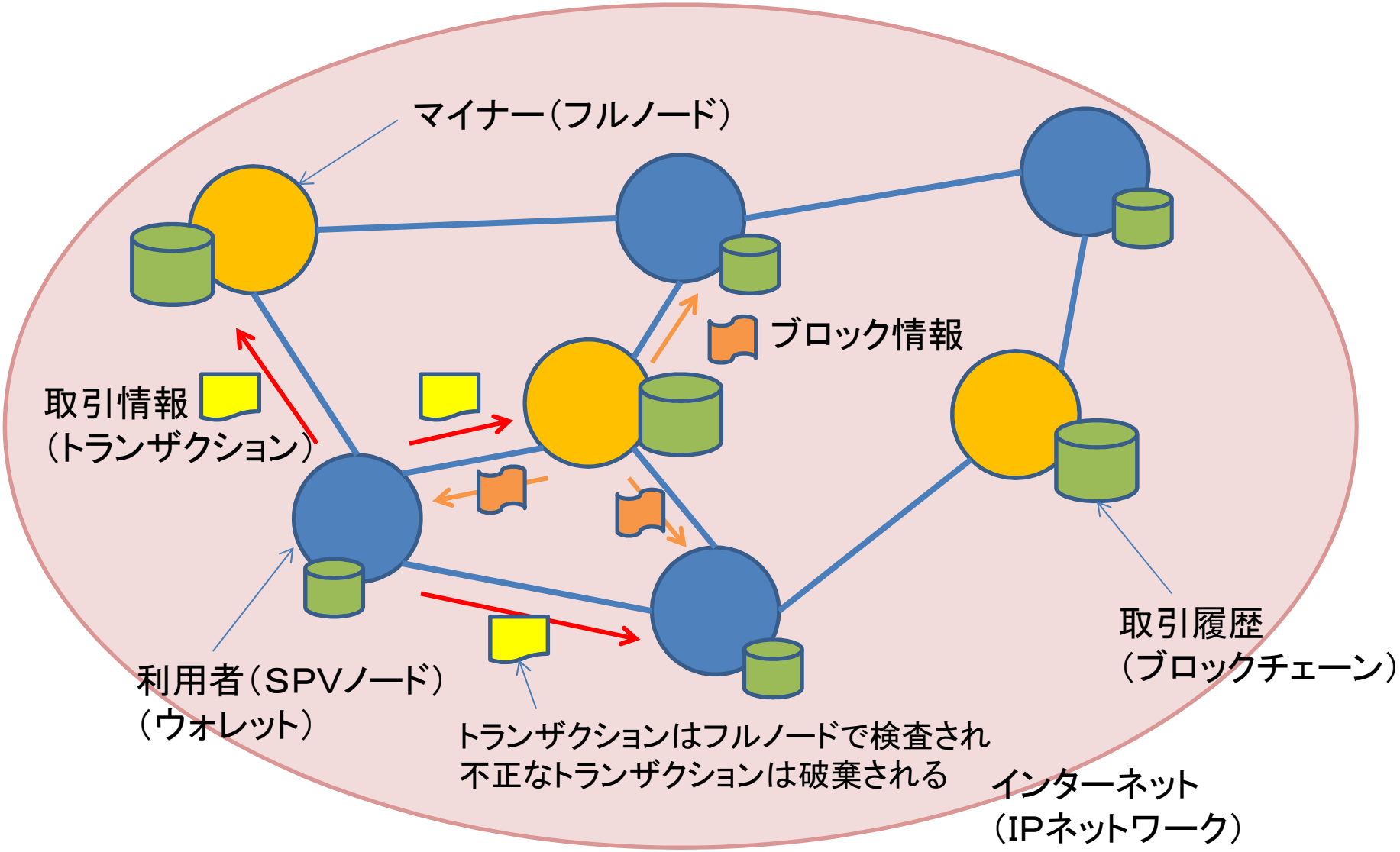


Proof-of-Work

- ブロックのハッシュ値があらかじめ定められた値以下になるNonce値を最初に見つけたマイナーがブロックを接続できる（Proof-of-Workの難しさは探索時間が一定になるよう自動調整される）
- 成功したマイナーは報酬と手数料を得ることができる（報酬分のBitCoinが自らに振り込まれる特殊な取引をブロックに入れる）←新たな貨幣供給になっている

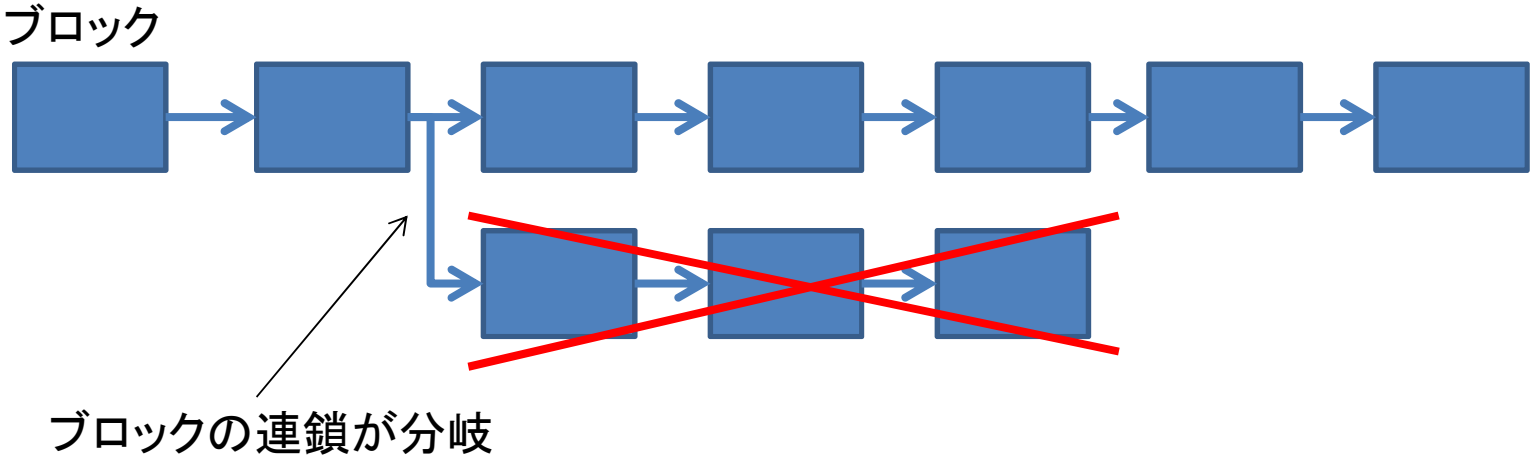


Bitcoinネットワーク



ブロックチェーン

- ネットワーク遅延や不正行為によりブロックチェーンの分岐が起こる
- ブロックの連鎖（Chain）が分岐した場合、最も長い連鎖が有効←計算量による多数決
- 既存の連鎖を無効にしようとする攻撃者はそれを上回る計算速度が必要（連鎖が長くなると指数関数的に困難になる）
- 一般的に、確認数（後続するブロック数）6程度で確定とされる



ブロックチェーンの分類

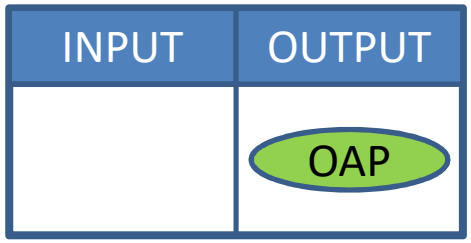
	一般参加者 （閲覧のみ）	管理者	コンセンサス	承認速度
パブリック型	不特定多数	なし （参加者）	PoW, PoS等	低速
コンソーシアム型	特定複数 （要許可／ 自由参加）	複数	参加組織間の 合意	高速
プライベート型	特定複数	単独	不要	高速

ブロックチェーンの応用

- CryptoKitties: ネコの育成ゲーム。ブロックチェーン上のトークンとして実装されているので実際の猫と同様に交換や交配ができる
- Everledger: ダイヤモンドや美術品等の高額資産を管理する電子台帳システム
- PowerLedger: 電力を仲介者なしに直接取引可能にするP2P型取引基盤システム
- ラーメン選手権の人気投票：北九州ラーメン王座選手権での実証実験
- ディジタルコンテンツの転々流通システムの検討：ディジタルコンテンツの譲り合い、貸し本サービス
- 公共WiFi認証システムの検討：利用者認証と匿名性の両立、地域活性化支援

Open Assets Protocol

- ブロックチェーンの性質を生かして、仮想通貨以外の様々な応用が考えられている(Bitcoin 2.0)→実現手法の一つ
- 有価証券の取引、不動産登記簿、各種ポイント、等



•Outputに特殊なマーカー(OAP)があるとアセットを扱うTransactionとみなされる
•最初にアセットが発行されたときAsset IDが一意に決まる
•Bitcoinのスクリプトを利用して様々なサービスが実現可能

→ビットコインスクリプトは簡易なスタック型言語でありチューリング完全でない

Ethereumとスマートコントラクト

- 2013年にEthereum FoundationでVitalik Buterinを中心にはじめられた
- ブロックチェーン上で様々なアプリケーションを実行するためのプラットフォームとしての位置付け（ワールドコンピュータ）
- Ethereumの内部通貨Etherは、トランザクション（プログラム実行）手数料Gasとしても使われる
- Ethereumのプログラム（スマートコントラクト）を記述する言語は、チューリング完全
- Solidityと呼ばれるJavaScriptライクなプログラミング言語で開発できる

BitCoinの特徴

- 独立性（物理媒体に依存しない）→〇
- 安全性（偽造、二重使用）→〇
  ただし、取引の承認までの待ち時間が必要
- プライバシー（匿名性）→〇
  匿名での追跡は可能
  ただし、違法取引等への対策はない
- オフライン支払い→×
- 移転性（他人への支払い）→〇
- 分割可能性→〇

BitCoinの問題点

- 価値（既存通貨との交換レート）の変動が激しい
  →既存通貨も変動するがBitCoinは国の介入等ができない
- マネーロンダリングや違法取引などに利用される
  →ID（公開鍵）で追跡はできるが、そのIDが誰かはわからない
- 処理速度(Transaction Rate)が遅い
- ファイナリティ（決済完了性）の問題
- 原理的に総発行量に上限がある
- オフラインでは使えない
- マイナーの寡占化が進んでいる
- 環境への悪影響