仮想通貨の
ブロックチェイン技術による
FinTech

近畿大学　山崎重一郎

FinTechの本命は

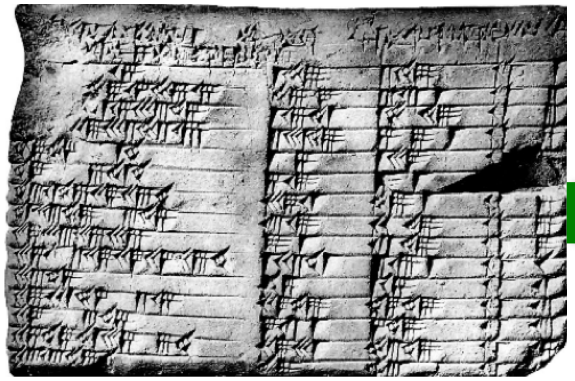
信頼できる記録を管理する技術

古代バビロニアのFinTech

信頼できる取引記録

法＝コードによる統治

確認



焼き固め

アーカイブ

信頼できる取引記録

ハムラビ王時代のバビロニア

- 法治国家＝「コード」による統治
- 鋳造貨幣（トークン）は存在していない

TELEX

AD1930年~2000年

電気通信技術によるFinTech

全銀ネット

日銀ネット

SWIFT

（国際銀行間通信）

銀行振込による決済はいつの時点で完了？

（1）送金者が振り込みをした時点

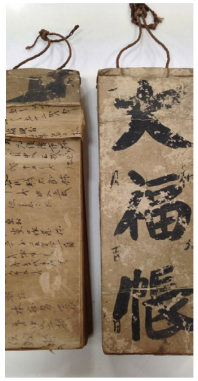
（2）受領者が入金を確認した時点

法的に正しいのは（1）

理由：銀行の送金記録は信用できる
（というルールになっているから）

取引記録管理技術の歴史

粘土板

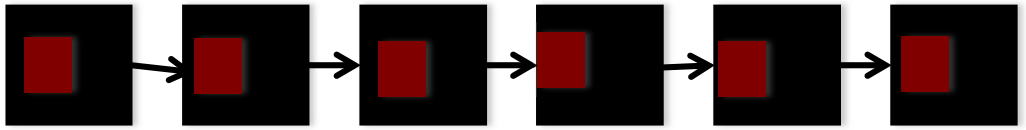


紙の帳簿

TELEX

コンピュータ
ネットワーク

ブロックチェイン

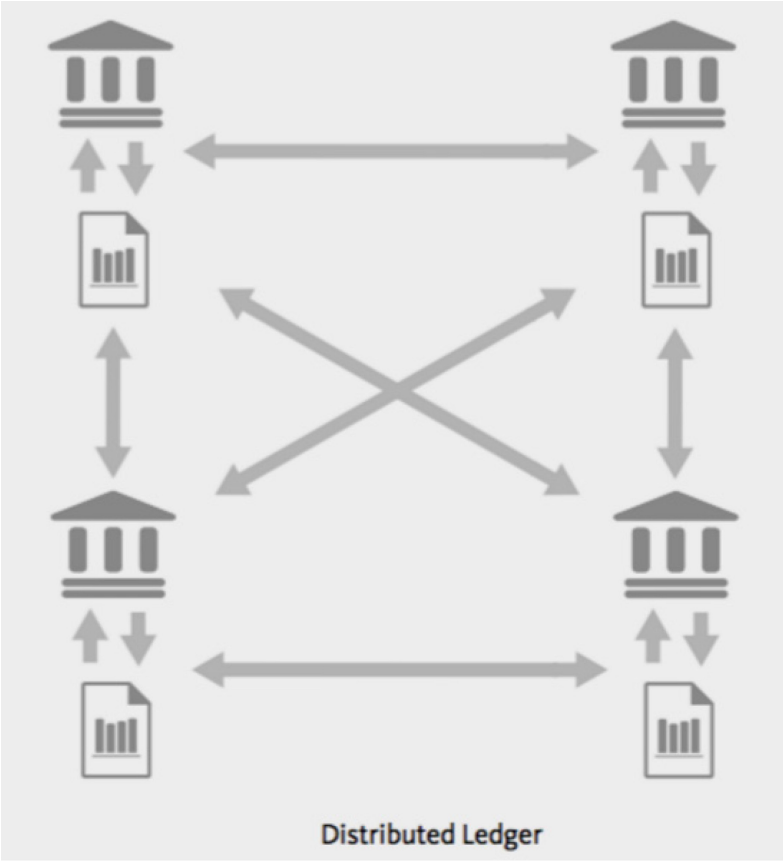


R3: メガバンクコンソーシアム

ブロックチェインの共同利用構想

- Bank of America,
- BNY Mellon,
- Mitsubishi UFJ Financial Group,
- Citi,
- Commerzbank,
- Deutsche Bank,
- HSBC,
- Morgan Stanley,
- National Australia Bank,
- Royal Bank of Canada,
- SEB,
- Societe Generale,
- Toronto-Dominion Bank

…



Bitcoin

ビットでできたコイン？

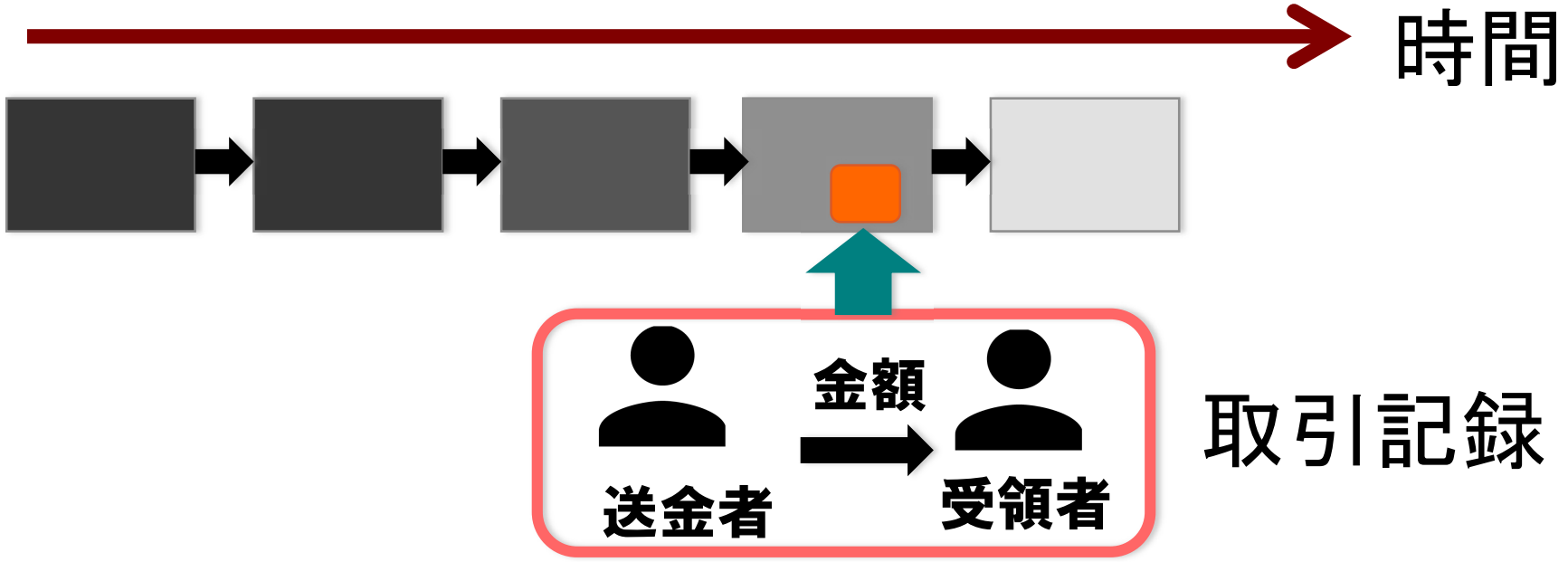
Bitcoinには

実は、コインは存在しません

価値記録の対象も存在しない

Bitcoinの本質は

出来事の非可逆的記録



従来の電子通貨研究

アトムのコインをビットのコインに

アトムでできたコイン

ビットでできたコイン

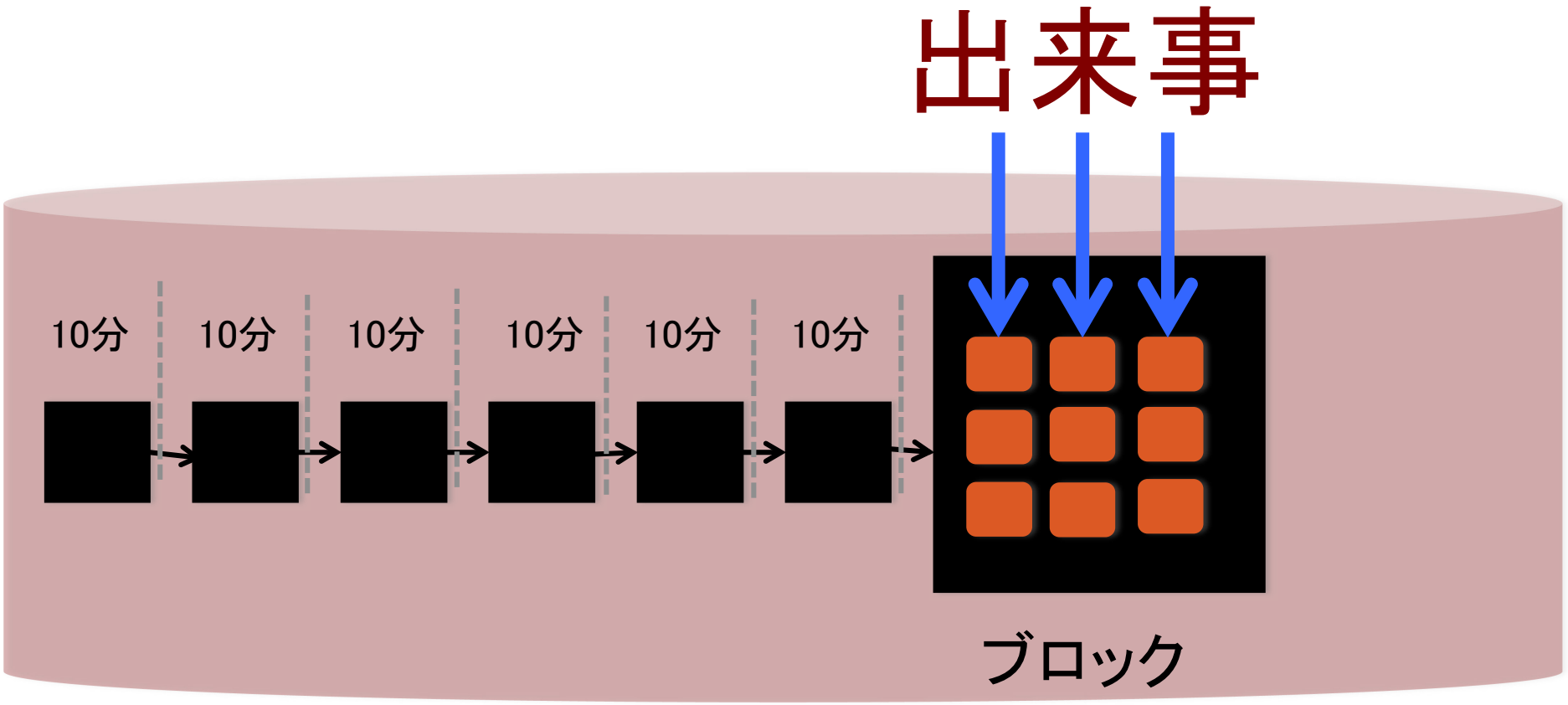
100円
19145688628917083994040390
48214754959144168148568993
65794840613080823883302O2

10円
21102336943757887962062431
98022317897796829477986168
22155467362809936434640 22

電子トークン実現技術

ブロックチェイン

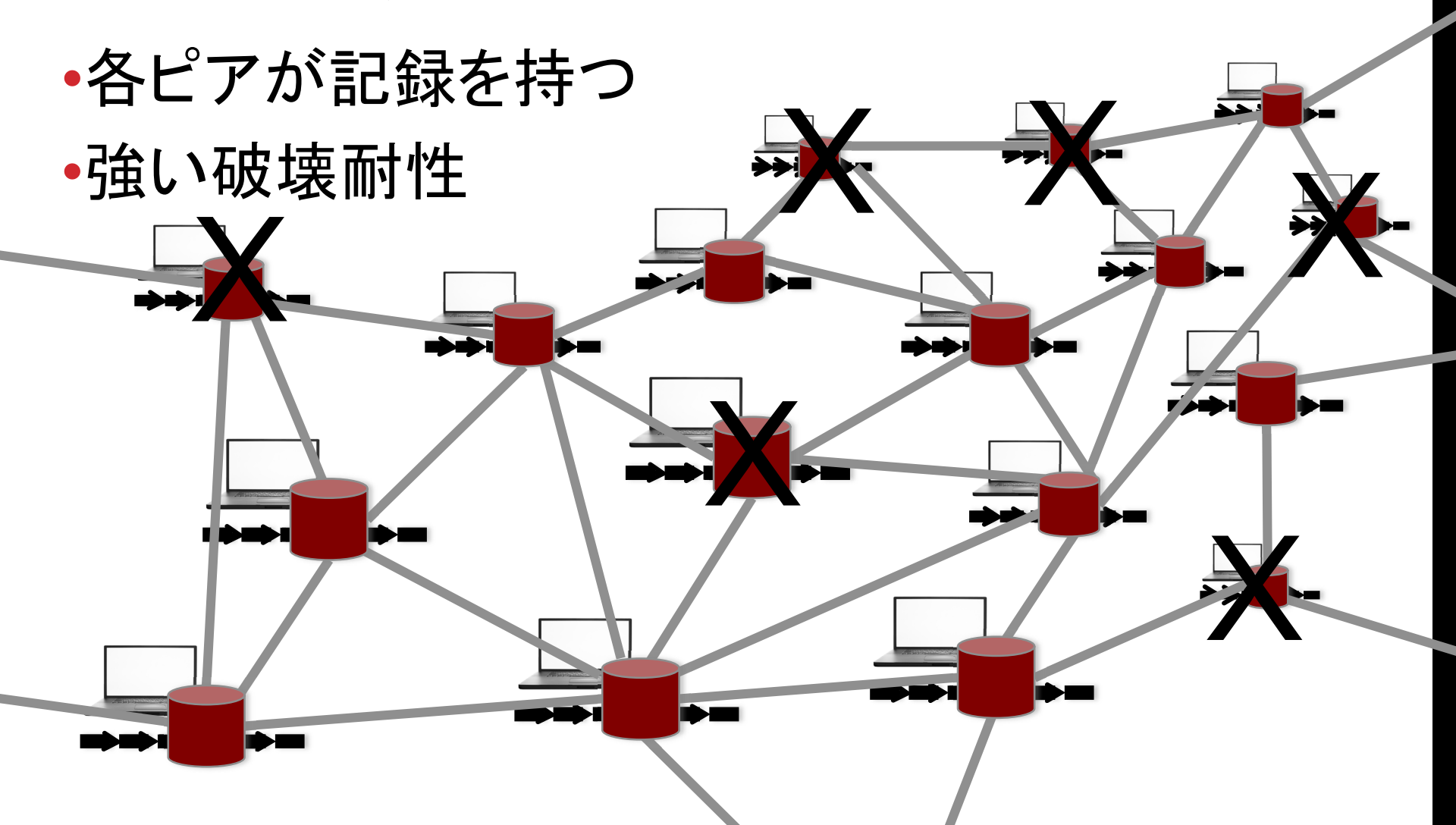
時系列的な出来事の記録簿



ブロックチェイン

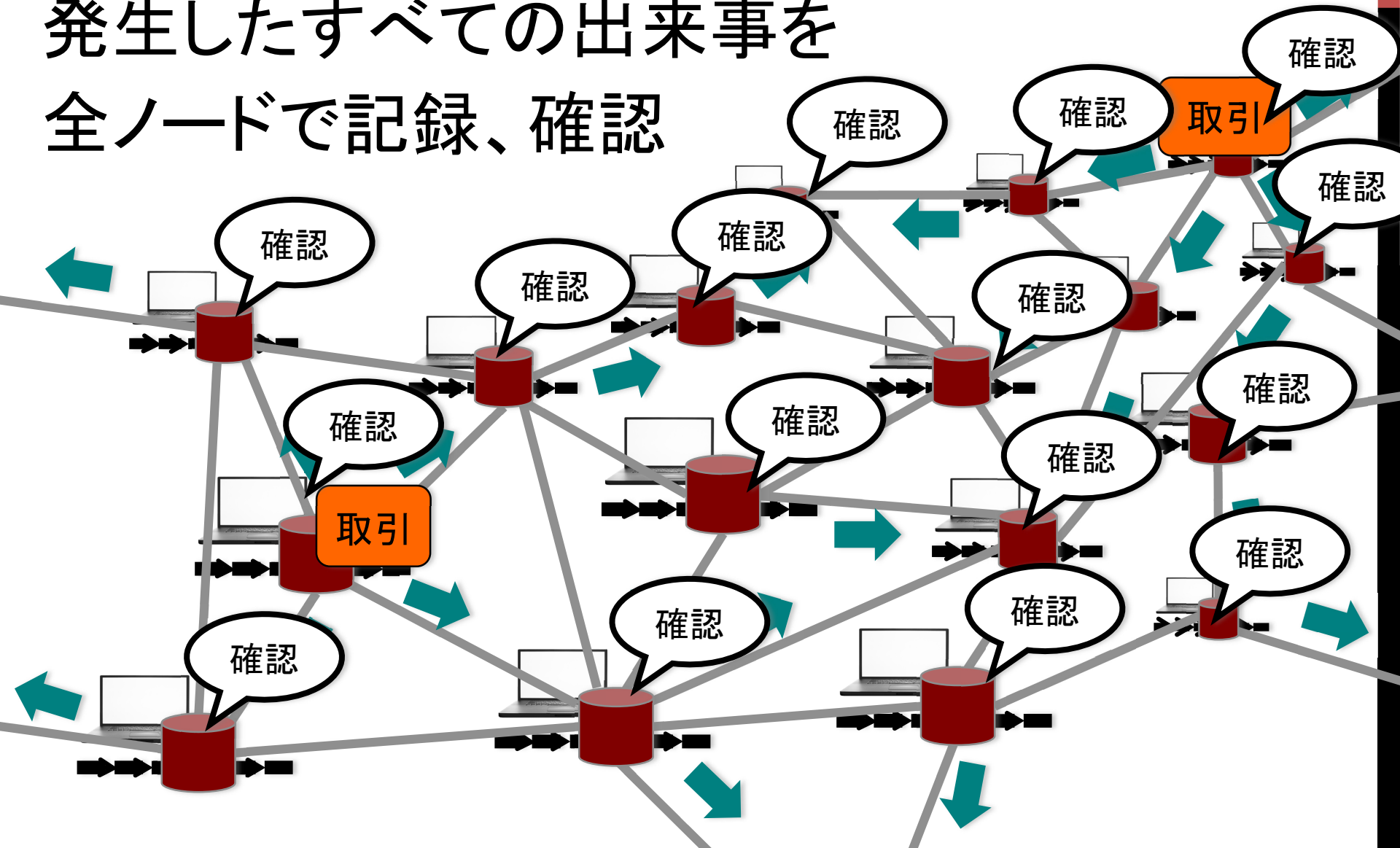
P2P型分散DB

- 各ピアが記録を持つ
- 強い破壊耐性



Bitcoinネットワーク

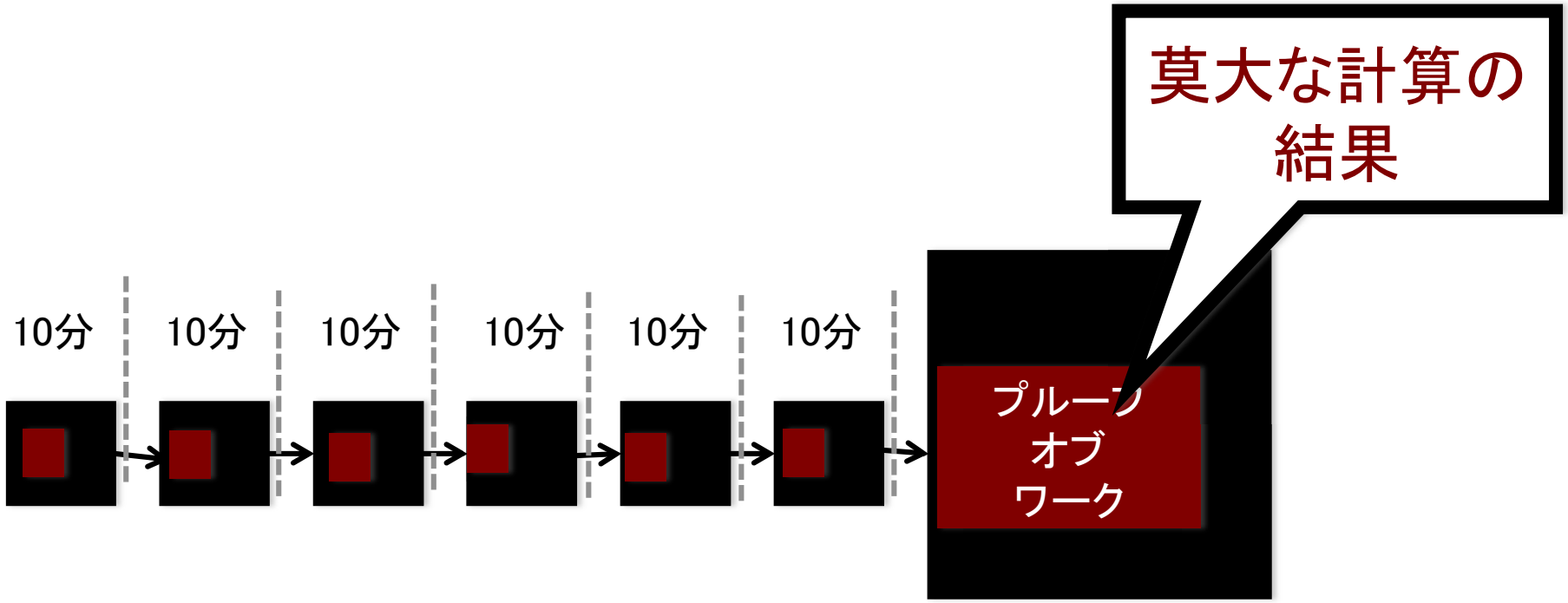
発生したすべての出来事を
全ノードで記録、確認



ブロックチェインの非可逆性

プルーフ・オブ・ワーク

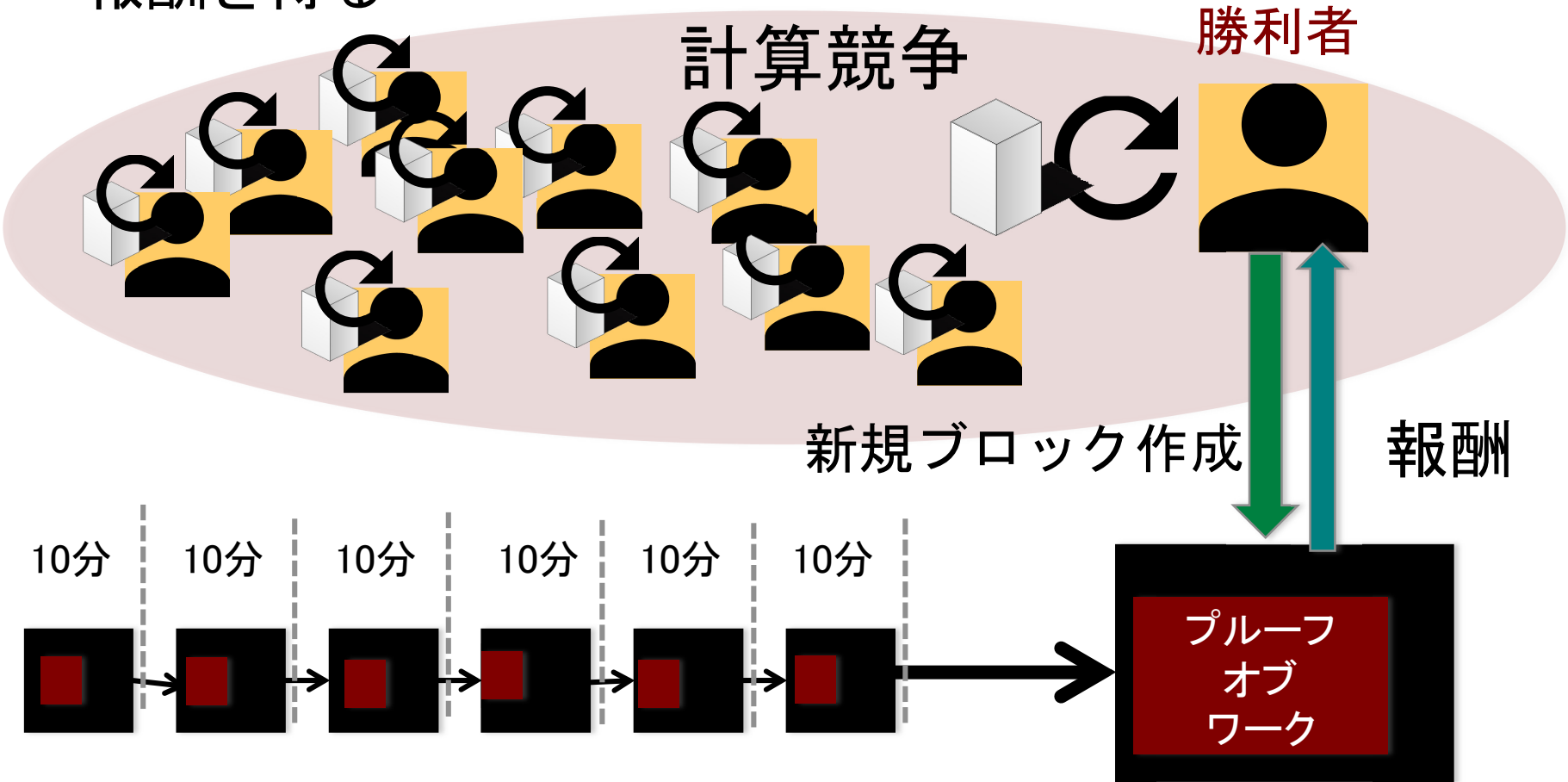
- 莫大な計算の証拠
- 時間を巻き戻すには莫大な再計算が必要



マイニング競争

プルーフオブワークの計算競争の勝利者

- 新しいブロックを作成
- 報酬を得る



トラストレス

信頼できる第三者機関が必要ない

参加者全員ですべての「出来事」を監視

- P2P型ネットワークで分散管理

ビザンティン将軍問題への耐性

- 巧妙に結託する裏切り者達がいても機能する

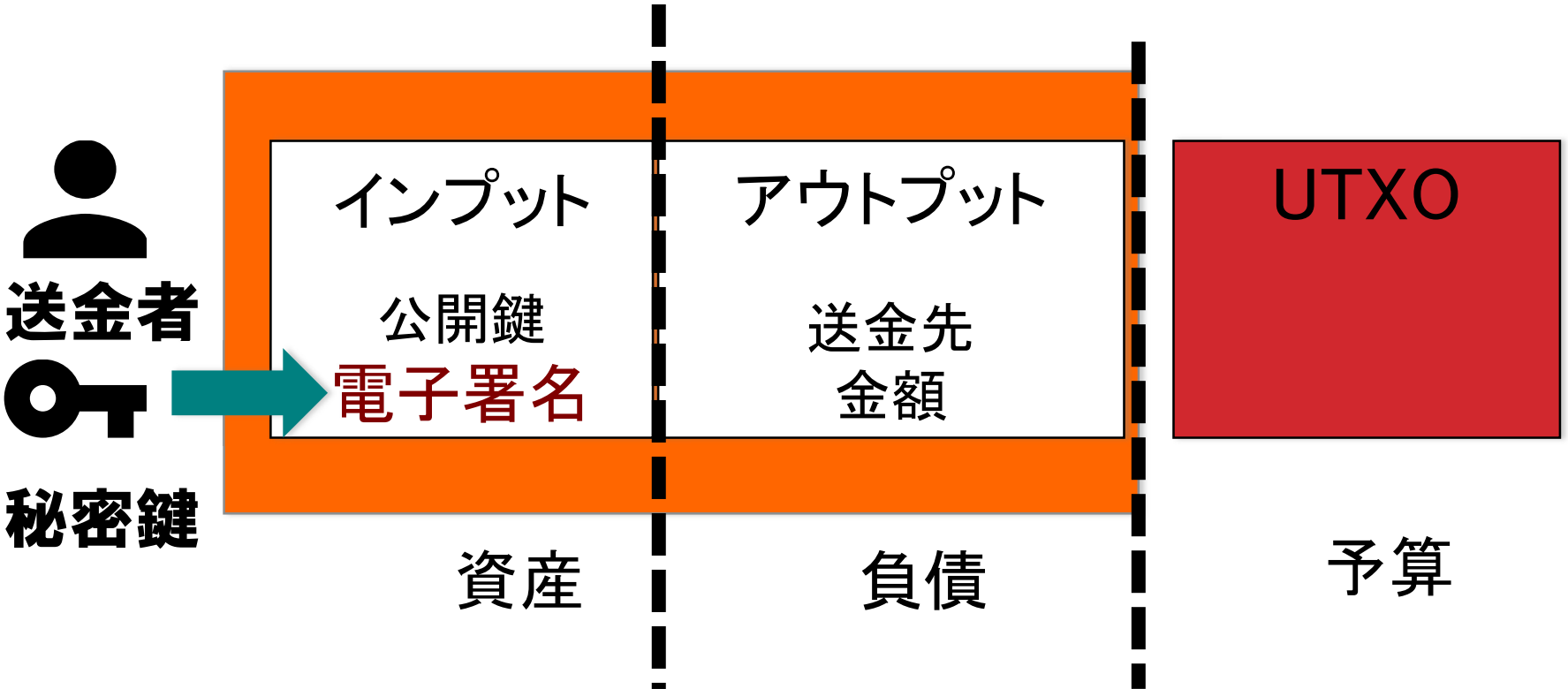
マイニング・インセンティブの利用

- 信頼できる第三者の代わりに欲望に基づく競争行動を利用

取引記録（できごと）

三式簿記の構造を持つ

（資産合計＝負債合計＝予算合計）



ニュートン力学のアナロジーで仮想通貨の原理を説明してみる

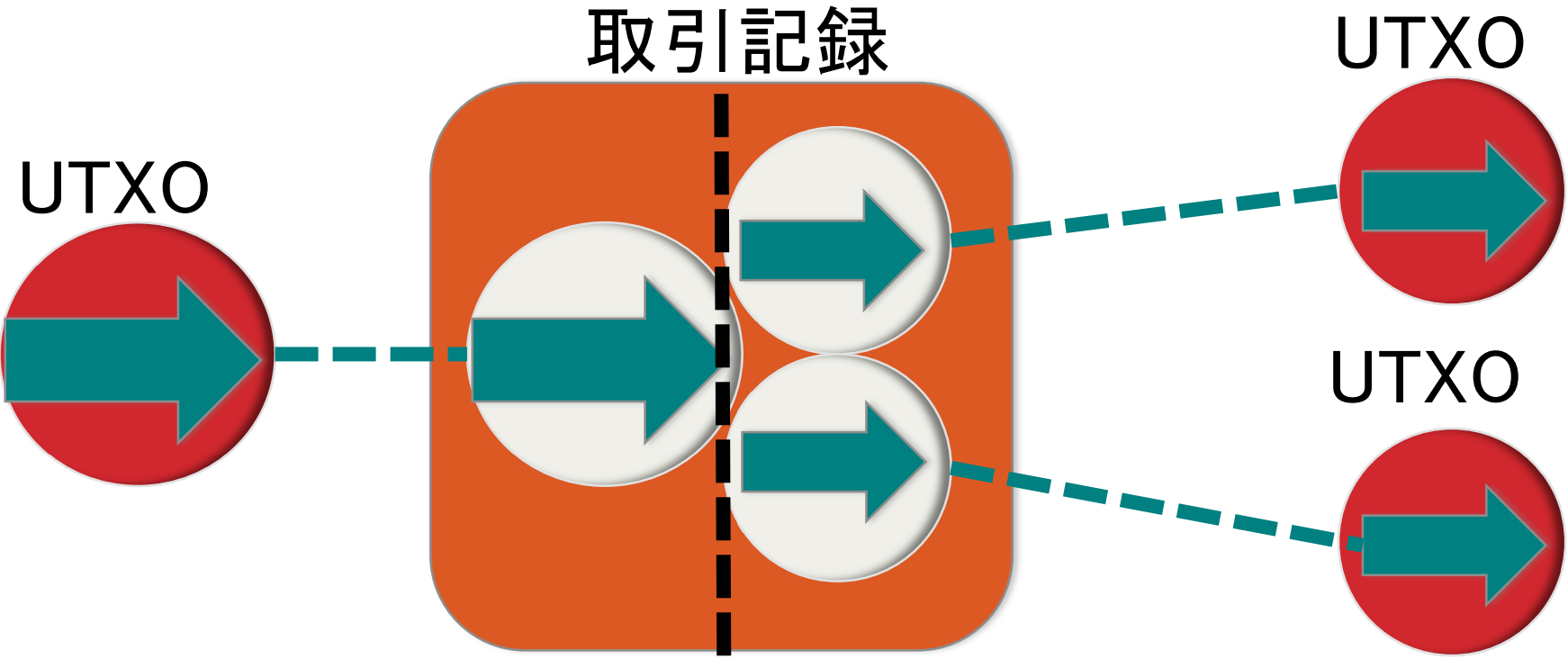
作用反作用の法則　＝ 運動量保存則

慣性の法則 ＝ 運動量を保持した等速直線運動

三式簿記と通貨価値の保存則

取引記録：衝突による運動量の移動

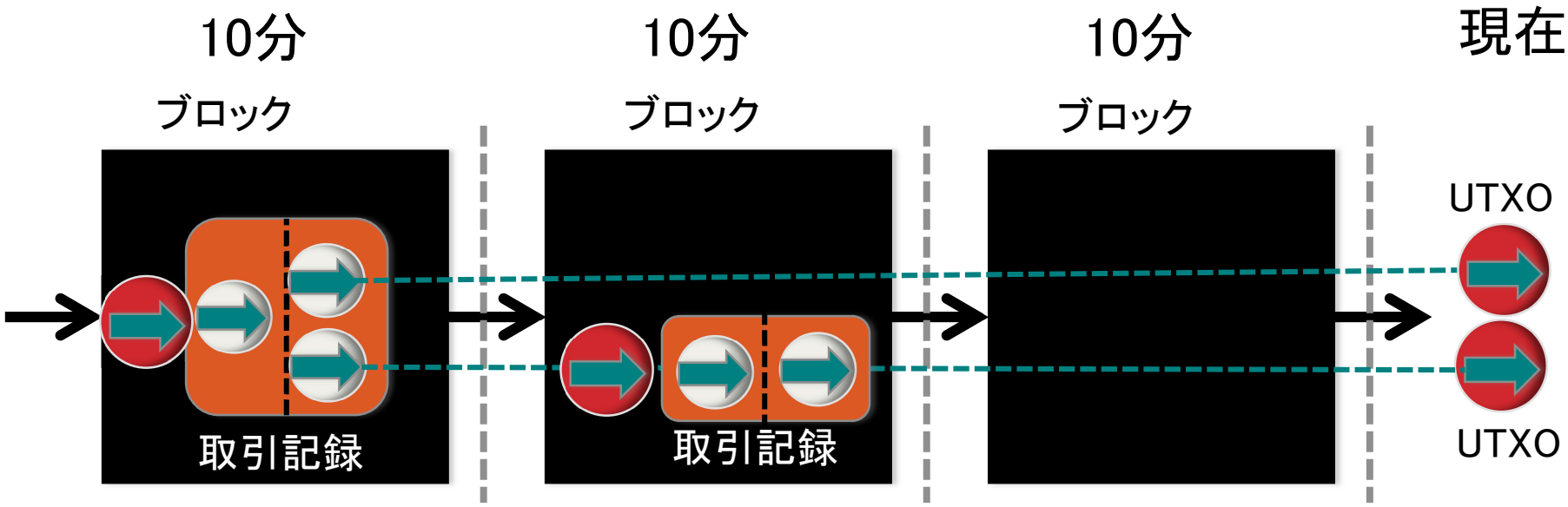
UTXO：衝突後の運動量の表現



慣性の法則

外力が働かない ＝ 新しい取引がないとき

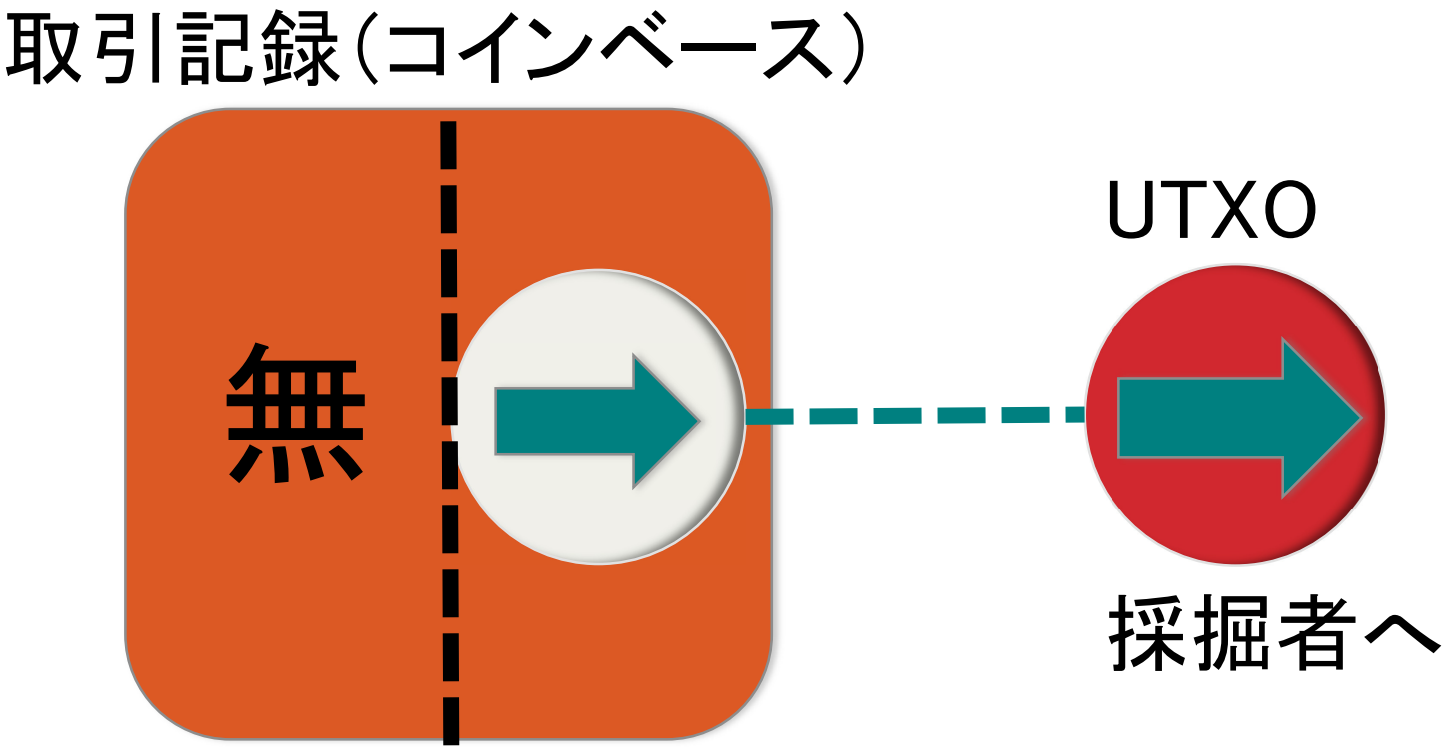
UTXOは、現在まで順次引き継がれる



最初の価値の発生は？

コインベース：通貨発行用の取引記録

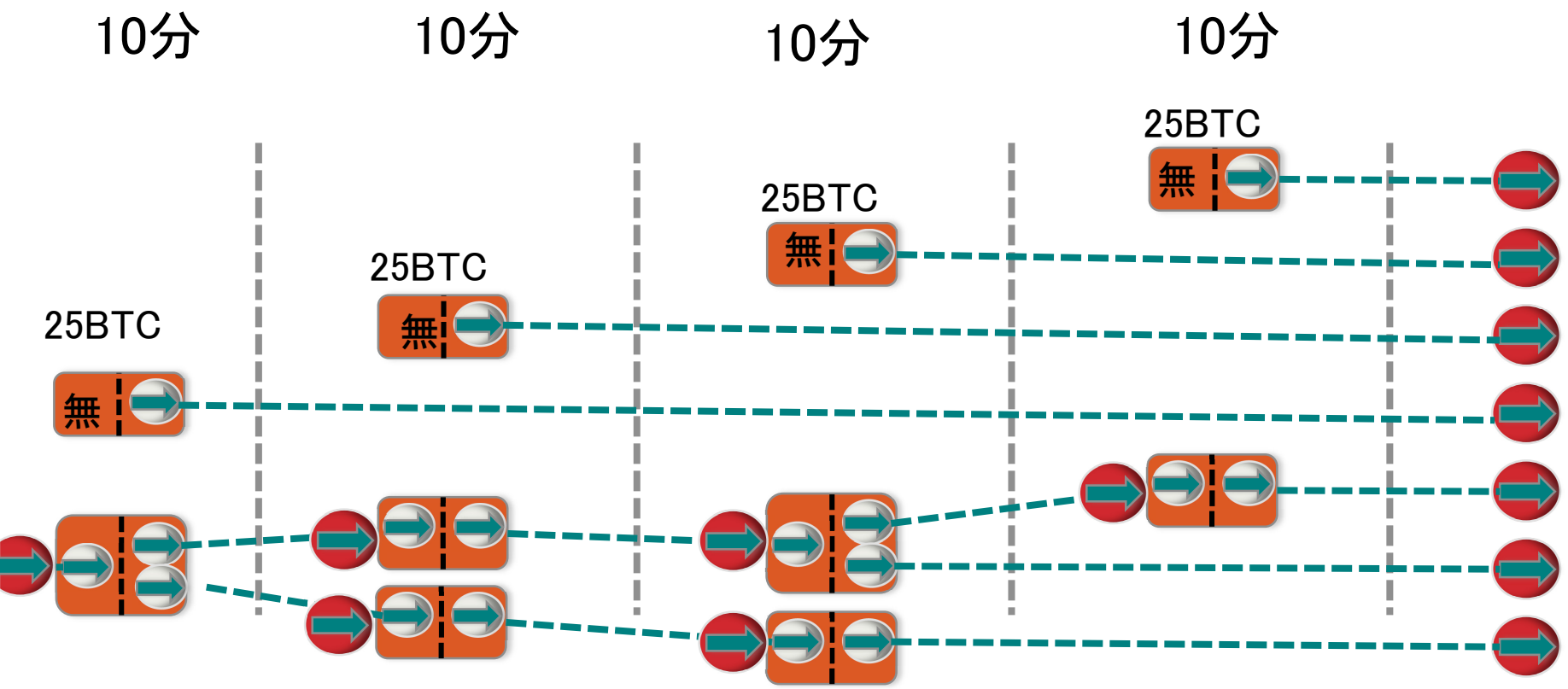
採掘者の報酬



経済圏全体の「量」は単調増加

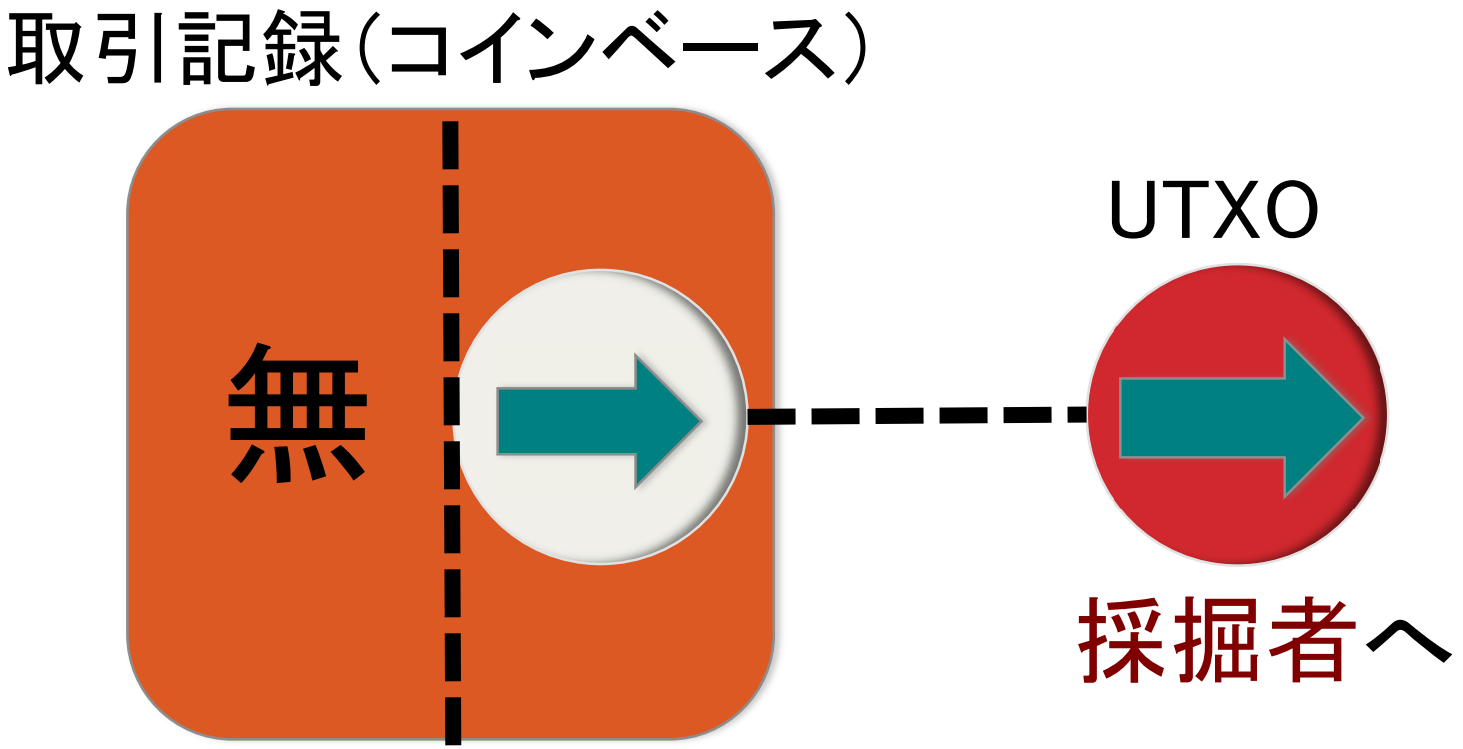
10分ごとに一定量増加している

- 増加量は（4年周期で半減）



採掘者は通貨発行者ではない

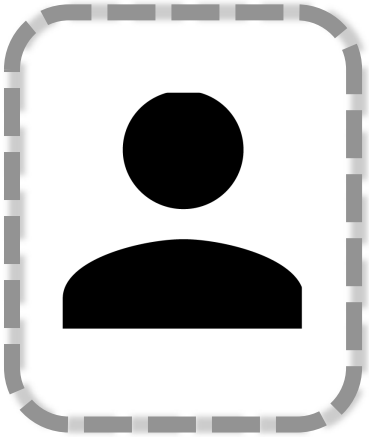
無から生じた価値を受領しただけ



Bitcoinは

債権債務関係を構成できない

「債務者」を定義できないから



債券発行者
債務者

Open Assets Protocol

Bitcoinのブロックチェインで債券を構成する技術

NASDAQなどが採用

NASDAQ is using Open Assets

BY COINPRISM · MAY 16, 2015

The work on Open Assets started end of 2013. At the time, Bitcoin 2.0 technologies were really nascent. Colored coins had been around for some time, but there was no good way to use them, no standard, and therefore no traction. This is how Open Asset (and Coinprism) got born.

Open Assets was first presented publicly in March 2013 at CoinSummit, though it was not yet called "Open Assets", and was not finalized.

bitcoinのスクリプト言語

Forth言語に似たスタック型言語

逆ポーランド記法＝日本語記法

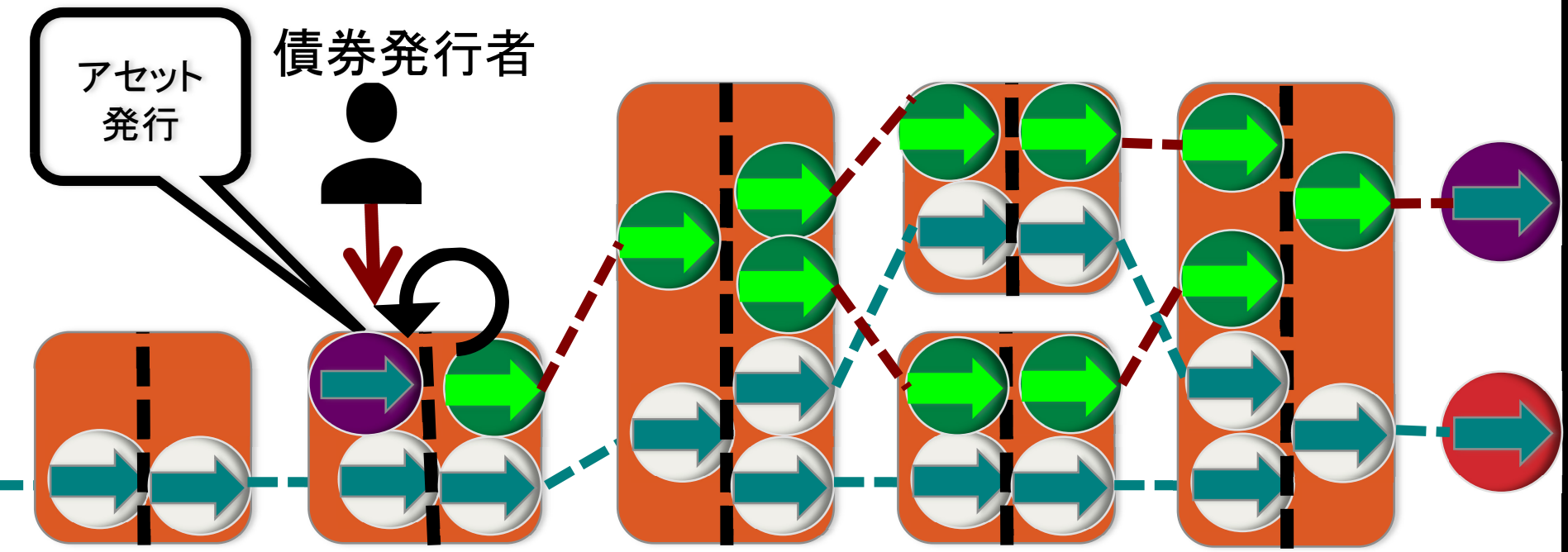
- OP_EQUALVERIFY ：
  - スタックの2要素を取り出し、双方が等しいことを確認する
- OP_CHECKSIG：
  - 公開鍵を使って電子署名を検証する
- …
- OP_RETURN：80バイトの任意の情報を記録できる

Open Assets とBitcoin

Open Assets

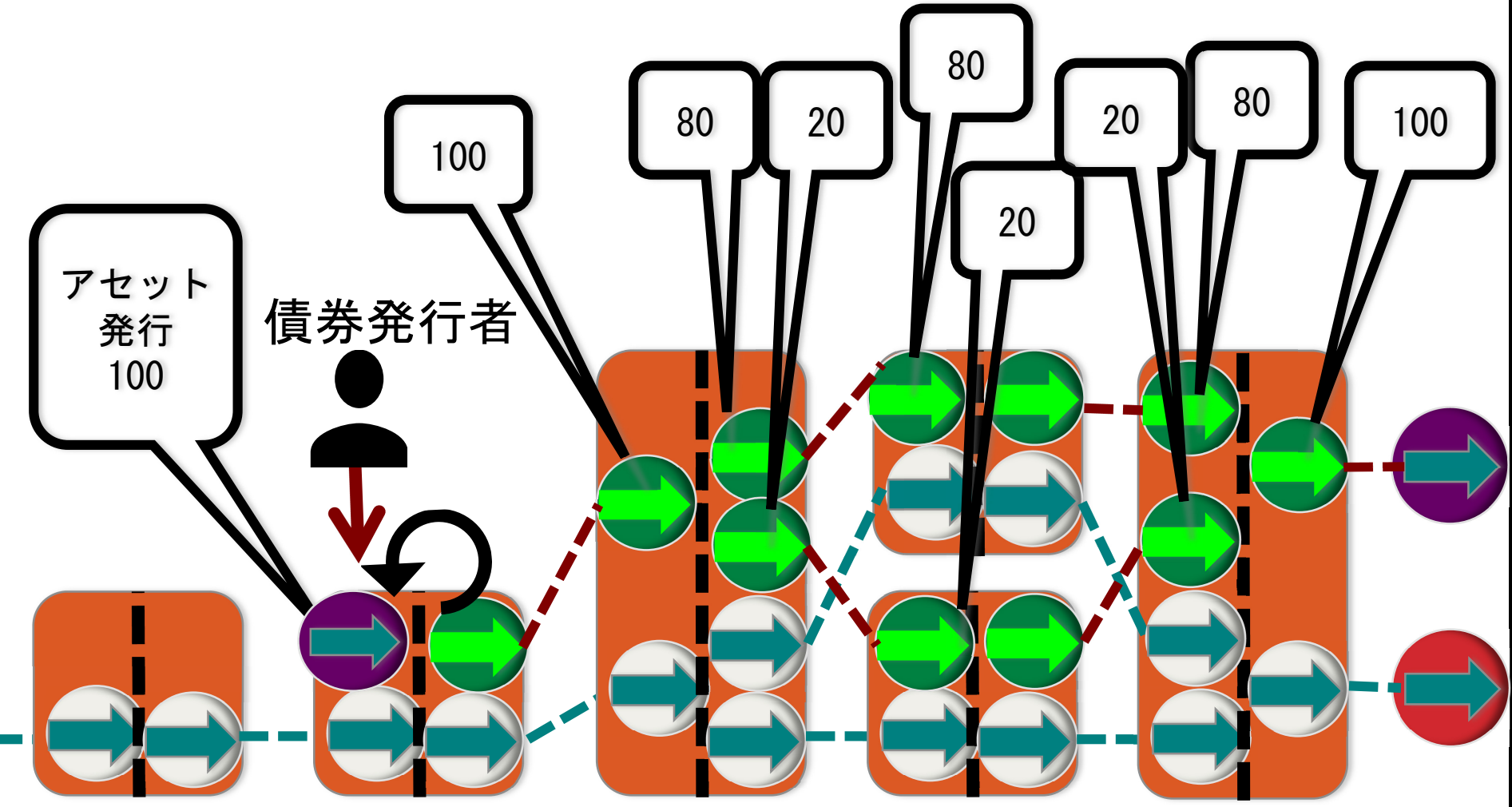
Bitcoin 0/1億 BTC) 約0.2円

- Bitcoinの上位レイヤとしてアセットを定義する
- 発行者(債務者)が存在する



Open Assetsの三式簿記

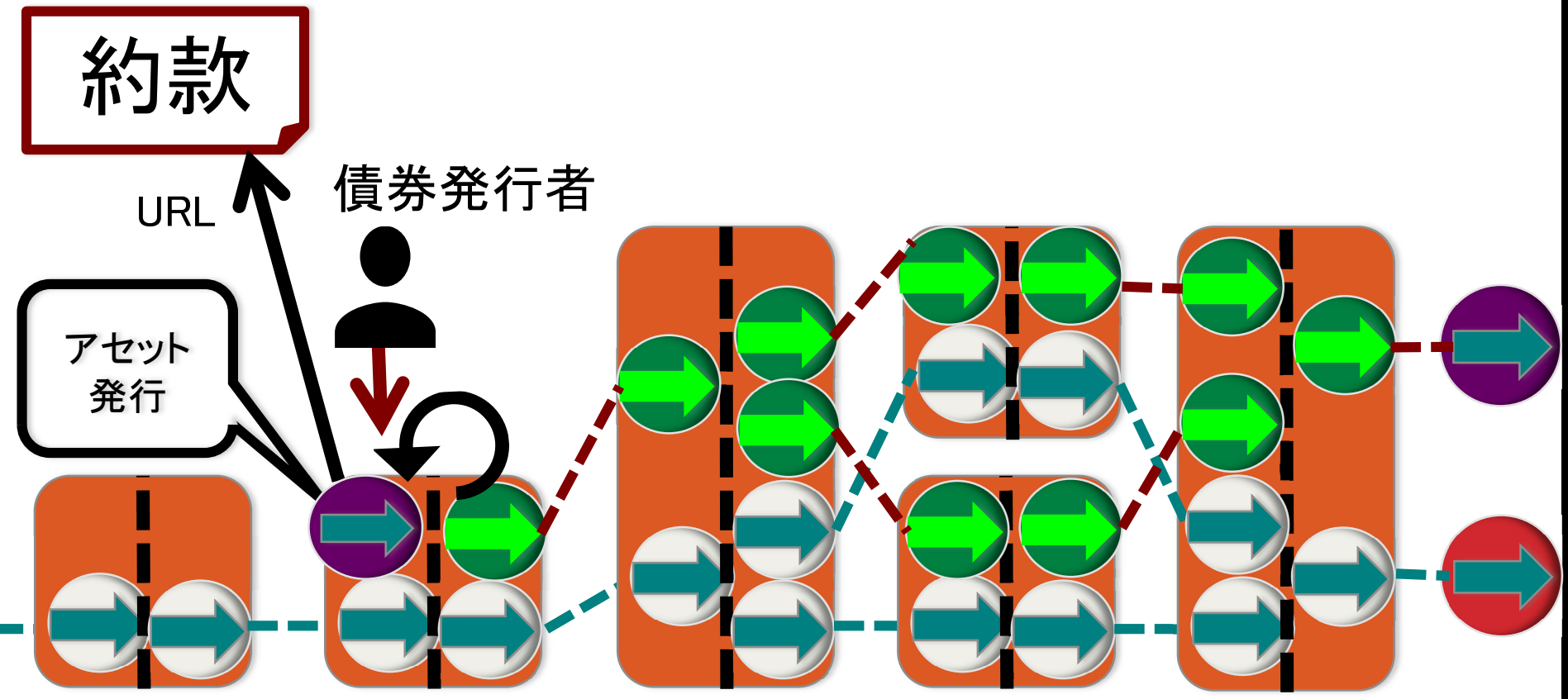
発行されたアセットの総量は保存される



Open Assetsの約款

Asset definition file

- URLでブロックチェインから参照されるJSONデータ
- 債券を定義できる



Asset definition File

{"asset_ids": [アセットID],
"name_short": 略称
"name": 名称,
"contract_url": "コンタクトURL",
"issuer": "アセット発行主体名",
"description": "約款の文書",
"description_mime": "MIME",
"type": "タイプ",
"divisibility": 分割可能性の桁数,
"link_to_website": ウェブサイトへの接続可能性,
"icon_url": アイコンへのURL,
"image_url": 画像へのURL,
"version": バージョン番号
}

PKIとビットコインの
アイデンティティの相違点

公開鍵証明書

CA

本人識別名

公開鍵

電子署名

ビットコインアドレス

17Lwkv258LqZv4nvjGcRTJVA1ppB4qHWoJ

ハッシュ関数

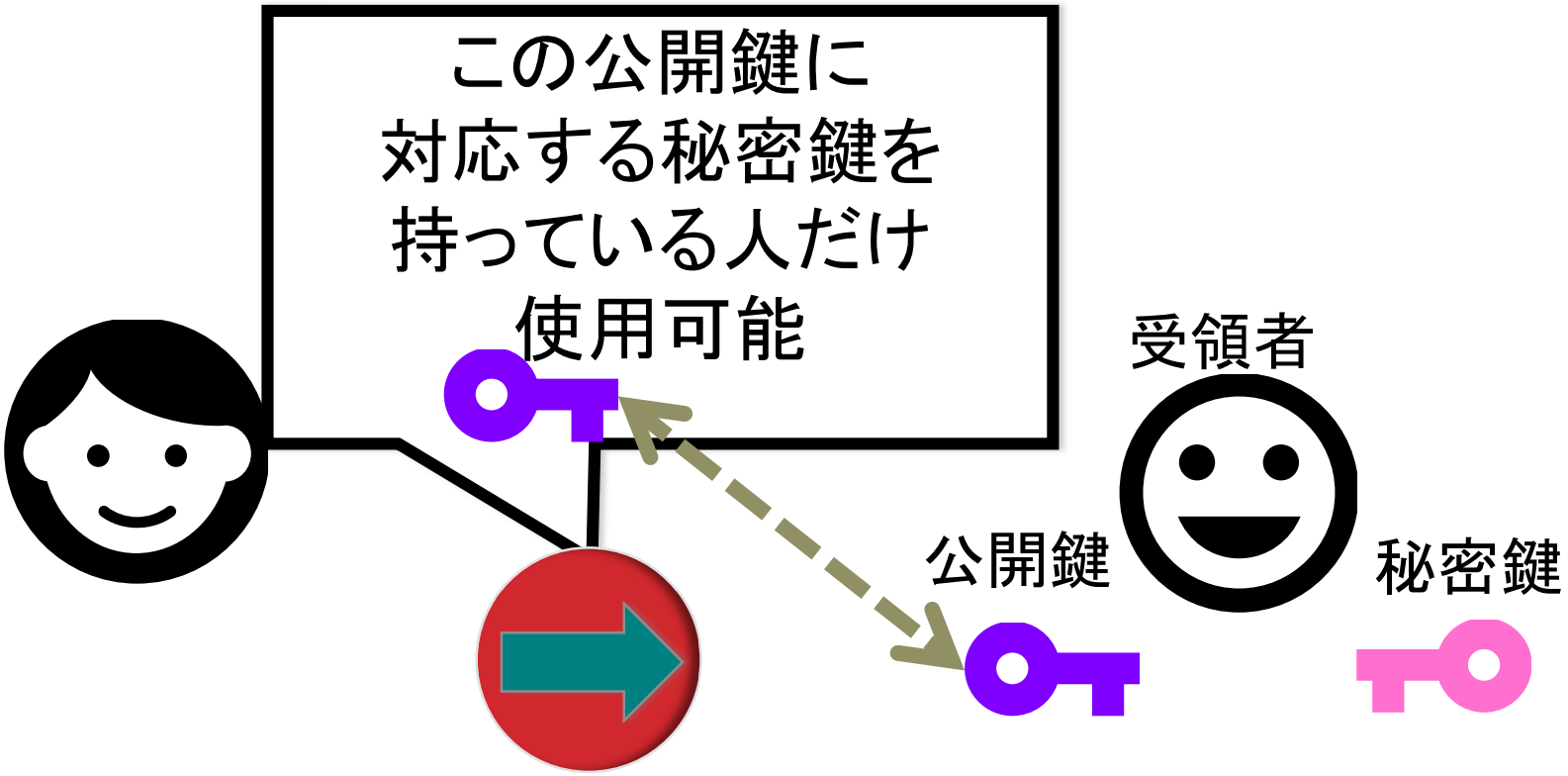
公開鍵

秘密鍵

取引記録のスクリプト

目的 送金された金額の使い方を規定

- 受領者が次に使うときに評価される



P2PKH（公開鍵ハッシュが条件）

条件：この公開鍵の所有者だけ次に使用できる

送金するためのinput

秘密鍵

（次の）
送金者

scriptSig:
〈電子署名〉〈公開鍵〉

scriptPubKey:
OP_DUP OP_HASH160 〈公開鍵Hash値〉 OP_EQUALVERIFY OP_CHECKSIG

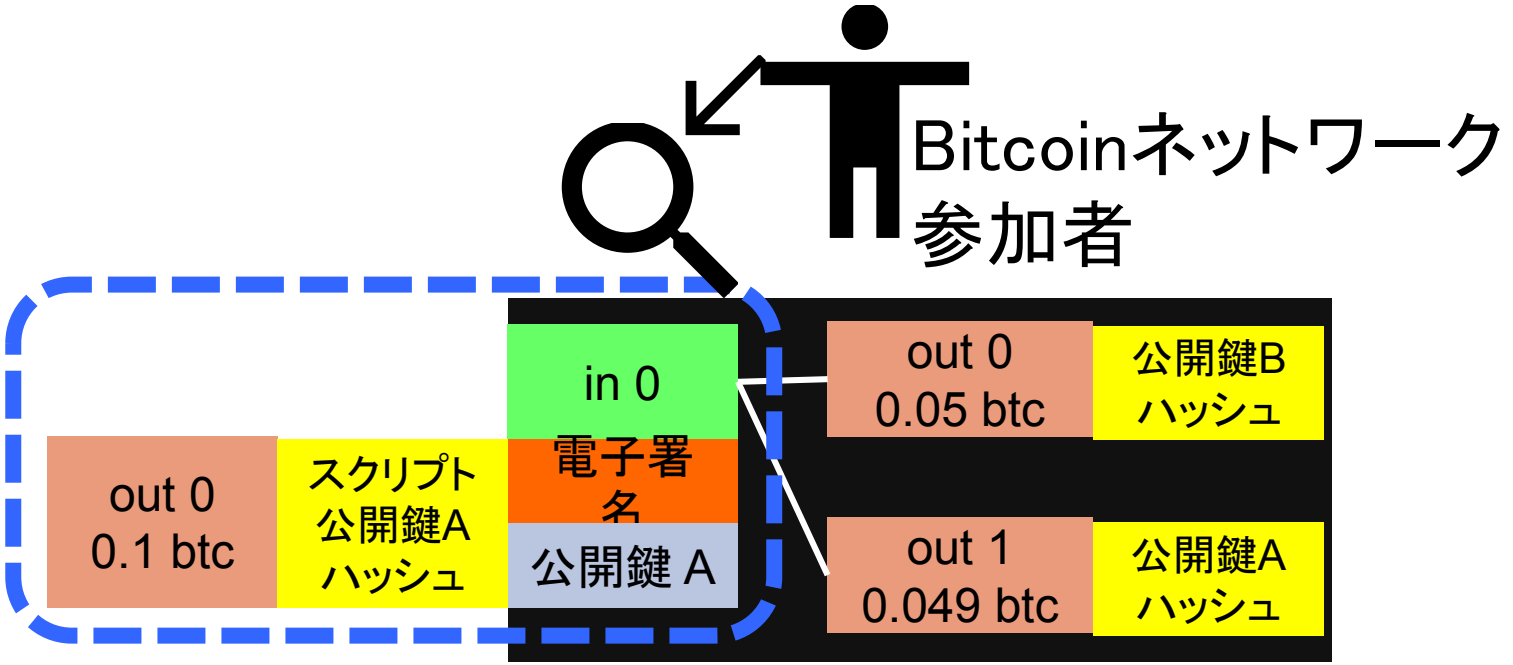
直前のoutput

証明すること
(1)この公開鍵は、公開鍵Hash値に対応していること
(2)電子署名によって公開鍵とペアになっている秘密鍵を持っていること

Stack	Script	説明
	<電子署名> <公開鍵> OP_DUP OP_HASH160 <公開鍵ハッシュ> OP_EQUALVERIFY OP_CHECKSIG	スタックは空
	OP_DUP OP_HASH160 <公開鍵ハッシュ> OP_EQUALVERIFY OP_CHECKSIG	最初の2つの定数をスタックにプッシュする
	OP_HASH160 <公開鍵ハッシュ> OP_EQUALVERIFY OP_CHECKSIG	スタックの先頭要素をコピーする
	<公開鍵ハッシュ> OP_EQUALVERIFY OP_CHECKSIG	スタックの先頭をsha256,RIPEMD160でダブルハッシュする
	OP_EQUALVERIFY OP_CHECKSIG	scriptPubKeyの公開鍵Hash値をスタックにプッシュする
	OP_CHECKSIG	スタックの先頭2要素を取り出して等しいことをチェック
		スタックの先頭2要素を取り出し、公開鍵から電子署名の検証を行う

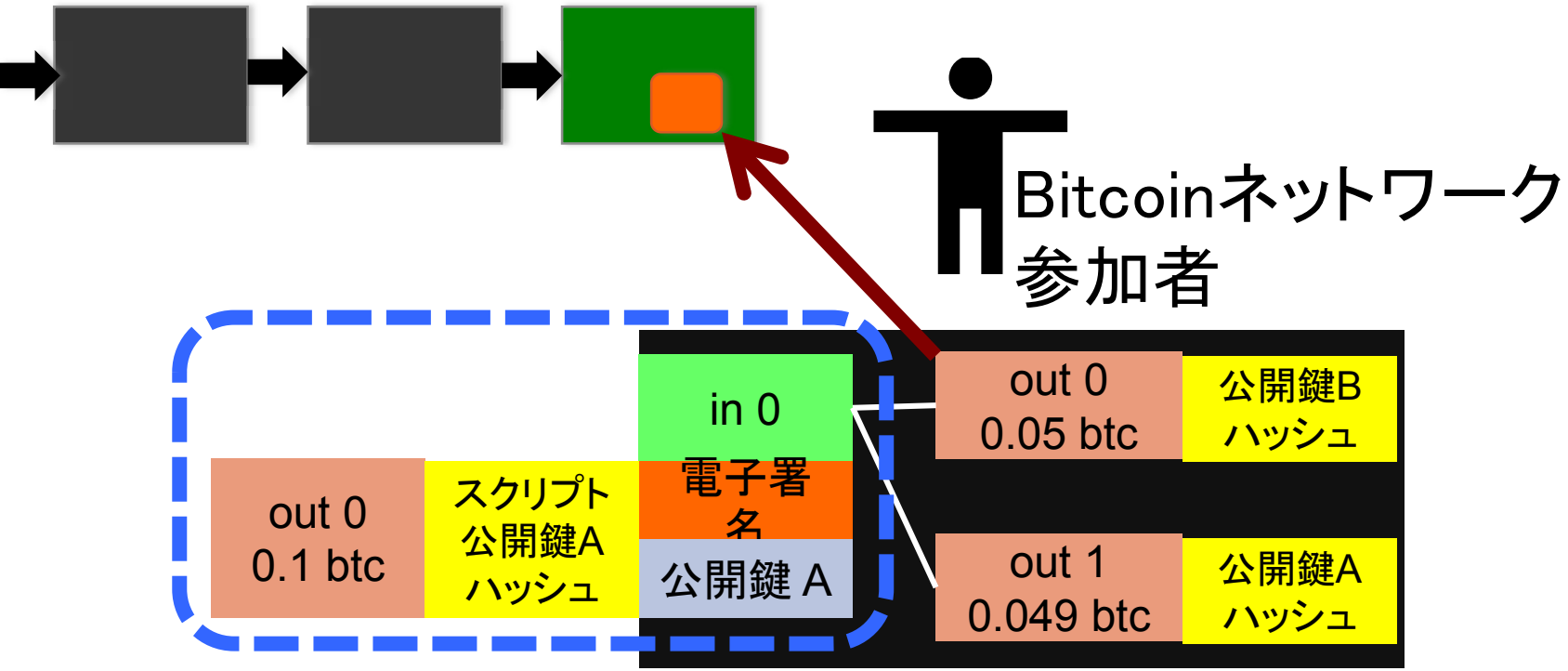
取引記録の検証

直前のoutput とinputの結合を検証



取引記録の検証と承認

検証に成功すればブロックチェインの
ブロックを承認



通貨に必要な性質

通貨には、汎用性と流通性が必要

汎用性：何でも買える（もの）

流通性：誰に対しても使える（人）

現在の仮想通貨や電子マネーは不十分

Open Assets債券の例

自己宛小切手

（銀行が発行する小切手）

- 発行者：銀行
- 内容：アセット量と同額の日本円と交換

実質的に日本円として流通する

理想の電子通貨が実現？

汎用性、流通性を備えた電子通貨

さらに仮想通貨の特性を備える

- 転々流通が可能
- 決済手数料が劇的に安い
- ソフトウェアのみで実現可能
- ユーザ登録不要
- モバイル決済可能
- web決済が可能

理想の電子通貨が実現？

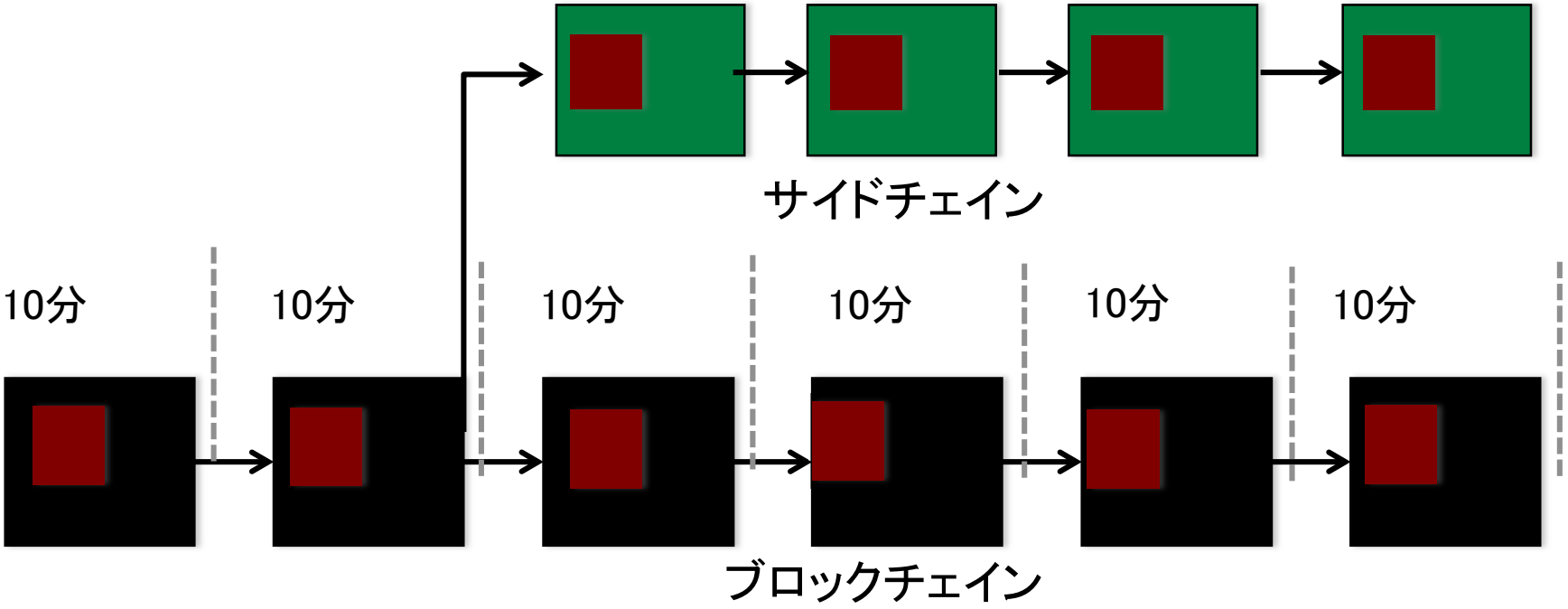
理想的すぎて

法制度的課題も多い

サイドチェインとは

ブロックチェインの分岐

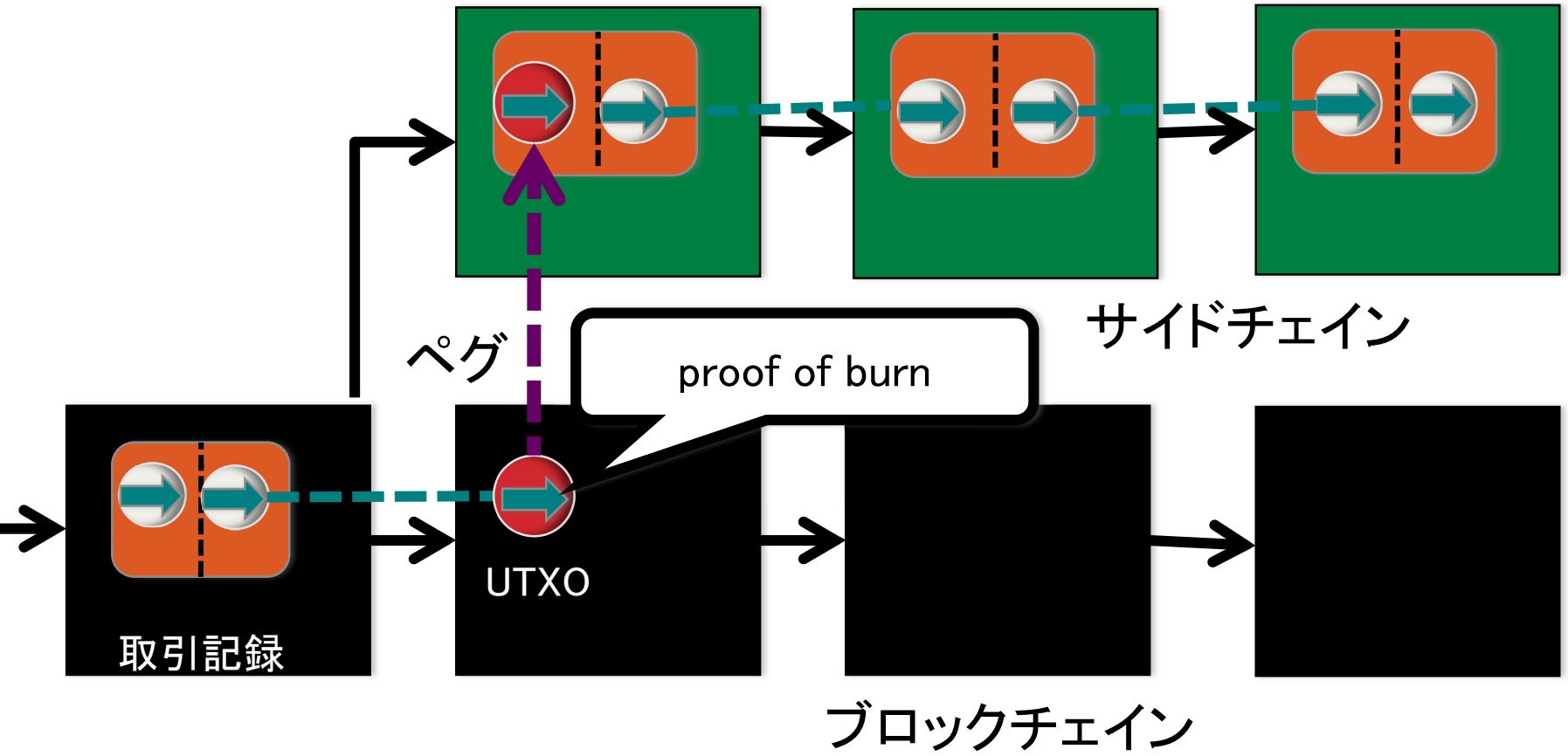
- 独自仕様のブロックが作成可能
- パブリックにしなくてよい



ペグ付きサイドチェイン

ブロックチェインのUTXOを使用不可状態に

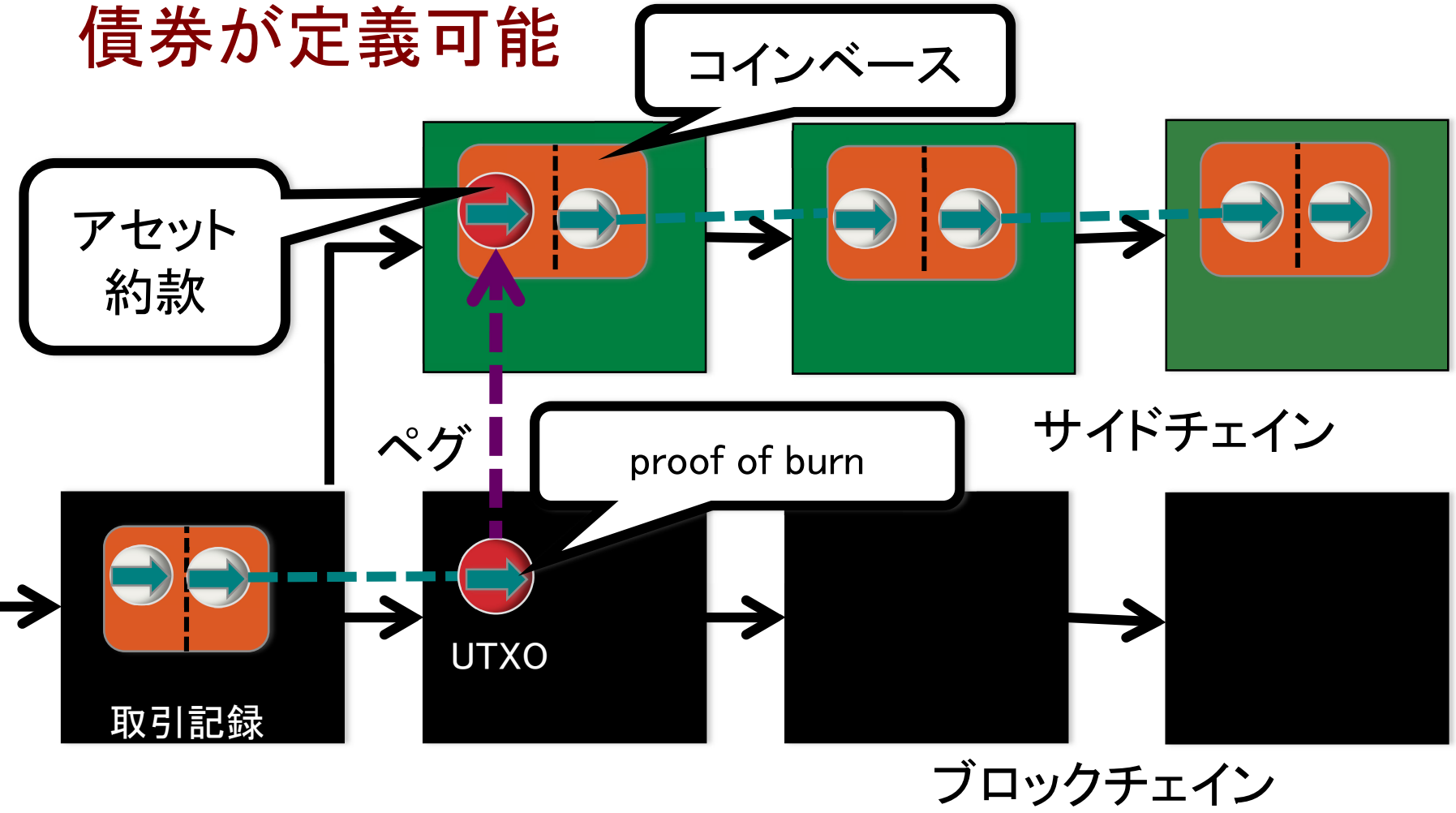
そのUTXOをサイドチェインに登場させる



サイドチェインによるアセット

コインベースにインプットが存在する

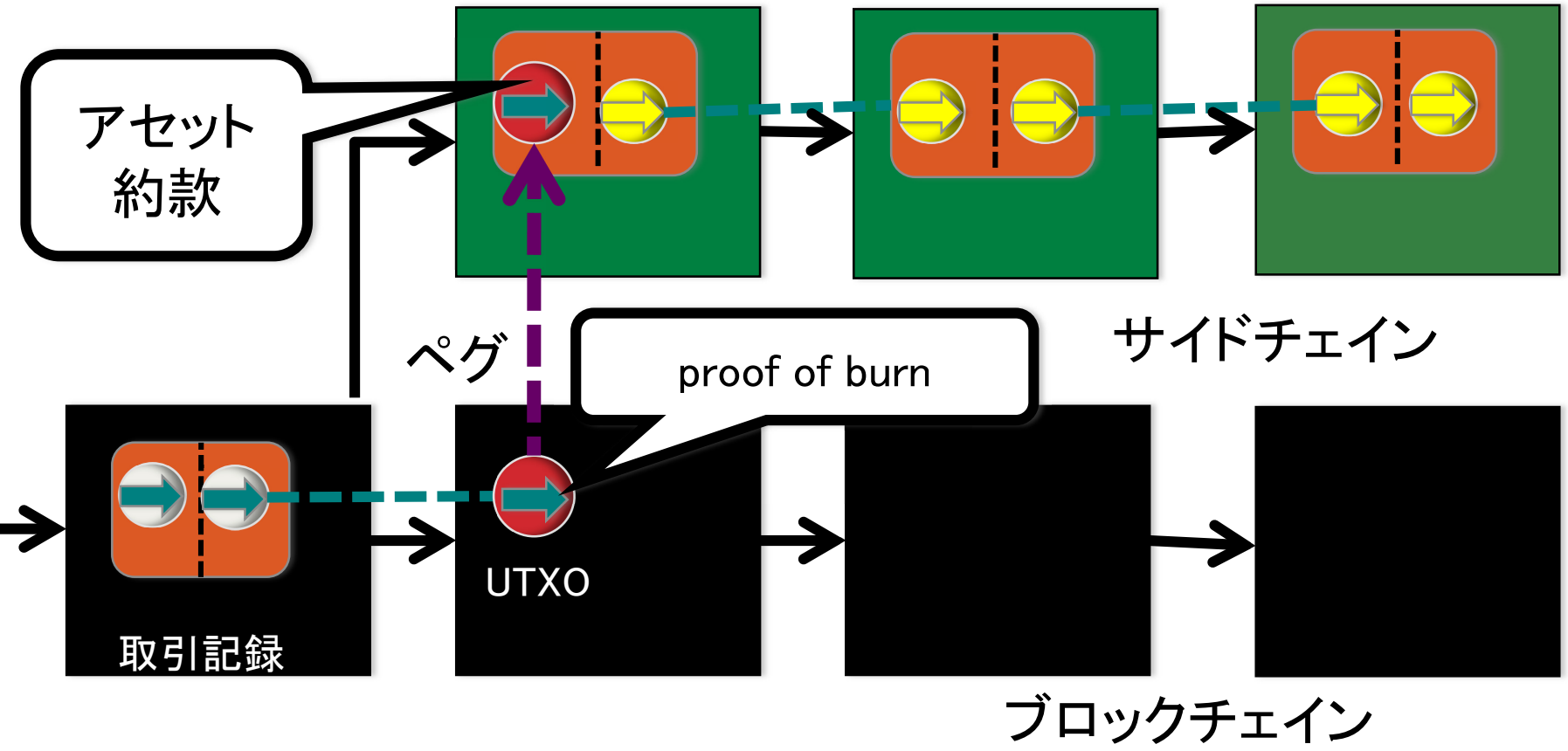
債券が定義可能



サイドチェインによるアセット

ビットコインは一切含まれない

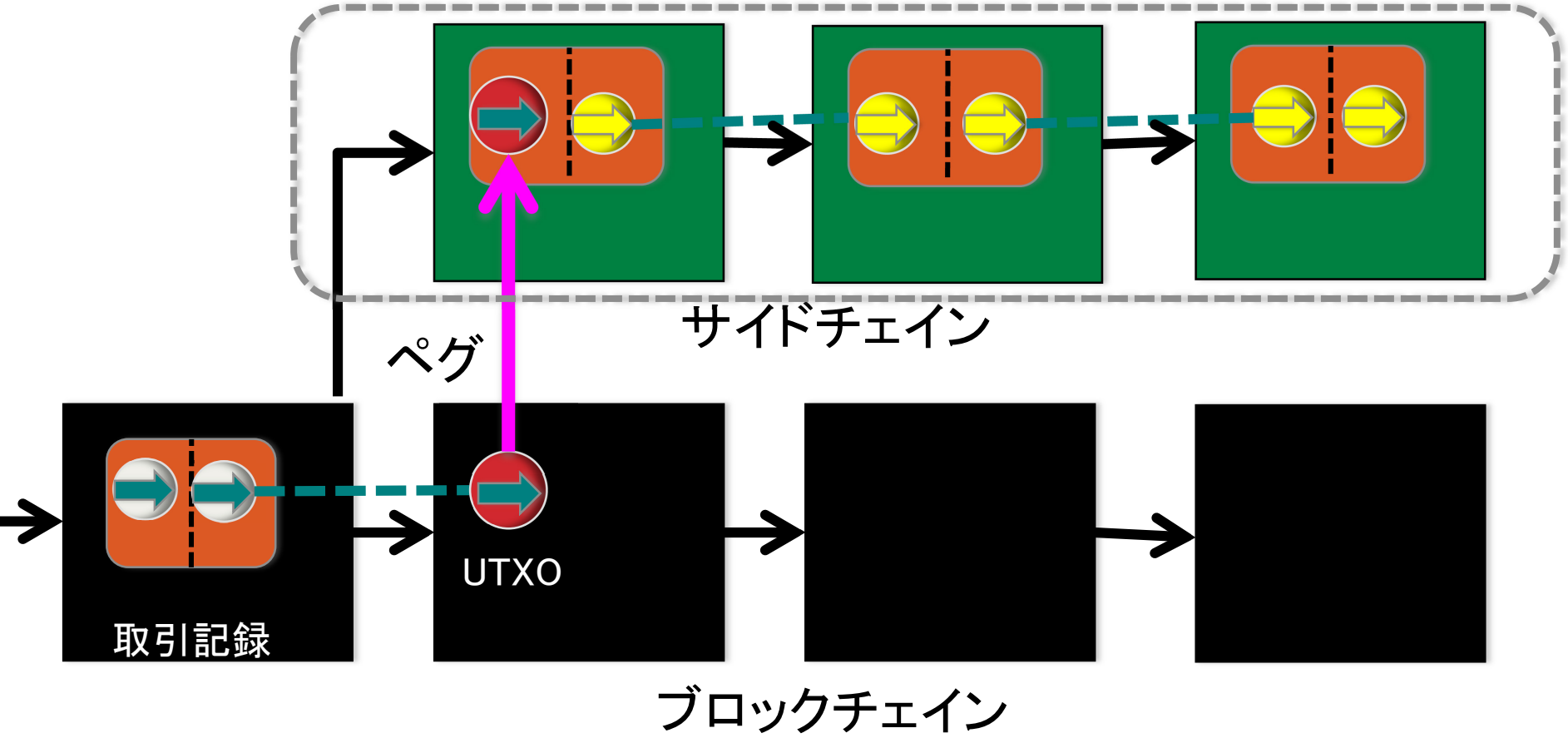
- ビットコインとは法的に独立に扱うことができる



サイドチェインの信用

プライベートなブロックチェインなので

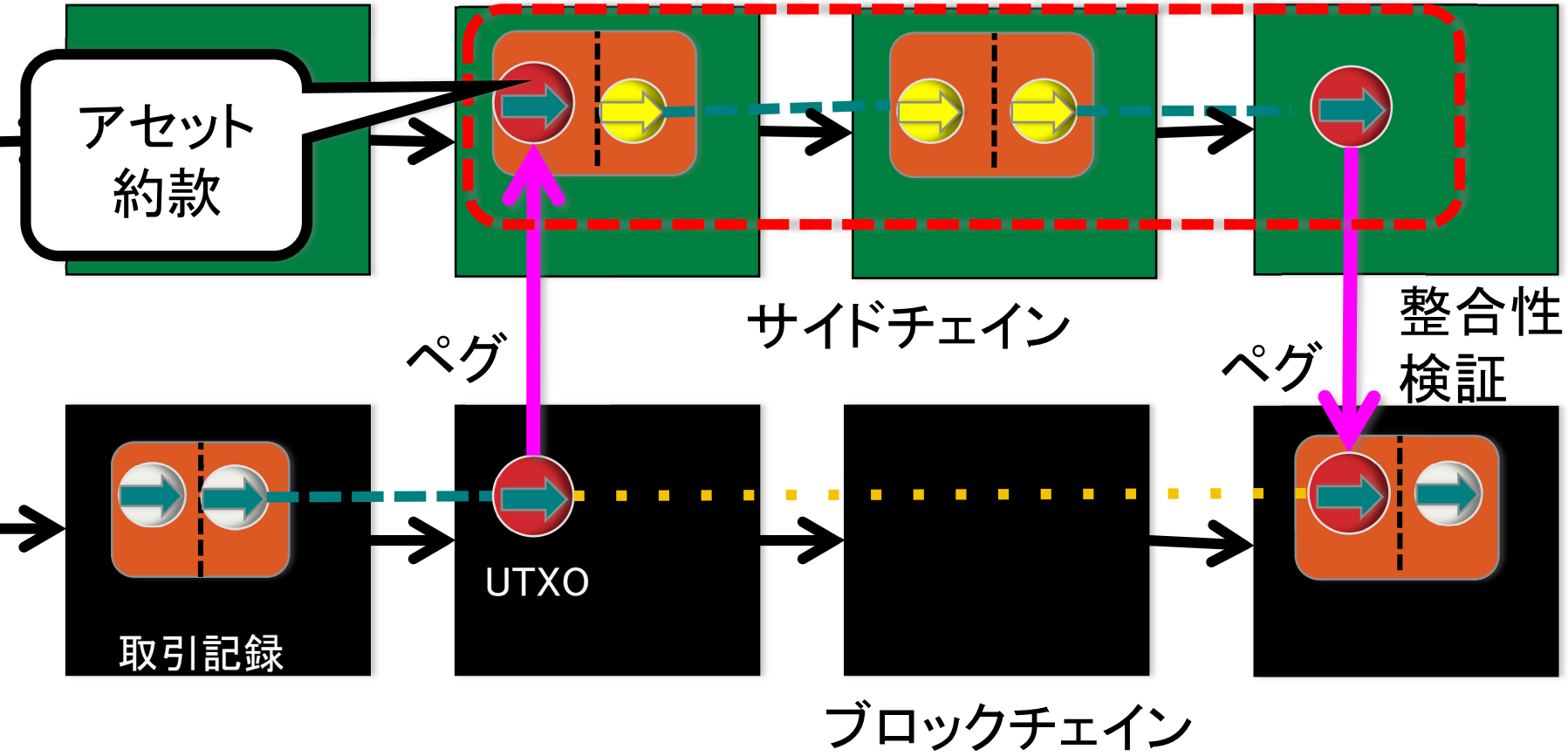
「信用できる記録」ではなくなる



2-way peg型サイドチェイン

UTXOをブロックチェインに復帰させる

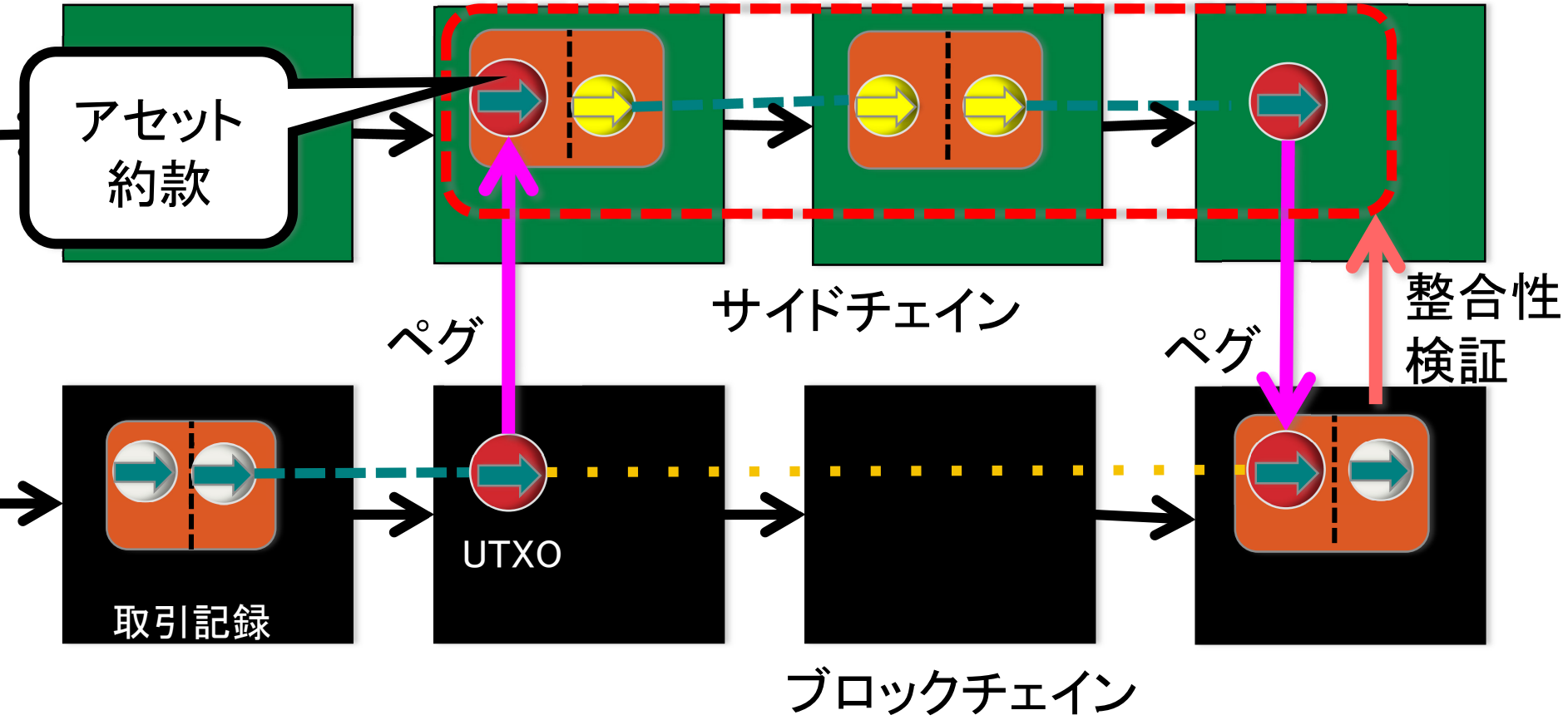
復帰させるときにサイドチェインの全整合性を検証



2-way peg型サイドチェイン

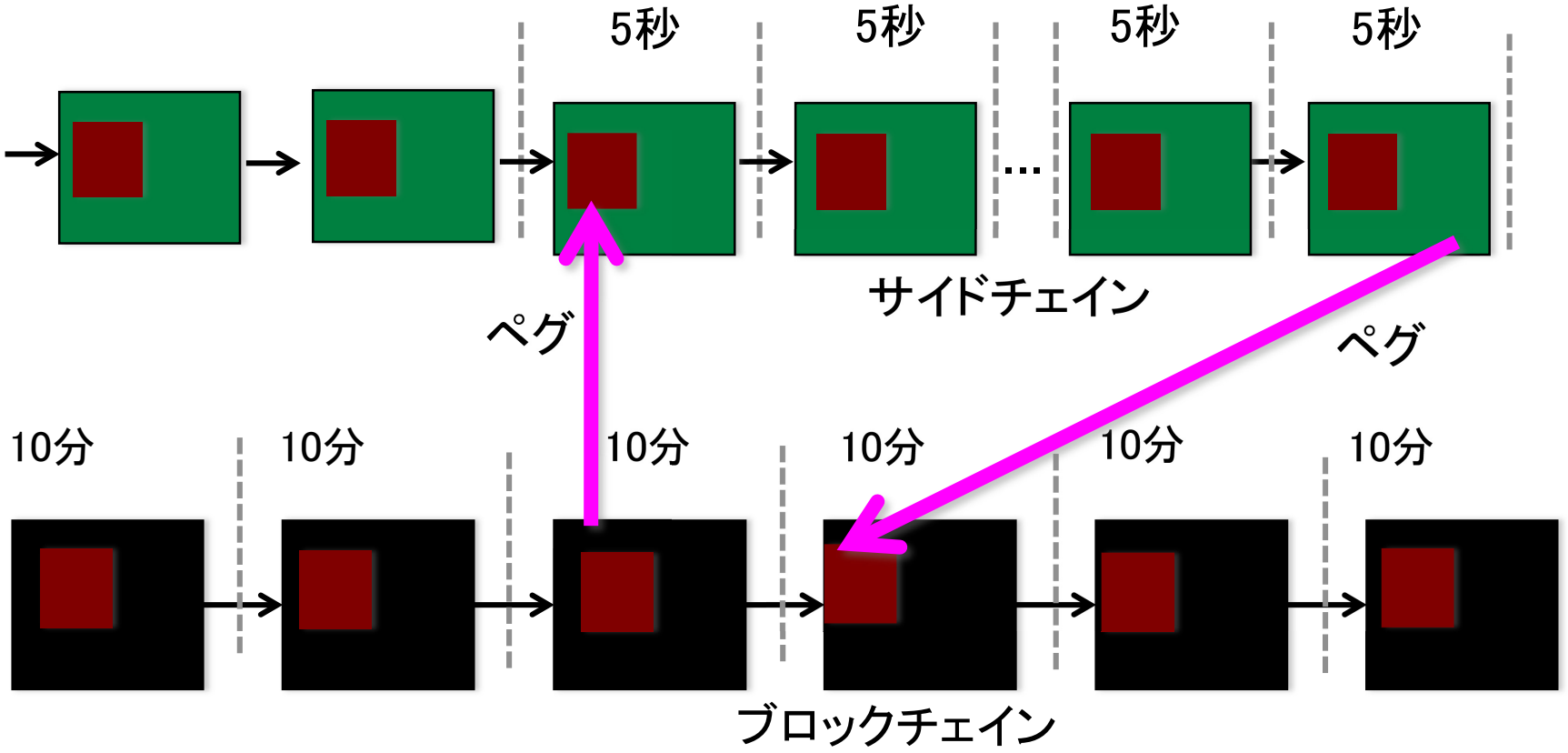
The Block Chainと同様の

「信頼できる記録」



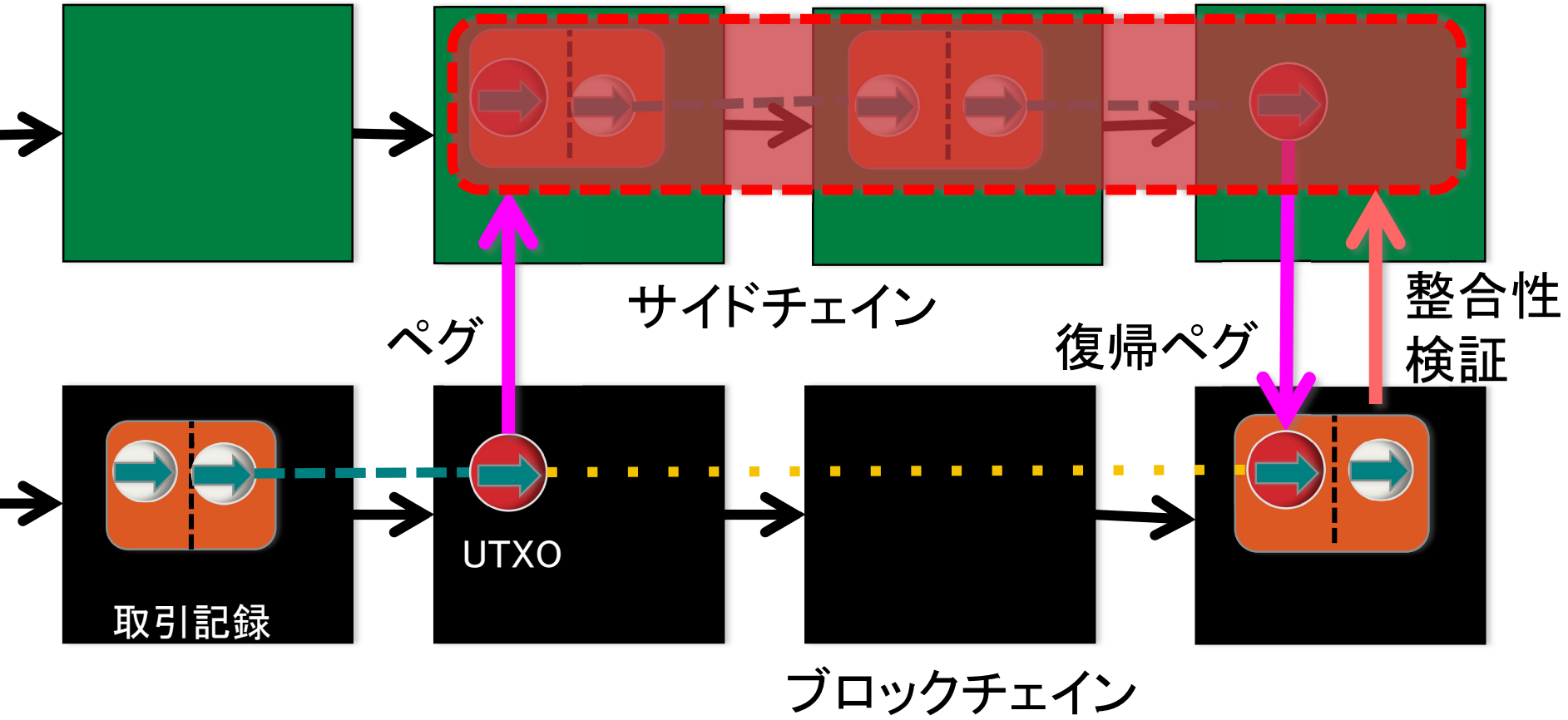
サイドチェインによる決済完了時間の加速

ブロック生成間隔を短くしたサイドチェイン



サイドチェインによる取引内容の隠蔽

復帰時の整合性検証にゼロ知識対話証明



Bitcoinの「コード」の統治

2-way peg型サイドチェーンの実現には

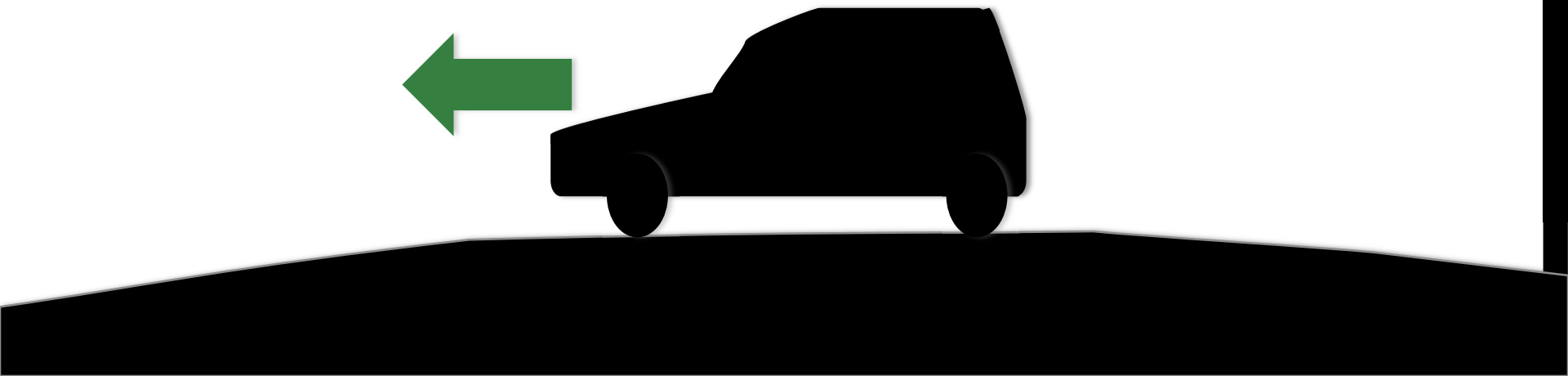
bitcoinの仕様拡張が必要

コードの統治の問題

The Block Chain

車のアクセルを踏んだとき

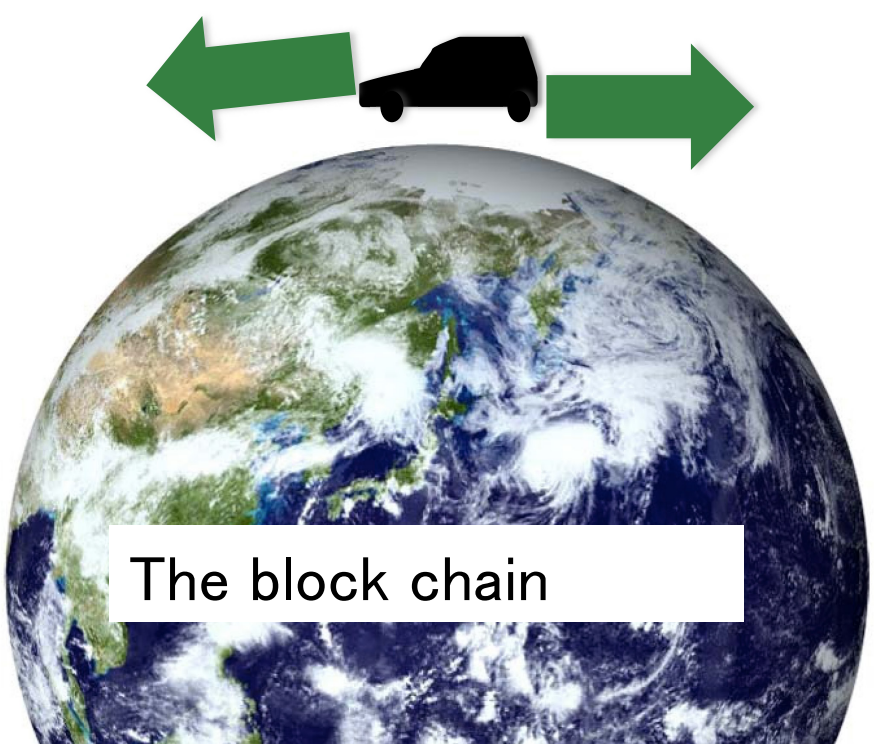
- 自分が加速していると思っている



The Block Chain

反作用で、後ろ向きに地球を回している

Bitcoin売買の反作用 = ボラティリティ



private chain

The Block Chain

ビットコイン経済の規模の拡大による

ボラティリティの減少

The Block Chain

現時点では、

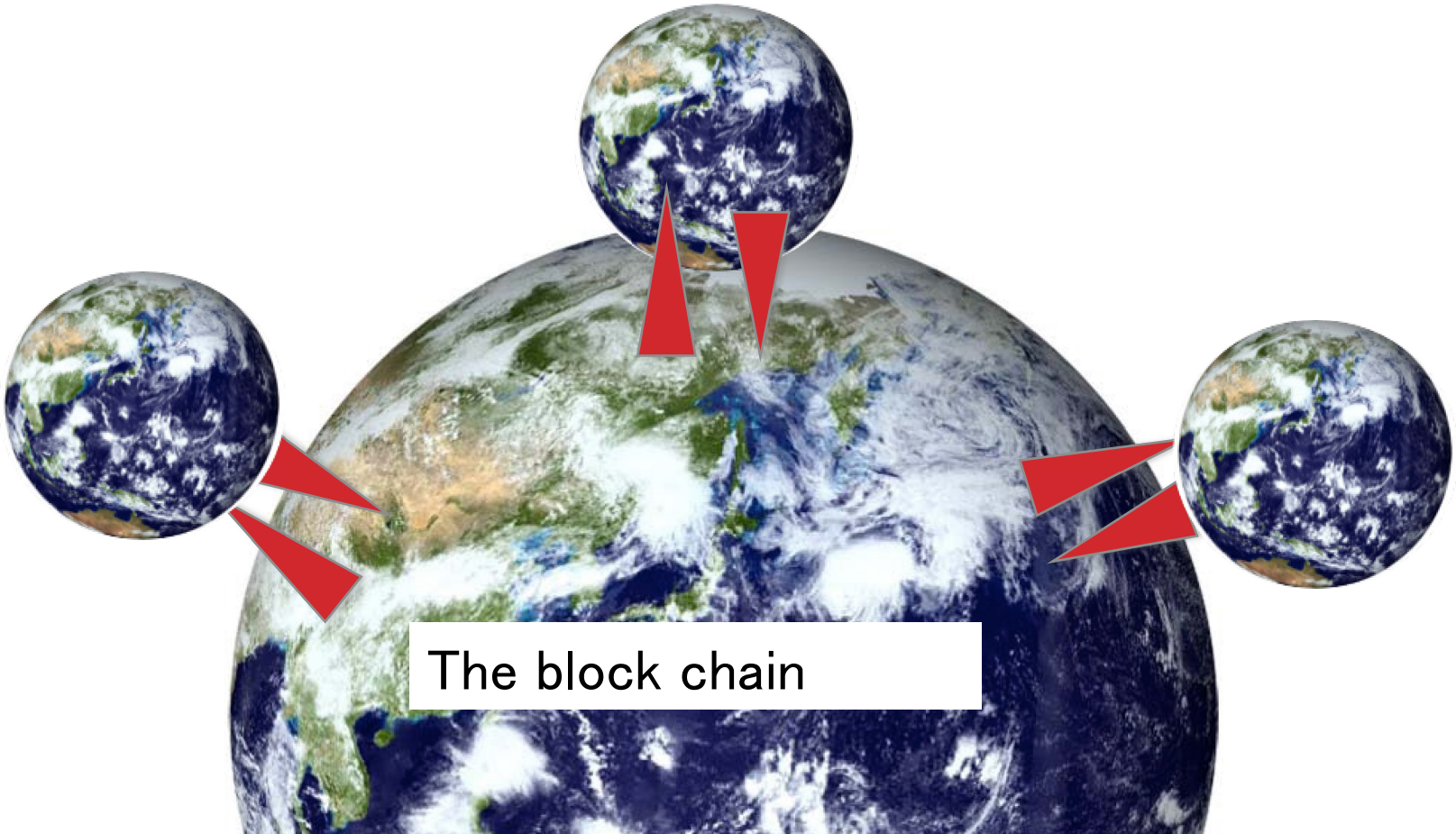
経済活動の大地と呼べるブロックチェイン

はBitcoinのブロックチェインだけ

でも、将来はわからない

2-way peg型サイドチェインによるスケーラビリティ

ペグする方、される方、双方にメリット

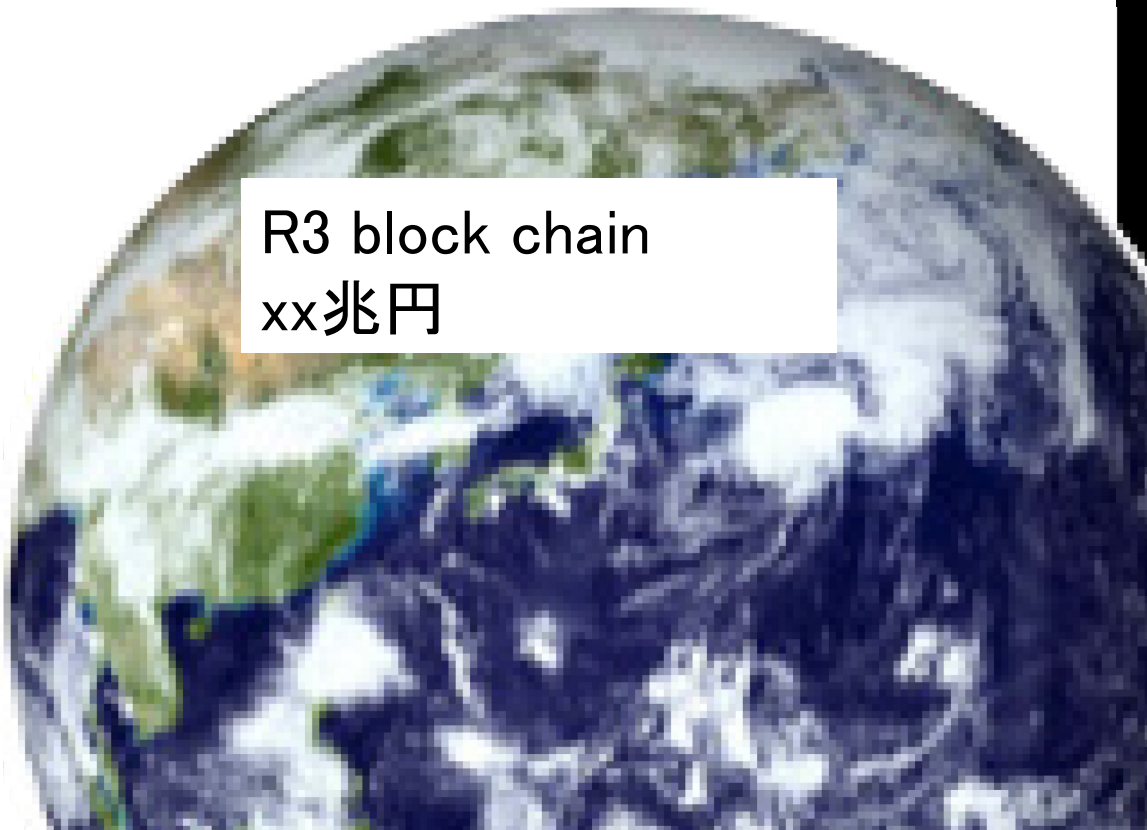


The Block Chain

bitcoin以外のブロックチェインが
巨大な大地になる可能性もある

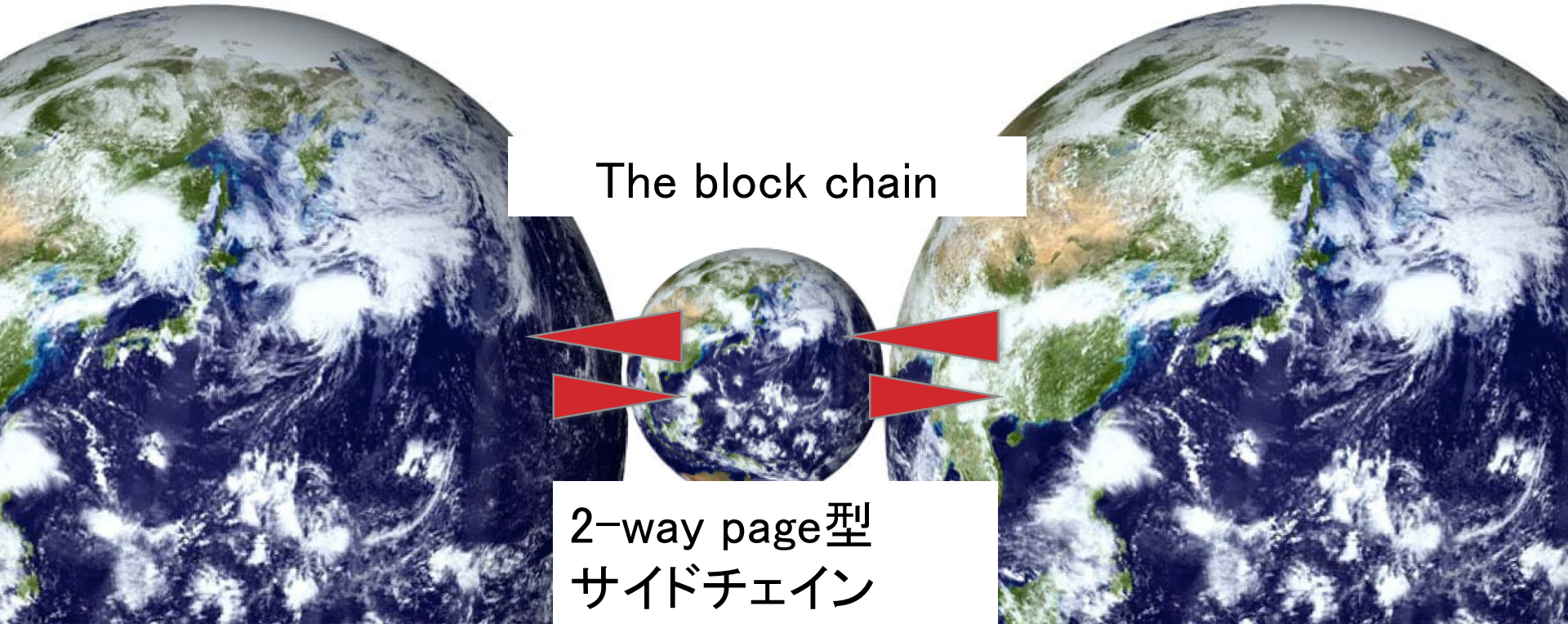
The block chain
6000億円

R3 block chain
xx兆円



The Block Chain

bitcoin以外のブロックチェインが
ハブになる可能性もある？



サイドチェイン技術

これから生態系が発展するでしょう

The block chainとの共生も

□

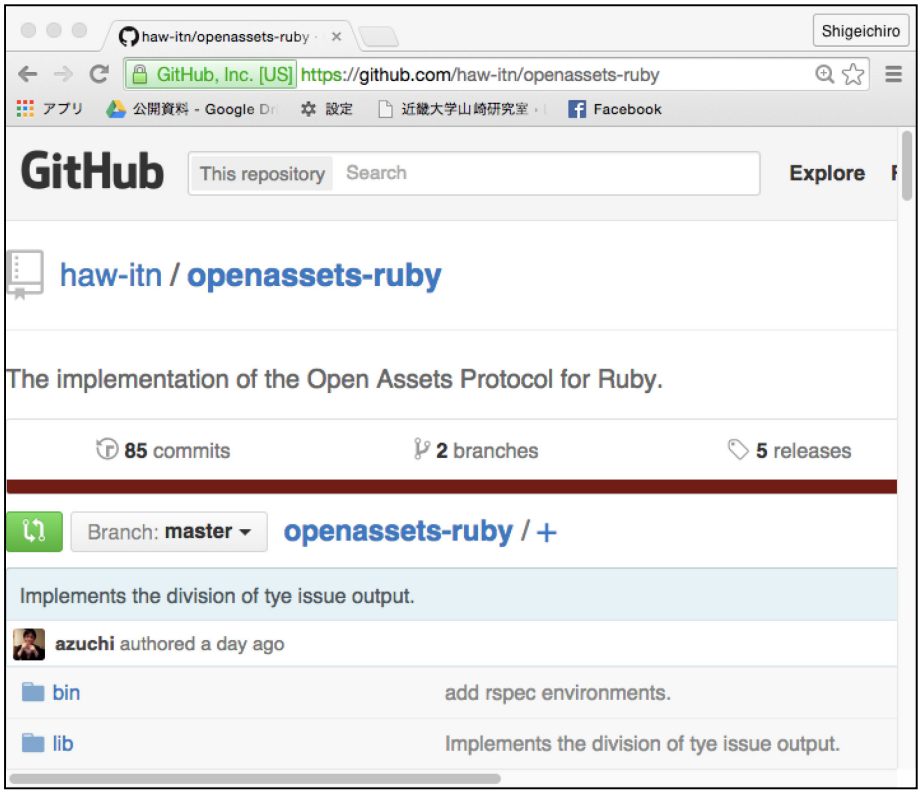
でも、技術的に未解決の問題も多数存在

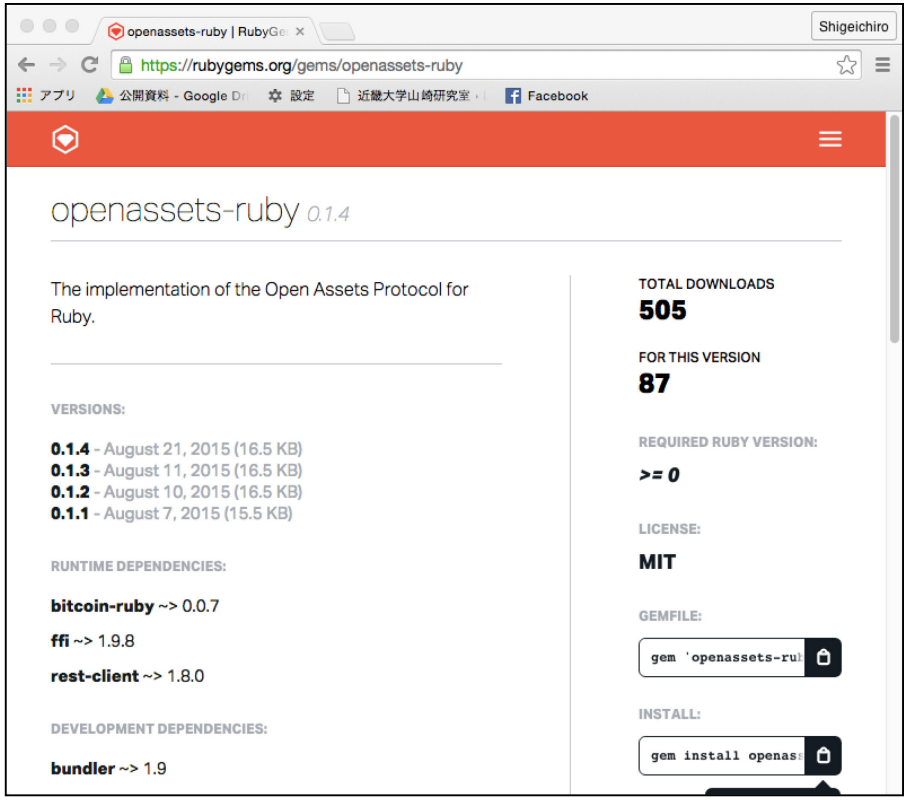
当面は、The block chain上で

アセットを定義する技術が実用的では

Open Assetsの独自実装 openasset-ruby

ハウ・インターナショナルさん開発





dis-embedding

ブロックチェイン技術の本質

体制に埋め込まれていたシステムを浮上させ
コードによる統治を行う

対象は経済システムだけでない
ブロックチェイン・ボーティング

北九州からあげ王者選手権

日本初のブロックチェイン投票実験

2015年8月29日、30日