ビットコインとはなんだったのか

仮想通貨とサイバー取引の現在

国立情報学研究所
情報社会相関研究系
岡田 仁志

本日の論題

1. 仮想通貨の仕組みと制度上の課題について数式を使わずにご説明します。
2. 仮想通貨の取引所が取引を停止した際に、消えたビットコインの行方を追います。
3. 海外における通貨発行自由化の議論に学び、仮想通貨の将来を論じます。

Jason Benjamin

ビットコインとは何か？

オリジナル論文

Satoshi Nakamoto (仮名)

Bitcoin: A Peer-to-Peer Electronic Cash System,

2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

信頼できる第三者機関
が存在しなくても
インターネット上を
流通する電子的価値

を、政府の力を借りずに実現する。

ソフトウェアだけで実現されている

主なbitcoinウォレット

Desktop wallets

Desktop wallets are installed on your computer. They give you complete control over your wallet. You are responsible for protecting your money and doing backups.

Bitcoin Core

MultiBit

Hive

Armory

Electrum

Mobile wallets

Mobile wallets allow you to bring Bitcoin with you in your pocket. You can exchange bitcoins easily and pay in physical stores by scanning a QR code or using NFC "tap to pay".

Bitcoin Wallet

iPhone
bitWallet
送金機能なし！

Web wallets

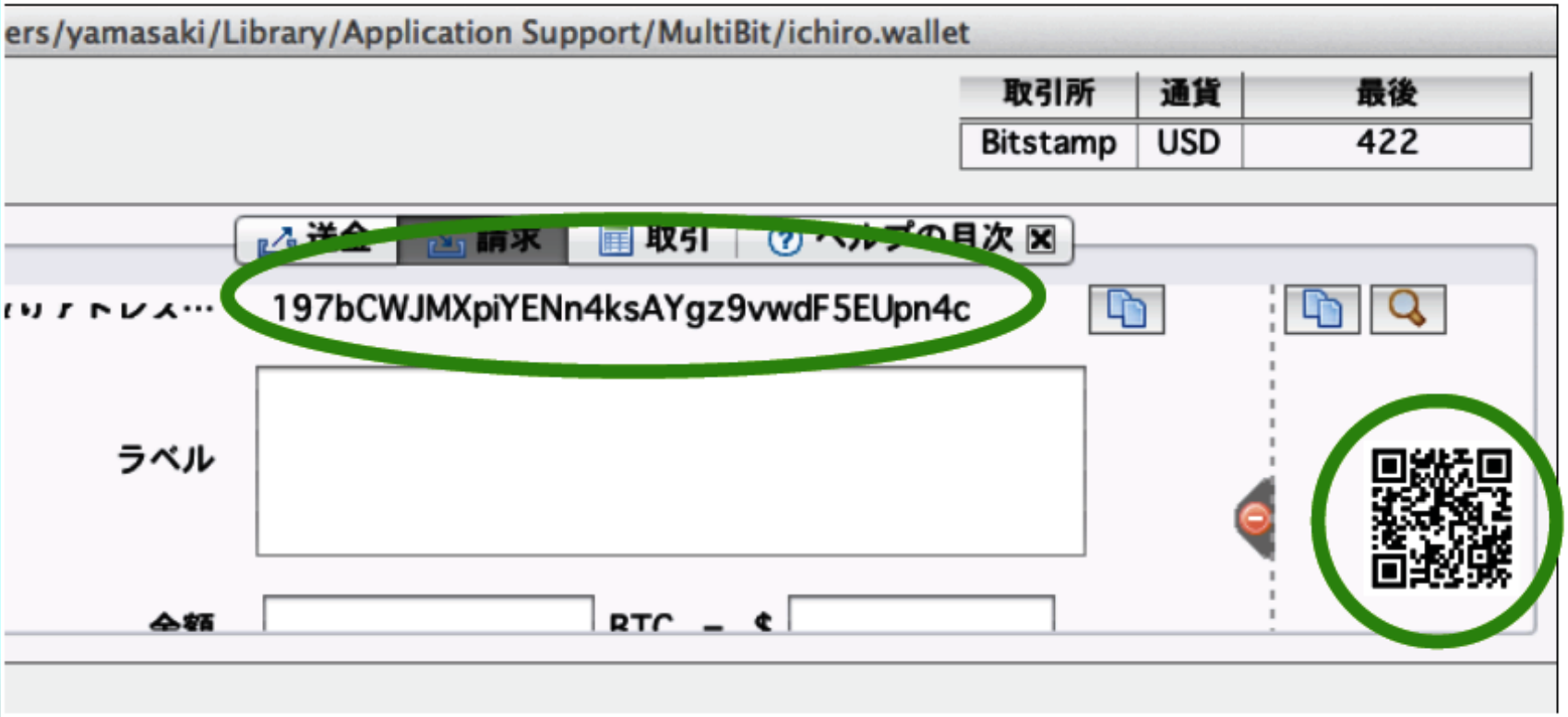
Web wallets allow you to use Bitcoin on any browser or mobile and often offer additional services. However, you must choose your web wallet with care as they host your bitcoins.

使い方は電子メールと同様

bitcoinウォレットの使い方

- bitcoinを受け取る

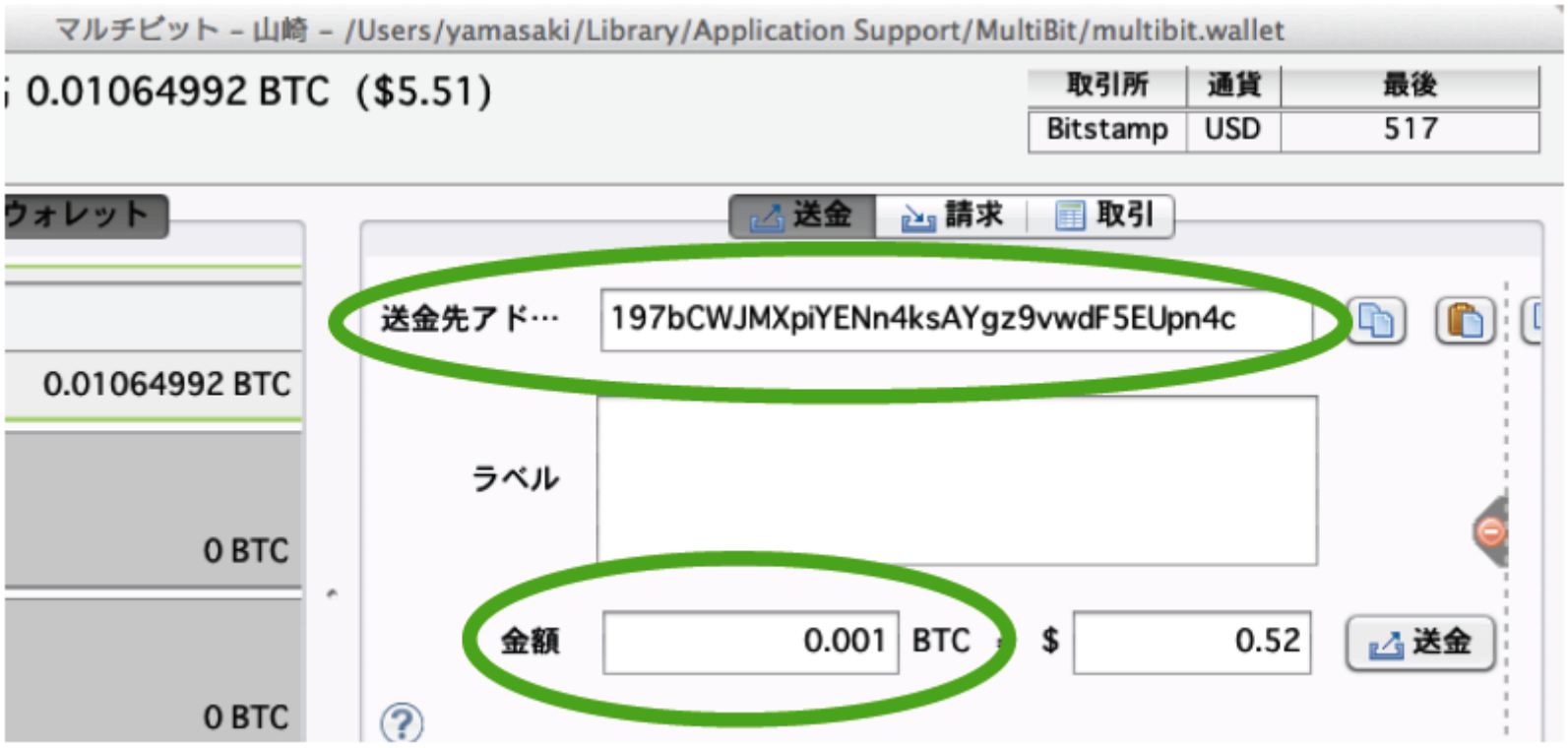
自分のbitcoinアドレスを相手に教える



bitcoinウォレットの使い方

- bitcoinを送金する

相手のbitcoinアドレスと金額を入れて送金

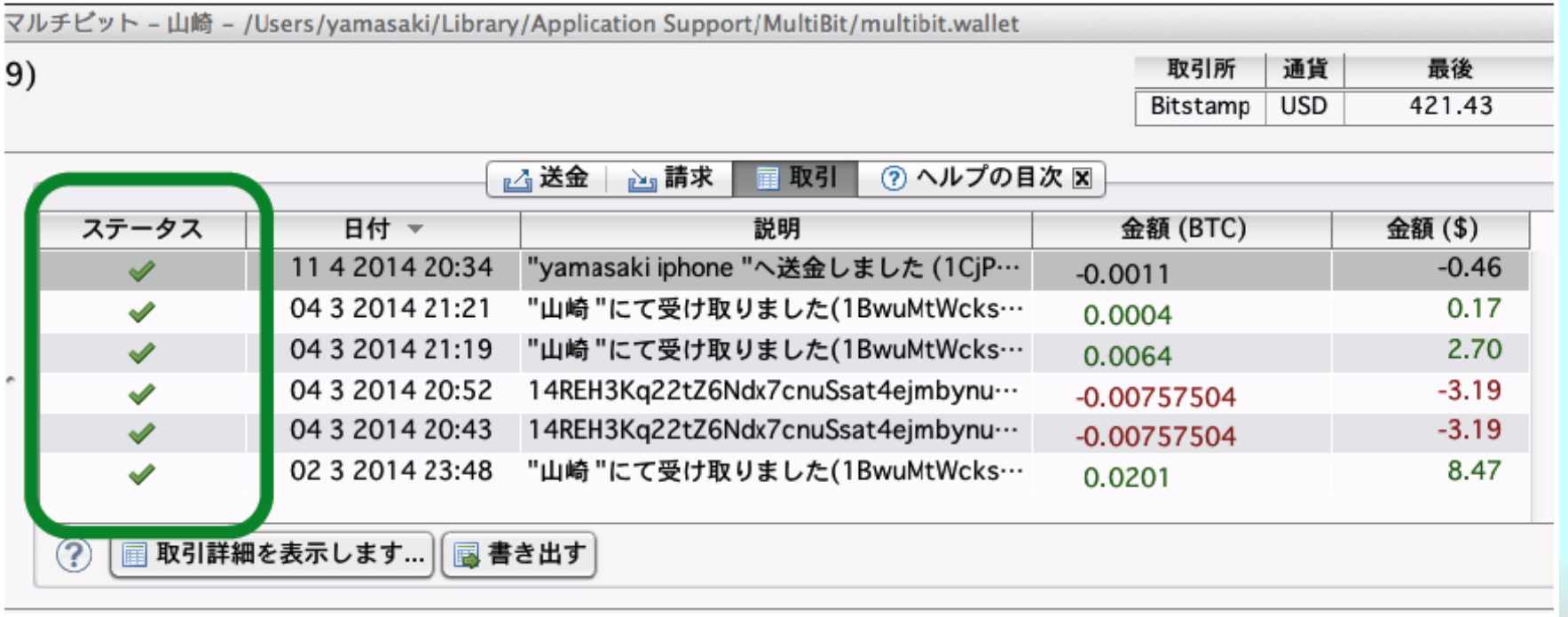


bitcoinウォレットの使い方

取引履歴の確認

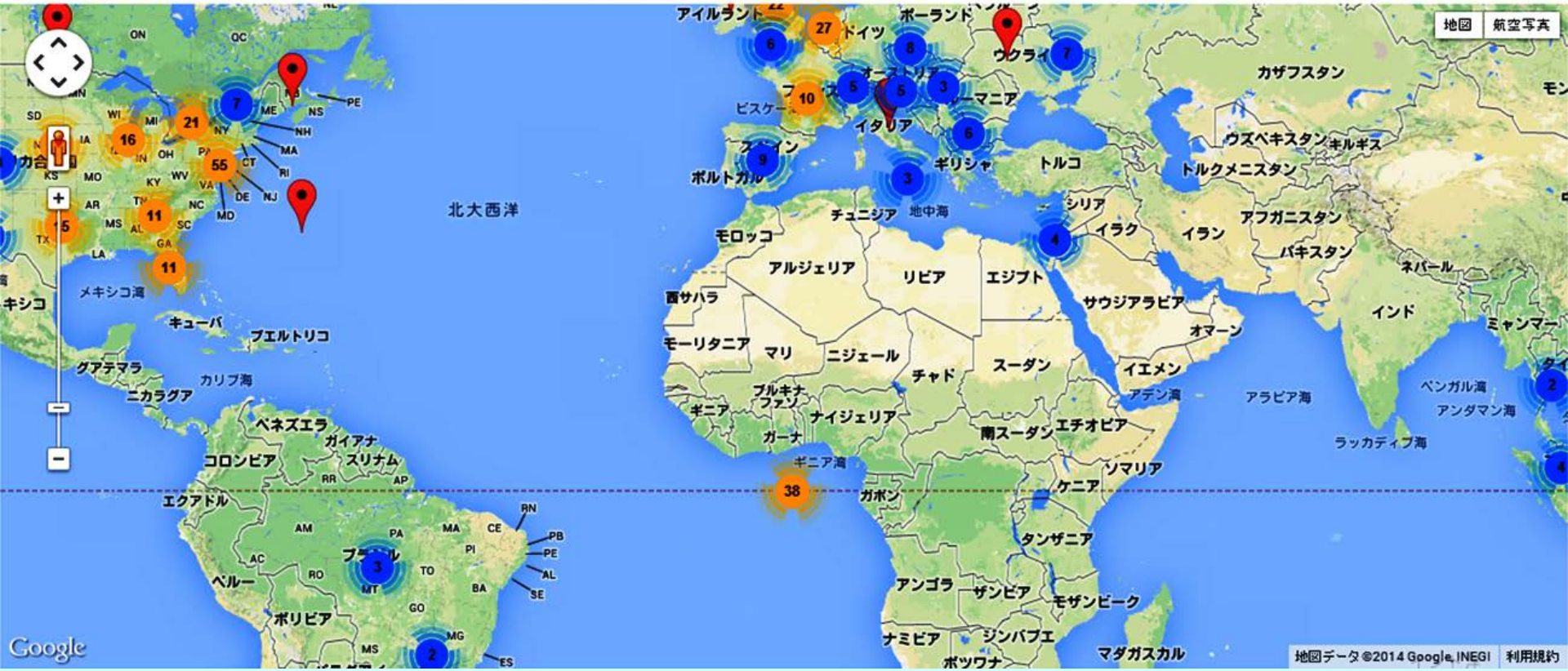
日時、アドレス、金額、ステータス（確認済みか？）

ステータスが確認済みなら、次の支払いに使用できる



Network Propagation ネットワーク全体の取引やブロックの分布を表示します

Inventory Hash: 5fd20deaa35a6d6b69102a3c7b46b2eb8df6035a6f126c141d32236c2c3701cd

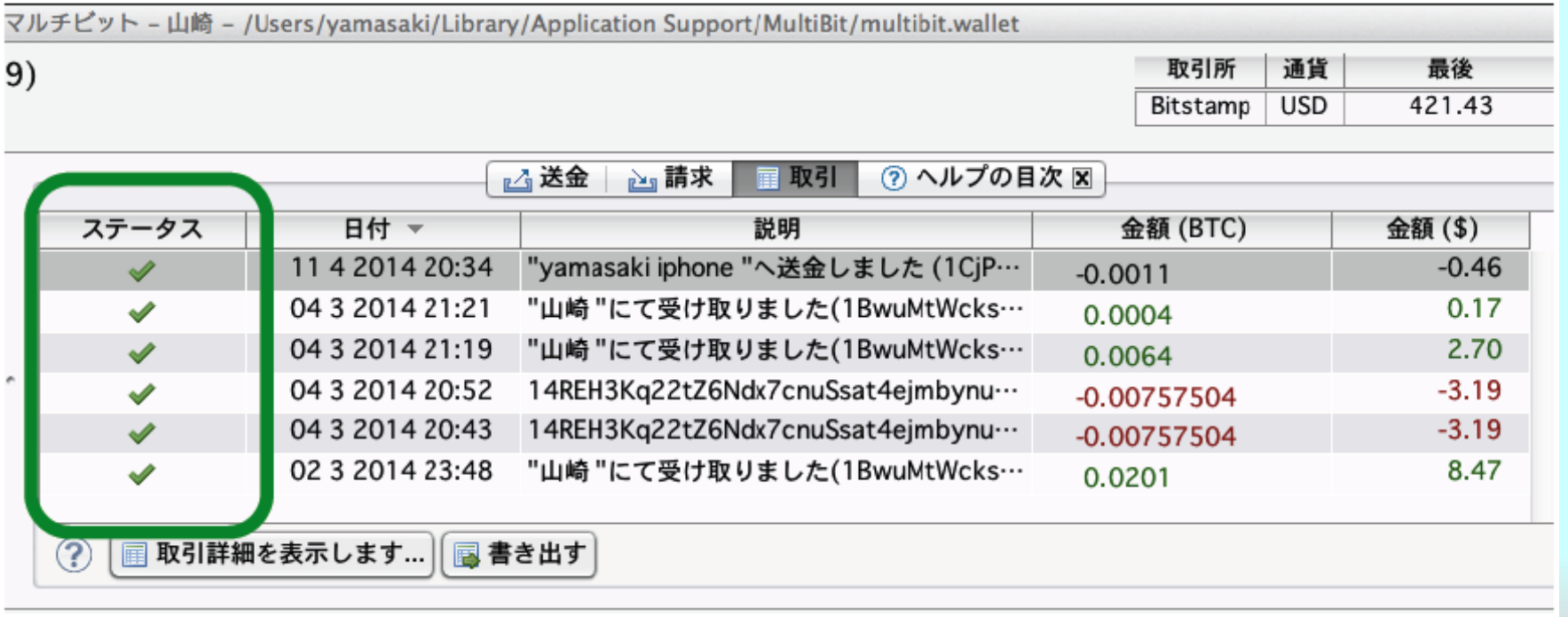


https://blockchain.info/

どこで手に入れるの？

bitcoinウォレットの使い方

親切な友人に送金してもらう。



交換所

Duncan Rawlinson

ATM

CC BY NC Duncan Rawlinson

ビットコインATM設置例

Halans BitRockets ATM

BY NC SA

Halans BitRockets ATM

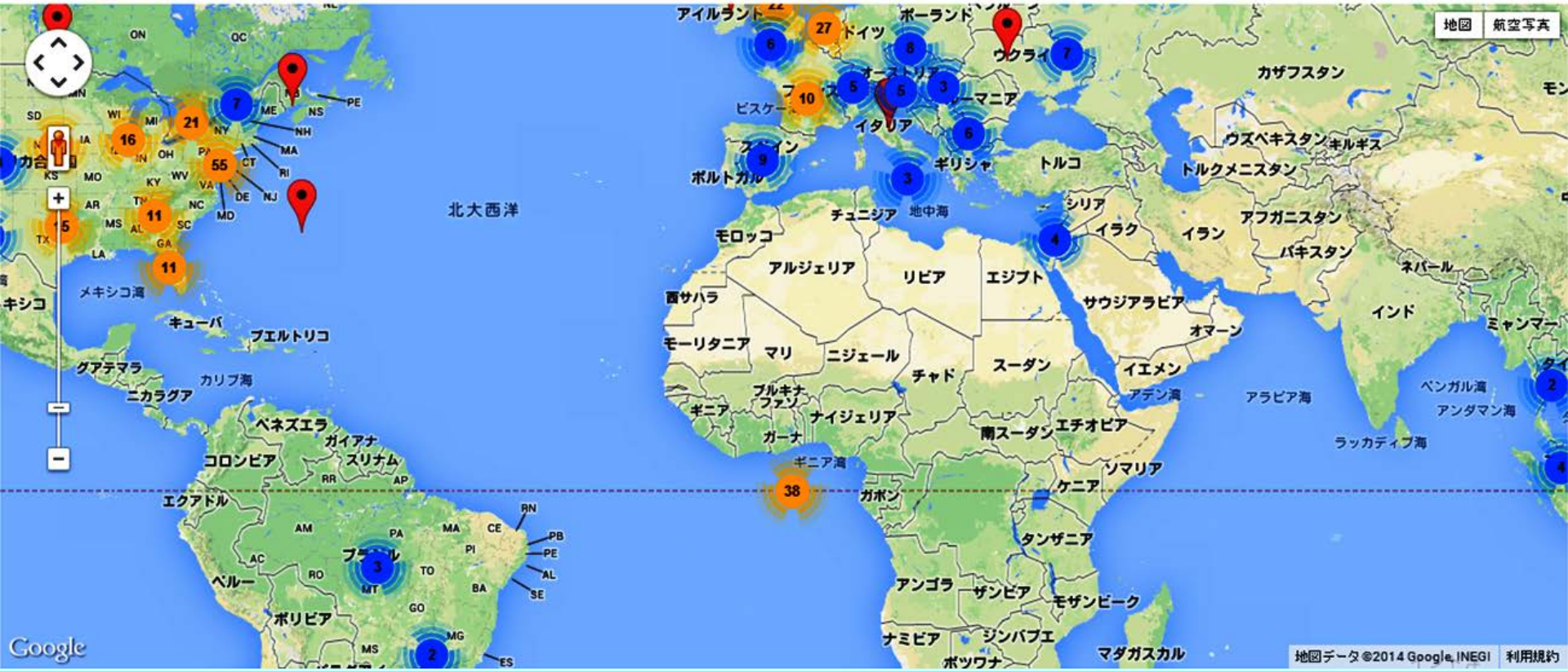
Philip MG5928

どこで使えるの？

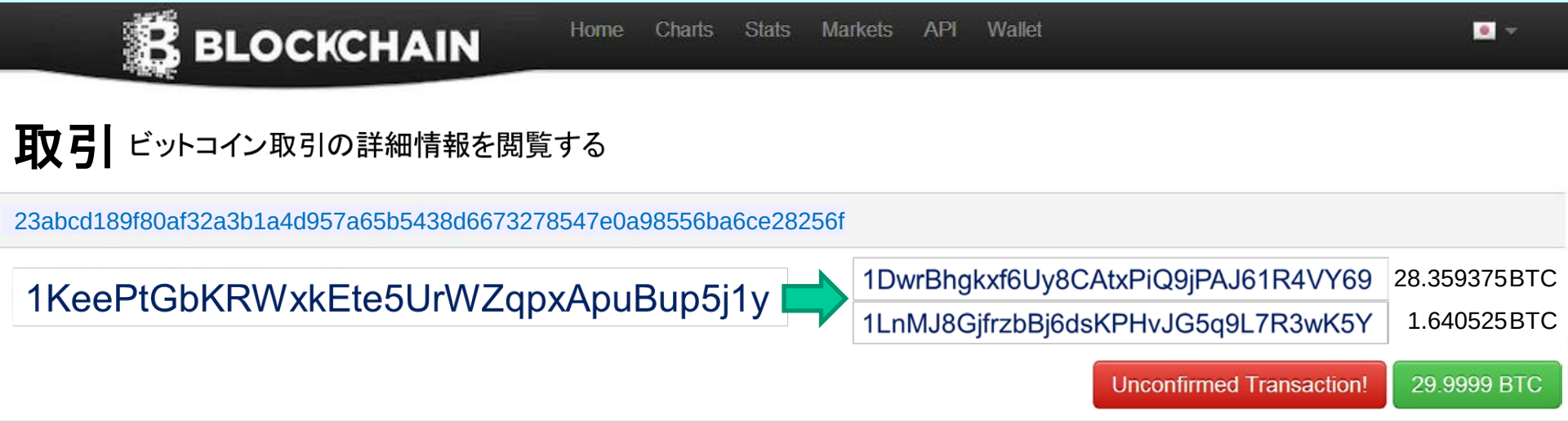
海外送金

Network Propagation ネットワーク全体の取引やブロックの分布を表示します

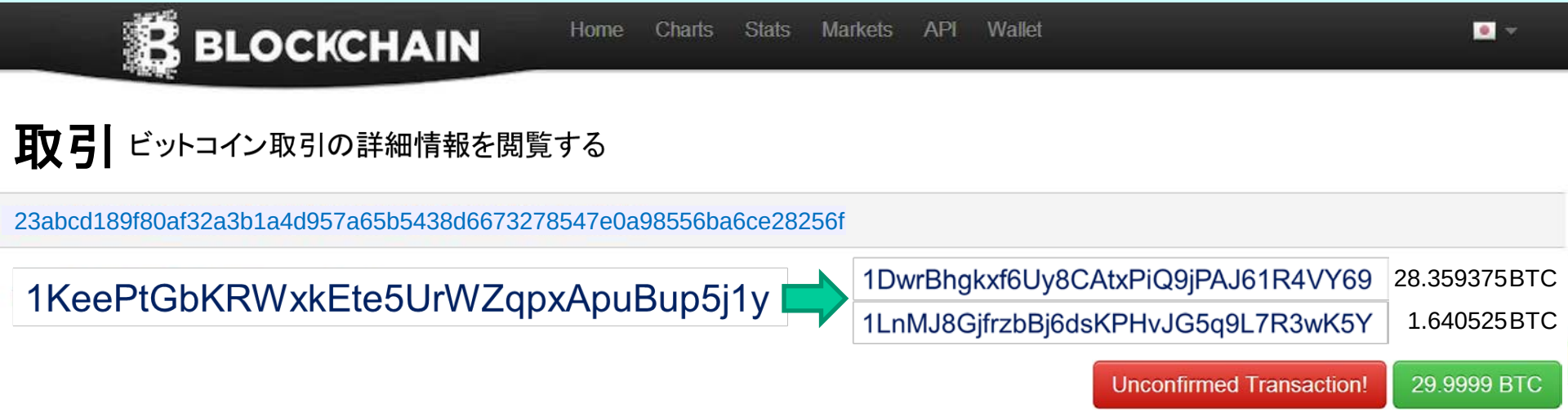
Inventory Hash: 5fd20deaa35a6d6b69102a3c7b46b2eb8df6035a6f126c141d32236c2c3701cd



https://blockchain.info/



https://blockchain.info/



FEE 0.0001 BTC

29.9999 BTC

編注）修正しました。(誤) 0.001 BTC⇒（正）0.0001 BTC

海外送金手数料 6円12銭

補注）1BTC=61,200円で換算

店頭支払

Cory Doctorow

Jason Tester Guerrilla Futures (上)

ビットコインでの支払はQRコードをスキャンして、当店のアカウントへ送金してください。

Duncan Rawlinson (左)

ここで使えます。

CoinDesk

仮想通貨の歴史

BLOCKCHAIN
Home
Charts
Stats
Markets
API
Wallet
Search
Market Price (USD)
ソース：blockchain.info
1,400
1,200
1,000
800
600
400
200
0
Market Price (USD)
2009年スタート
Jul '12
Sep '12
Nov '12
Jan '13
Mar '13
May '13
Jul '13
Sep '13
Nov '13
Jan '14
Mar '14
May '14
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - 全期間
Logarithmic Scale - 7 day average - データポイントの表示 - (CSV - JSON)

BLOCKCHAIN
Home
Charts
Stats
Markets
API
Wallet
Search
Market Price (USD)
ソース：blockchain.info
1,400
1,200
1,000
800
600
400
200
0
Market Price (USD)
GEEK達の実験
Market Price (USD) 6
Jul '12
Sep '12
Nov '12
Jan '13
Mar '13
May '13
Jul '13
Sep '13
Nov '13
Jan '14
Mar '14
May '14
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - 全期間
Logarithmic Scale - 7 day average - データポイントの表示 - (CSV - JSON)

vmax137

vmax137

BLOCKCHAIN
Home
Charts
Stats
Markets
API
Wallet
Search
Market Price (USD)
ソース：blockchain.info
1,400
1,200
1,000
800
600
400
200
0
Market Price (USD)
キプロス財政破綻
Market Price (USD) 238
Jul '12
Sep '12
Nov '12
Jan '13
Mar '13
May '13
Jul '13
Sep '13
Nov '13
Jan '14
Mar '14
May '14
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - 全期間
Logarithmic Scale - 7 day average - データポイントの表示 - (CSV - JSON)

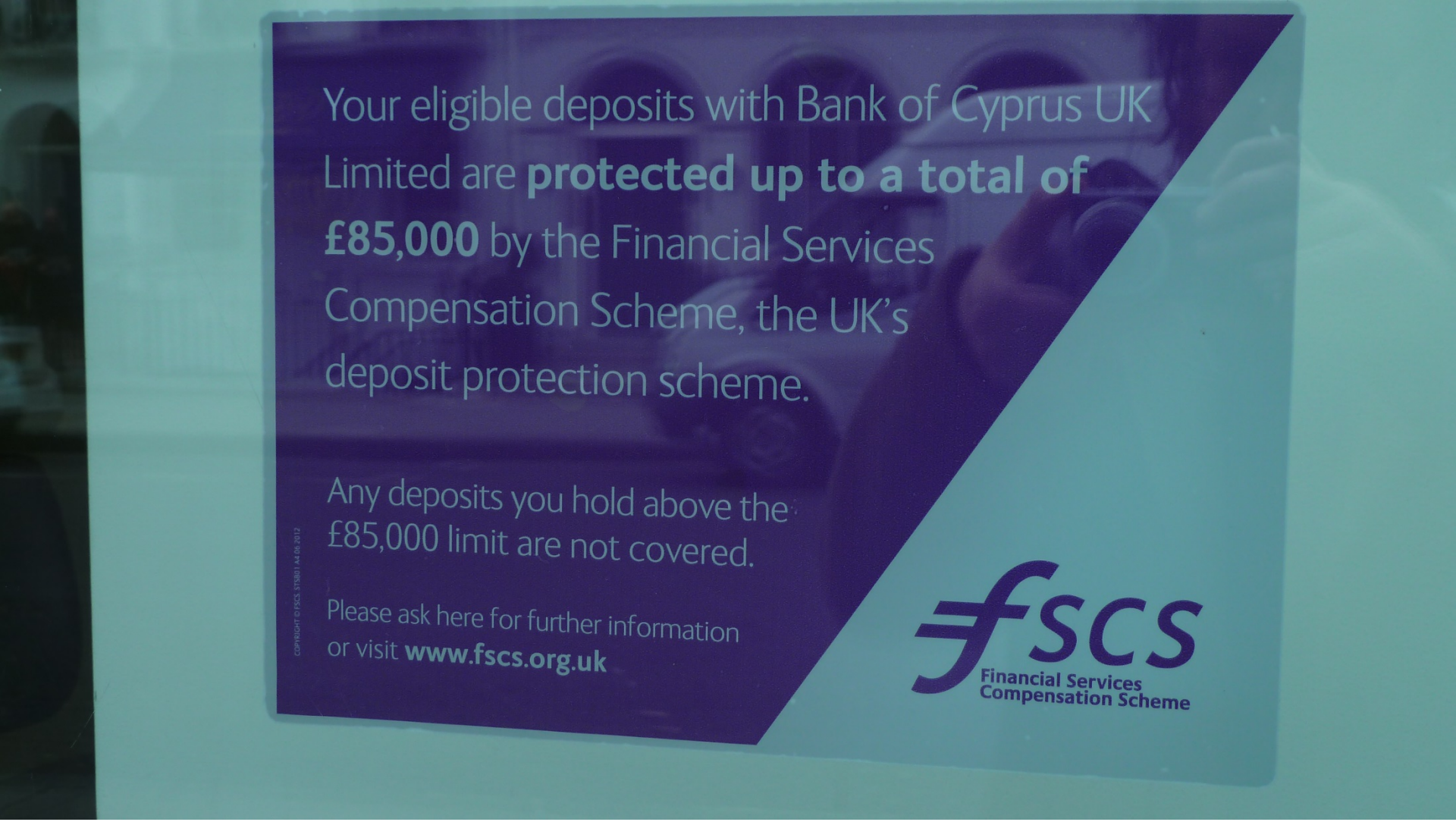
κύριασity (左)

経営破綻したキプロスの銀行（英国の支店）

Popicinio (右)

心配して集まった人々
（キプロス共和国）
2013年3月

キプロス銀行の支店と集まった人々



London Permaculture

キプロス銀行英国支店の預金払戻し保護上限額を 85,000ポンドに制限することを告知する貼り紙。 (英国金融サービス庁)

BLOCKCHAIN
Home
Charts
Stats
Markets
API
Wallet
Search
Market Price (USD)
ソース：blockchain.info
Market Price (USD) 1,151
中国で理財ブーム
Market Price (USD)
1,400
1,200
1,000
800
600
400
200
0
Jul '12
Sep '12
Nov '12
Jan '13
Mar '13
May '13
Jul '13
Sep '13
Nov '13
Jan '14
Mar '14
May '14
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - 全期間
Logarithmic Scale - 7 day average - データポイントの表示 - (CSV - JSON)

Philip

（左上・右上）中国の仮想貨幣交換所広告

（左）中国で開催された仮想貨幣研討会

Chris Price

BLOCKCHAIN Home Charts Stats Markets API Wallet Search

30 Days - 60 Days - 180 Days - 1 Year - 2 Year - 全期間

Logarithmic Scale - 7 day average - データポイントの表示 - (CSV - JSON)

仮想通貨の使い道

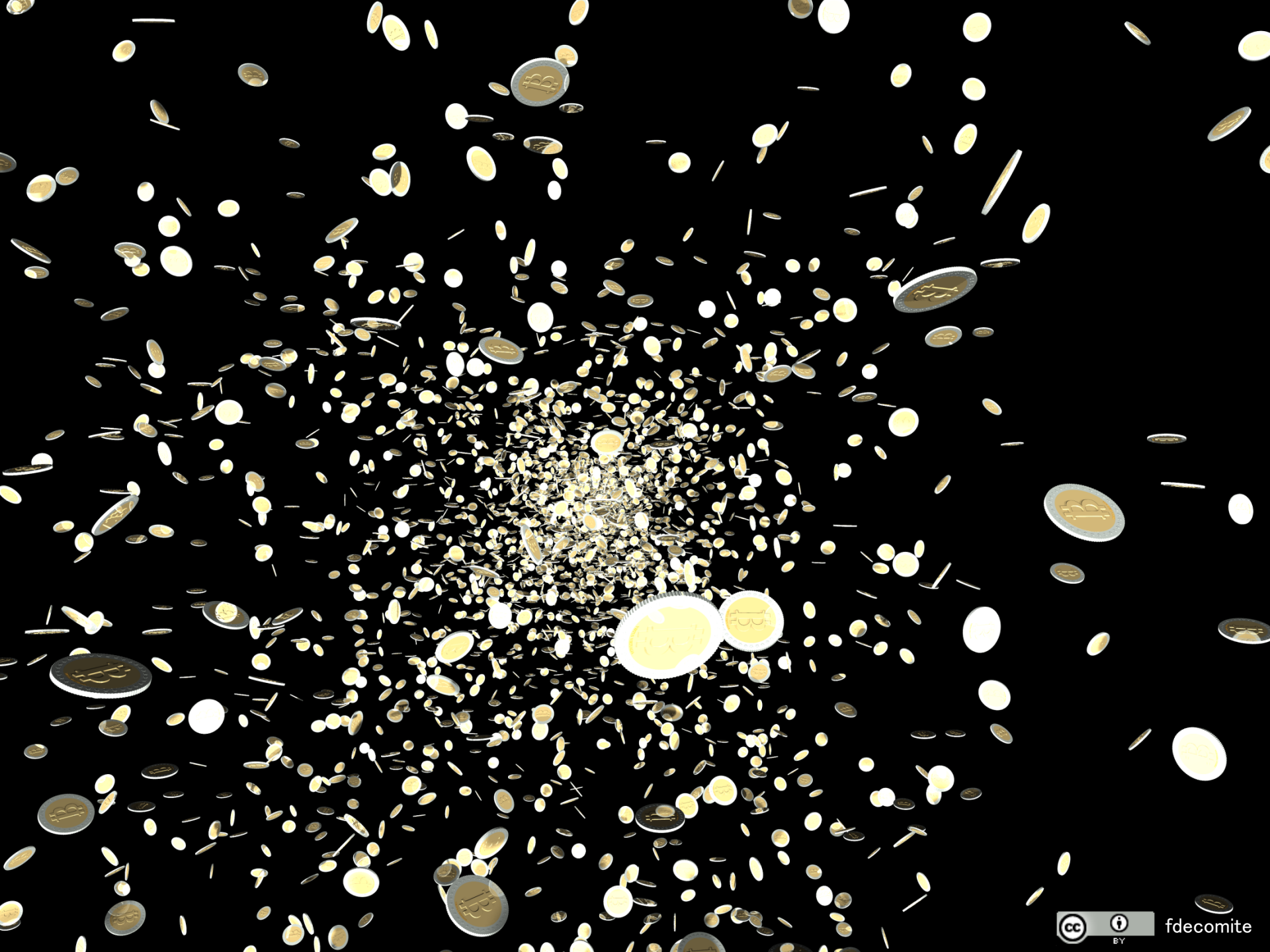
海外への送金

店舗での支払

投資と投機

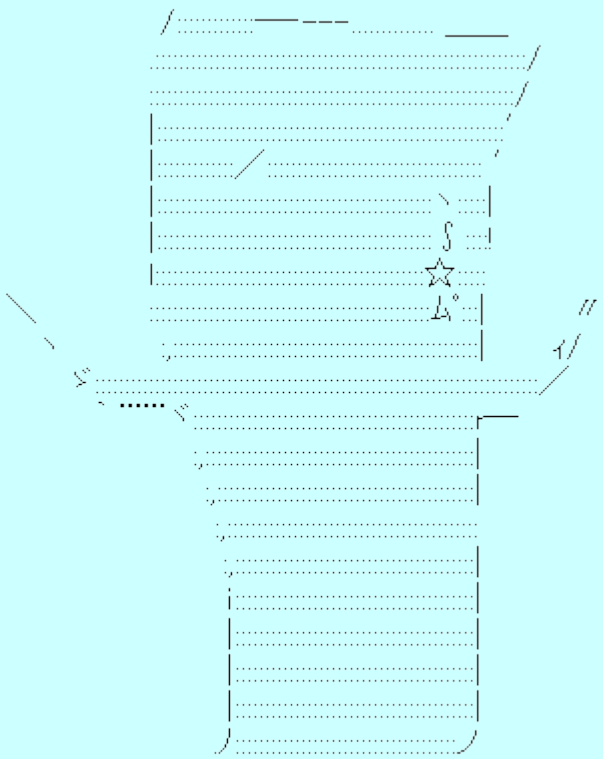
BLOCKCHAIN
Home
Charts
Stats
Markets
API
Wallet
Search
Market Price (USD)
ソース：blockchain.info
1,400
1,200
1,000
800
600
400
200
0
Market Price (USD)
MT.GOXが破綻
Market Price (USD) 528
Jul '12
Sep '12
Nov '12
Jan '13
Mar '13
May '13
Jul '13
Sep '13
Nov '13
Jan '14
Mar '14
May '14
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - 全期間
Logarithmic Scale - 7 day average - データポイントの表示 - (CSV - JSON)

ykanazawa1999


fdecomite

仮想通貨に実体はあるか

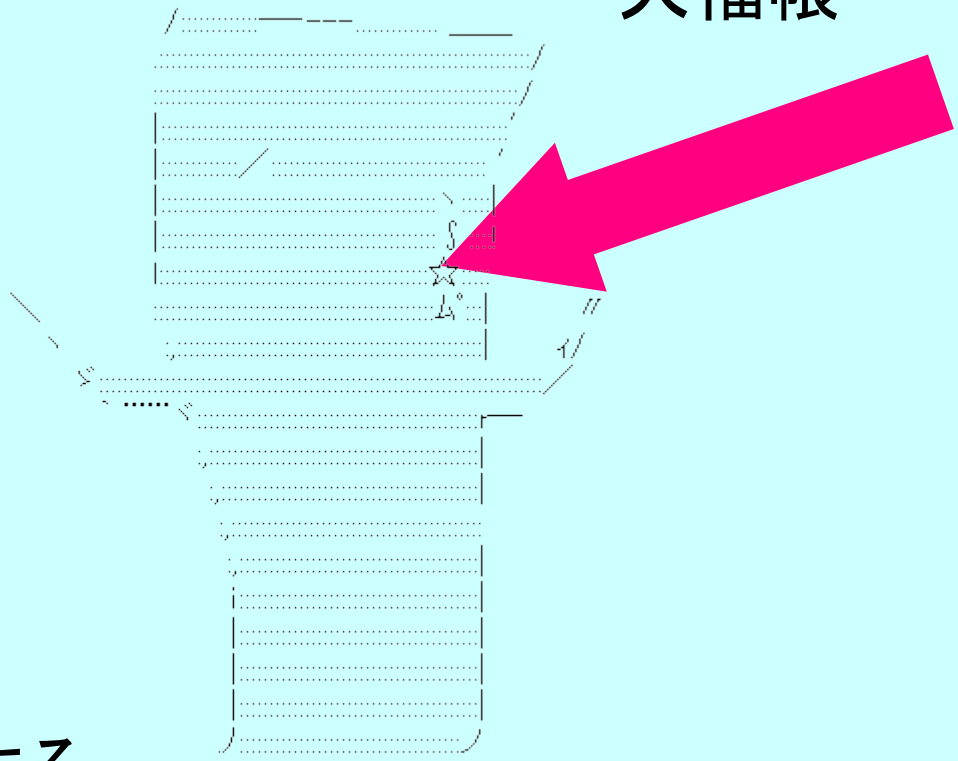
ビットコインとは



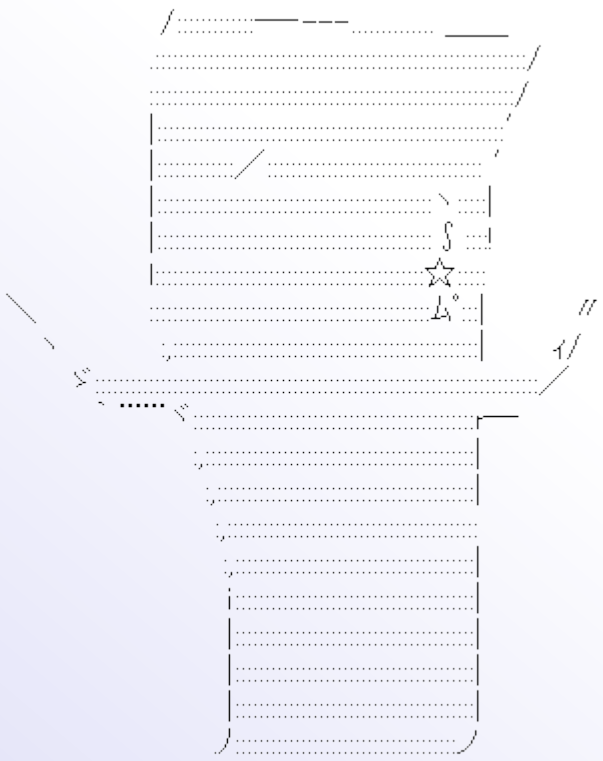
CC BY

http://aa.ja.utf8art.com/node/5684

見える人にだけ見える
大福帳



大福帳を管理する
銀行みたいなものはない



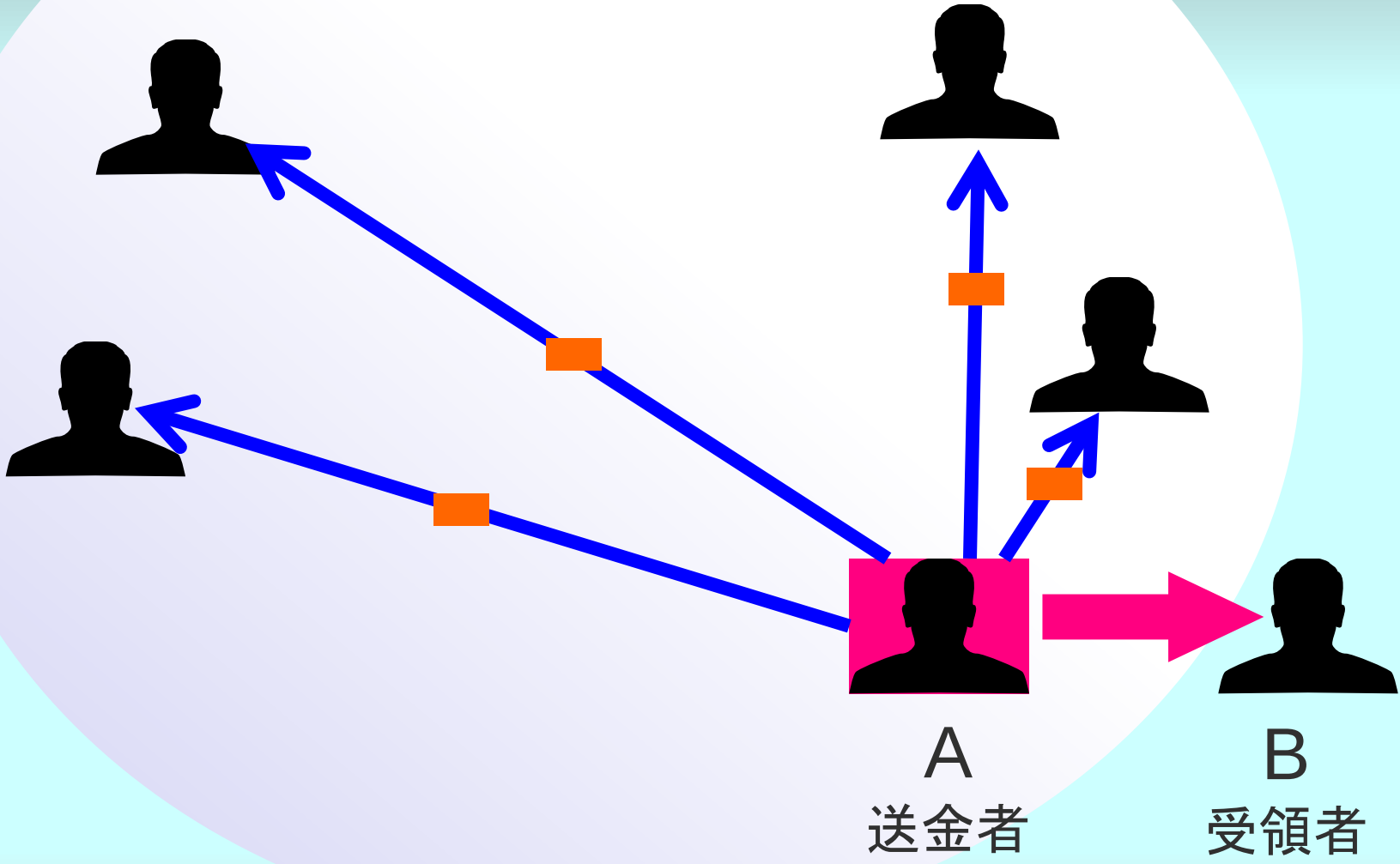
取引の記録

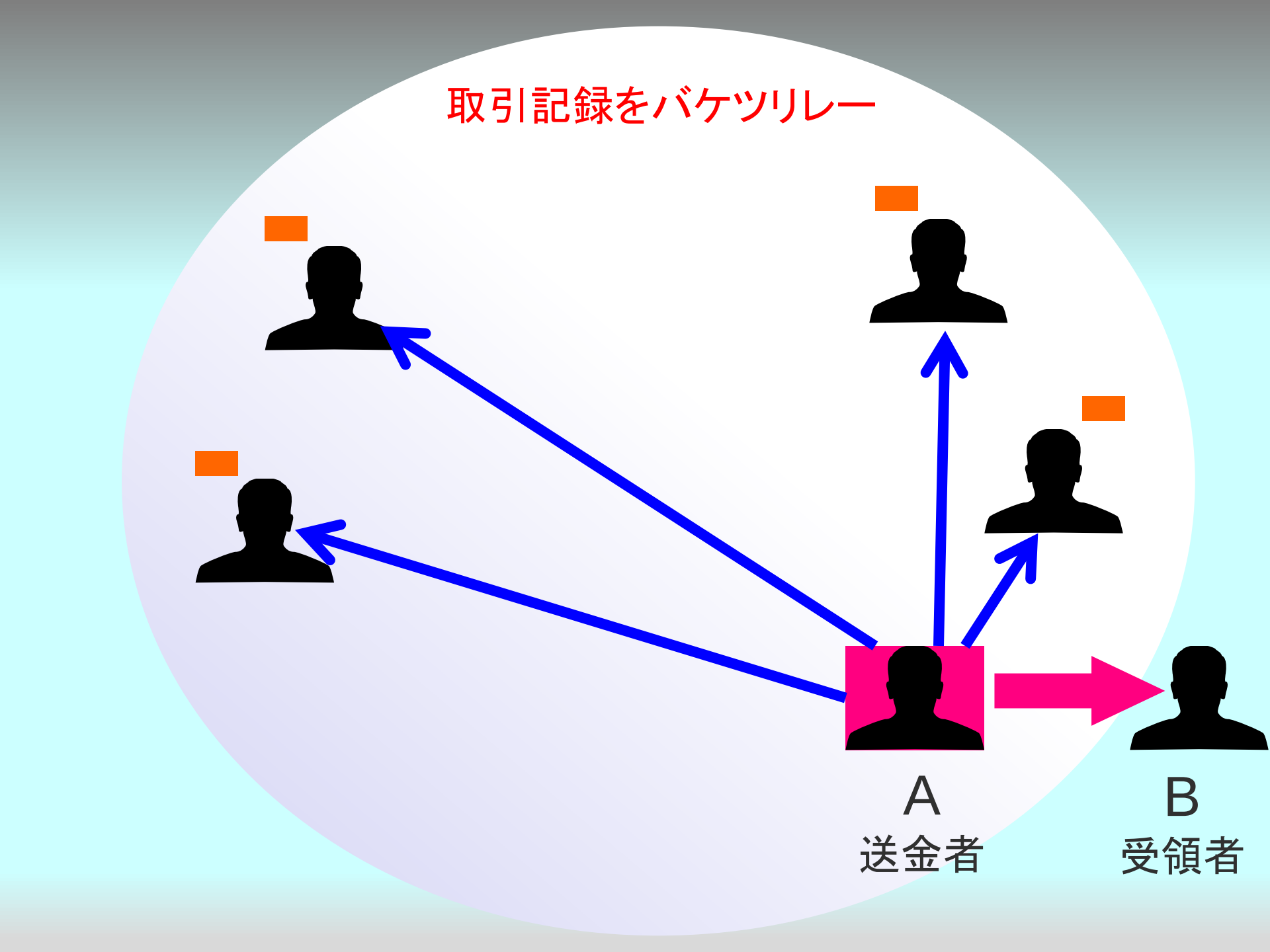
AがBに5.0BTC支払った

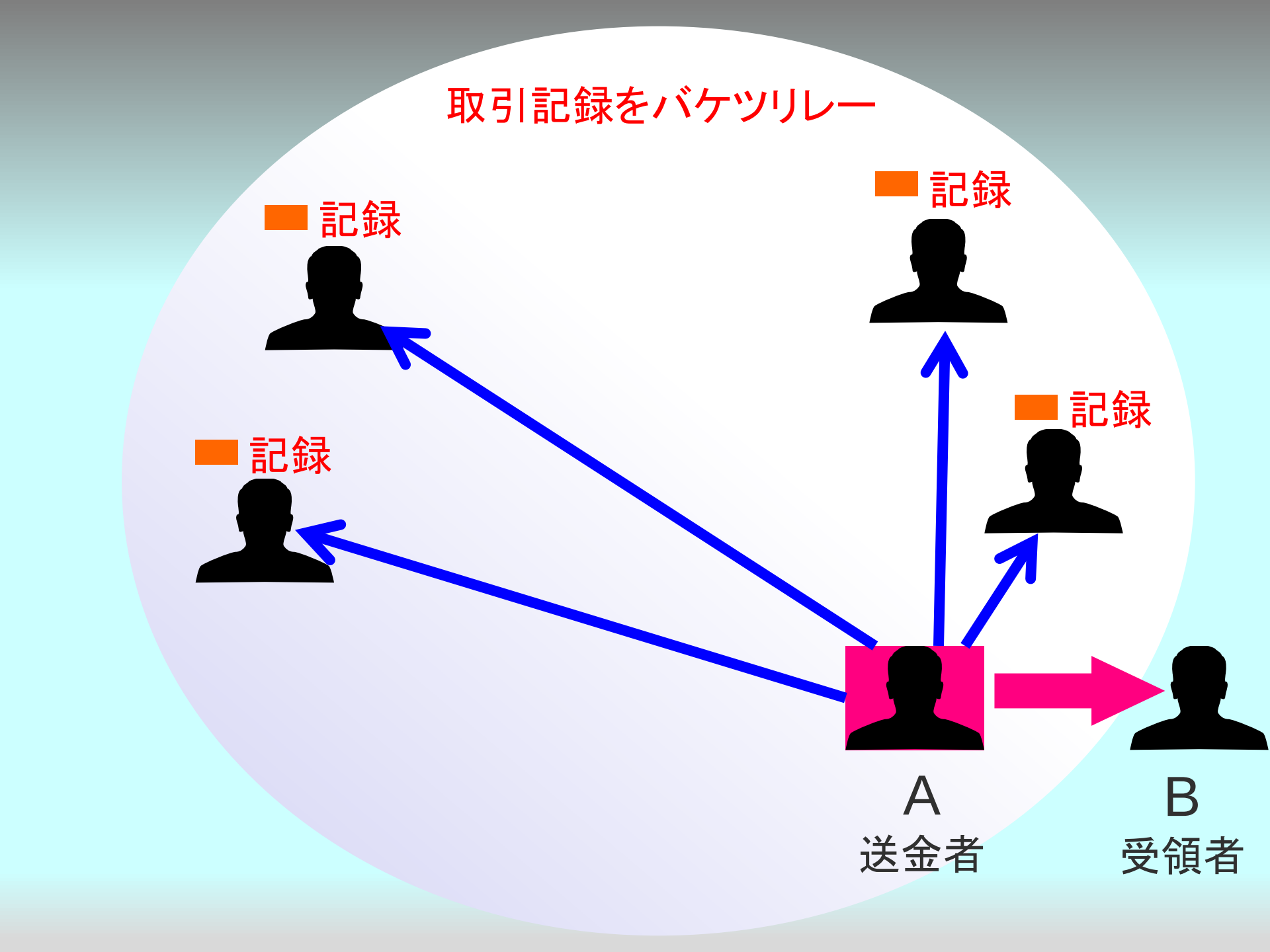
A
送金者

B
受領者

◆ 取引記録をバケツリレー

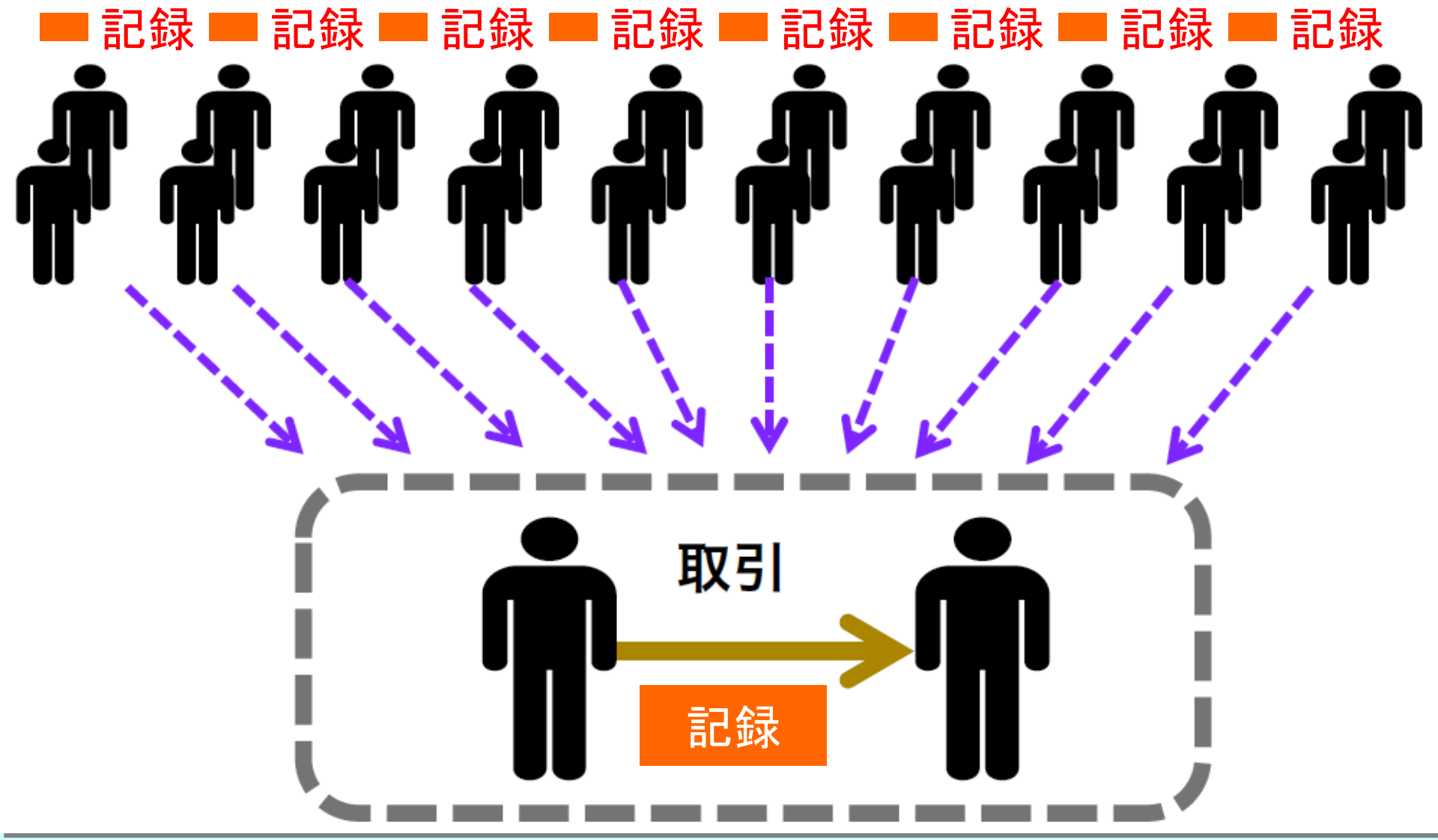



取引記録をバケツリレー
A
送金者
B
受領者


取引記録をバケツリレー
記録
記録
記録
記録
A
送金者
B
受領者

みんなの記憶

みんなの記憶は結構正しい

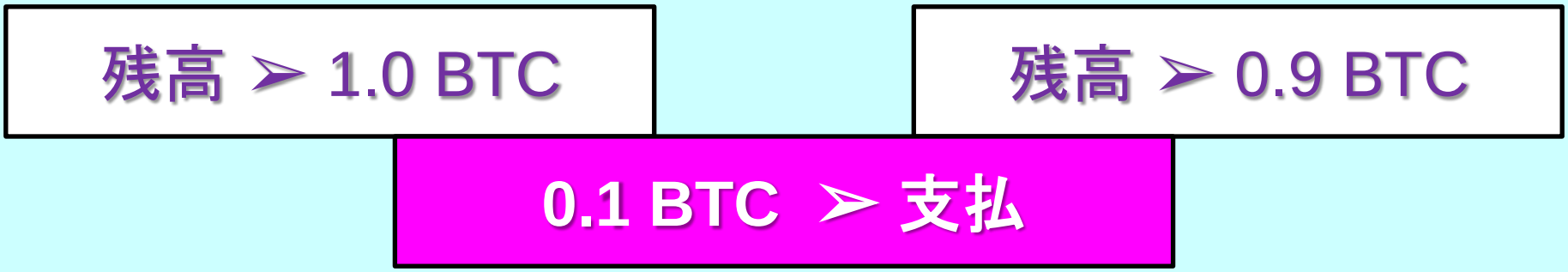


個々の取引

過去

現在

未来


残高 ➢ 1.0 BTC
残高 ➢ 0.9 BTC
0.1 BTC ➢ 支払

過去

未来

残高➢誰か　0.0BTC

入金➢自分　1.0 BTC

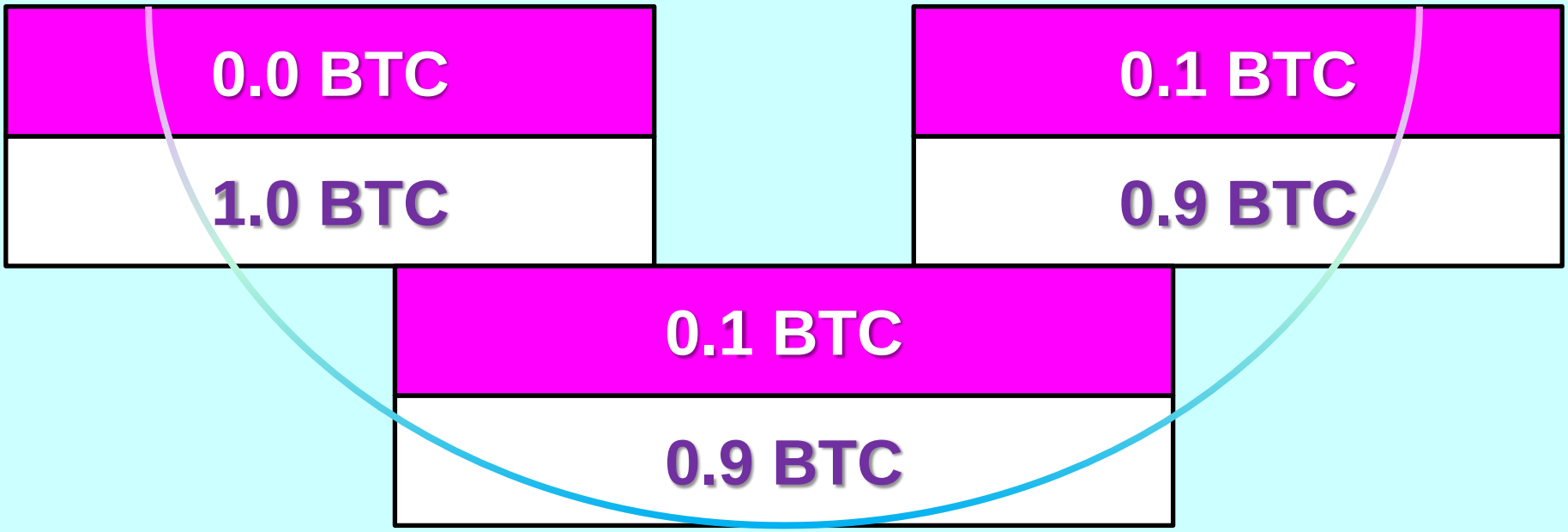
入金➢誰か　0.1 BTC

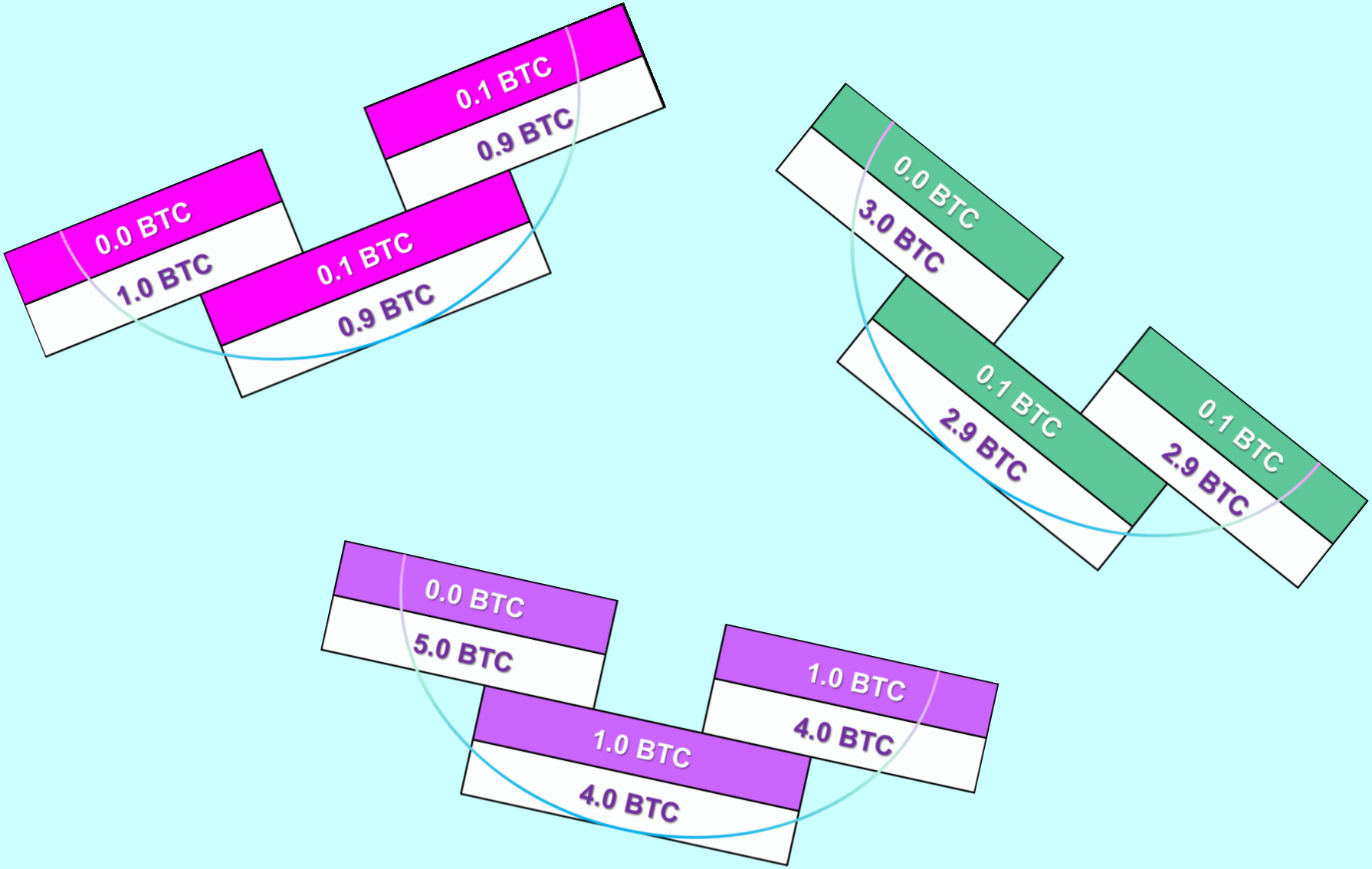
残高➢自分　0.9 BTC

0.1 BTC　支払➢誰か

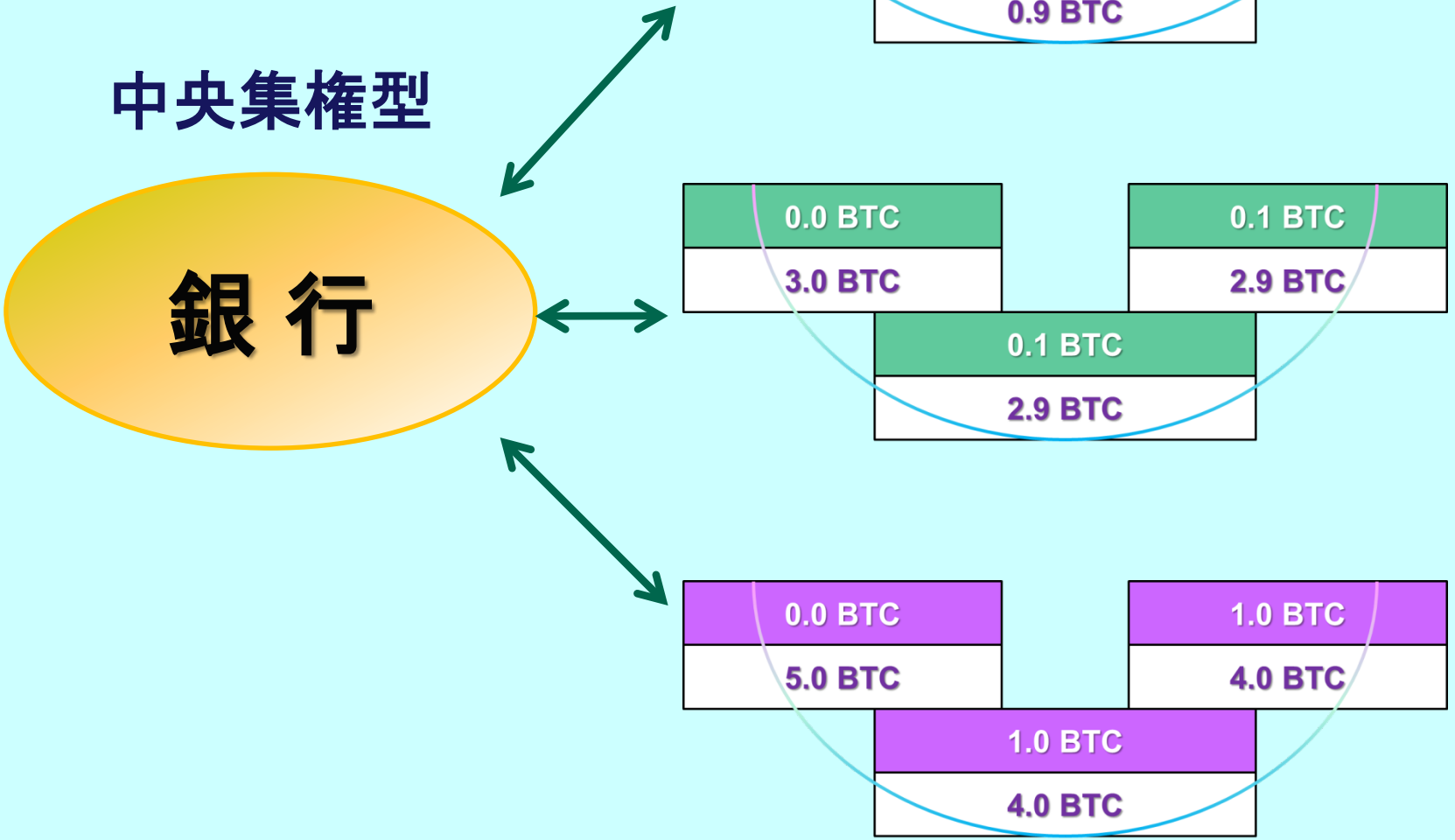
0.9 BTC　釣り➢自分

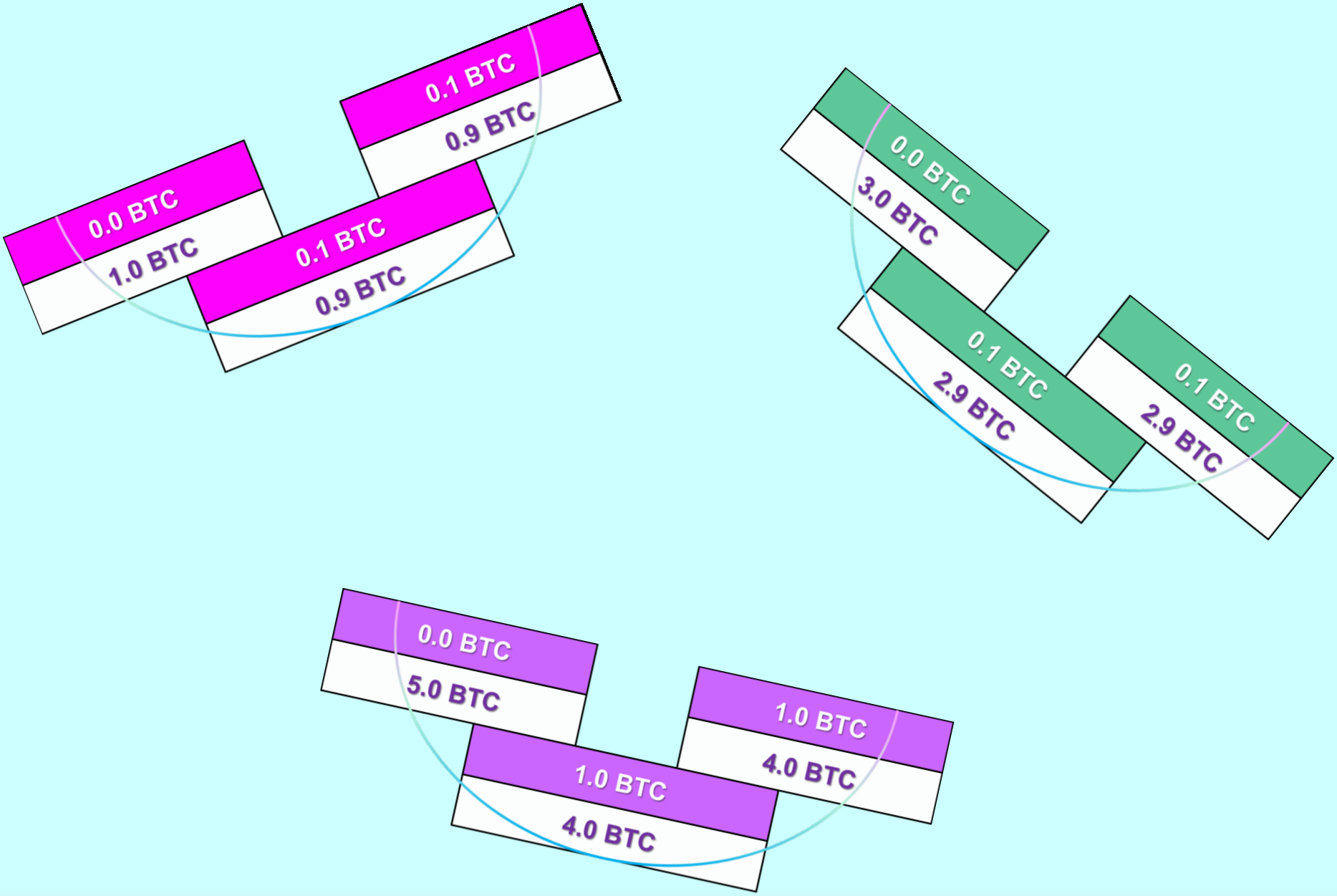
現在

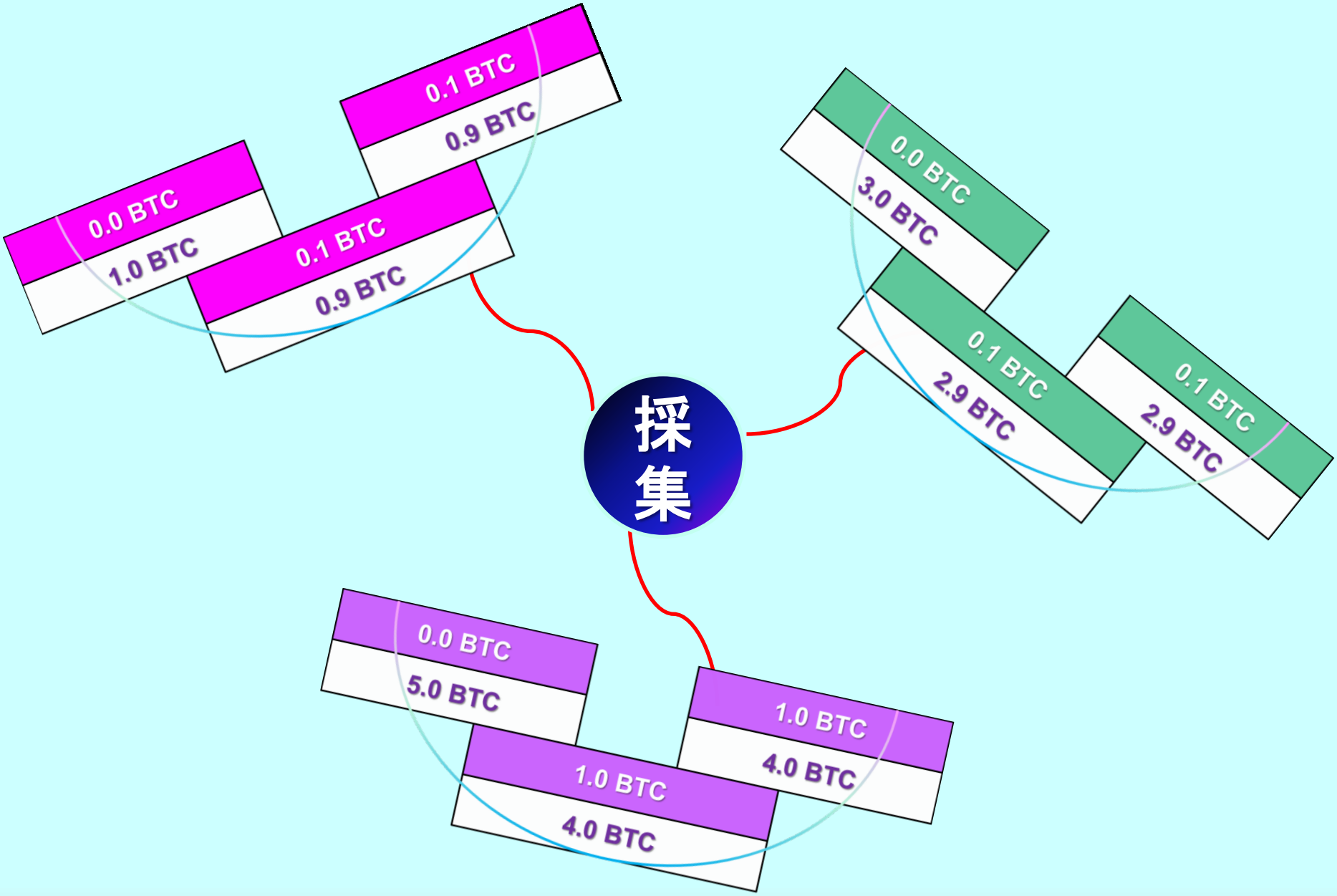

0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC


0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
1.0 BTC
4.0 BTC

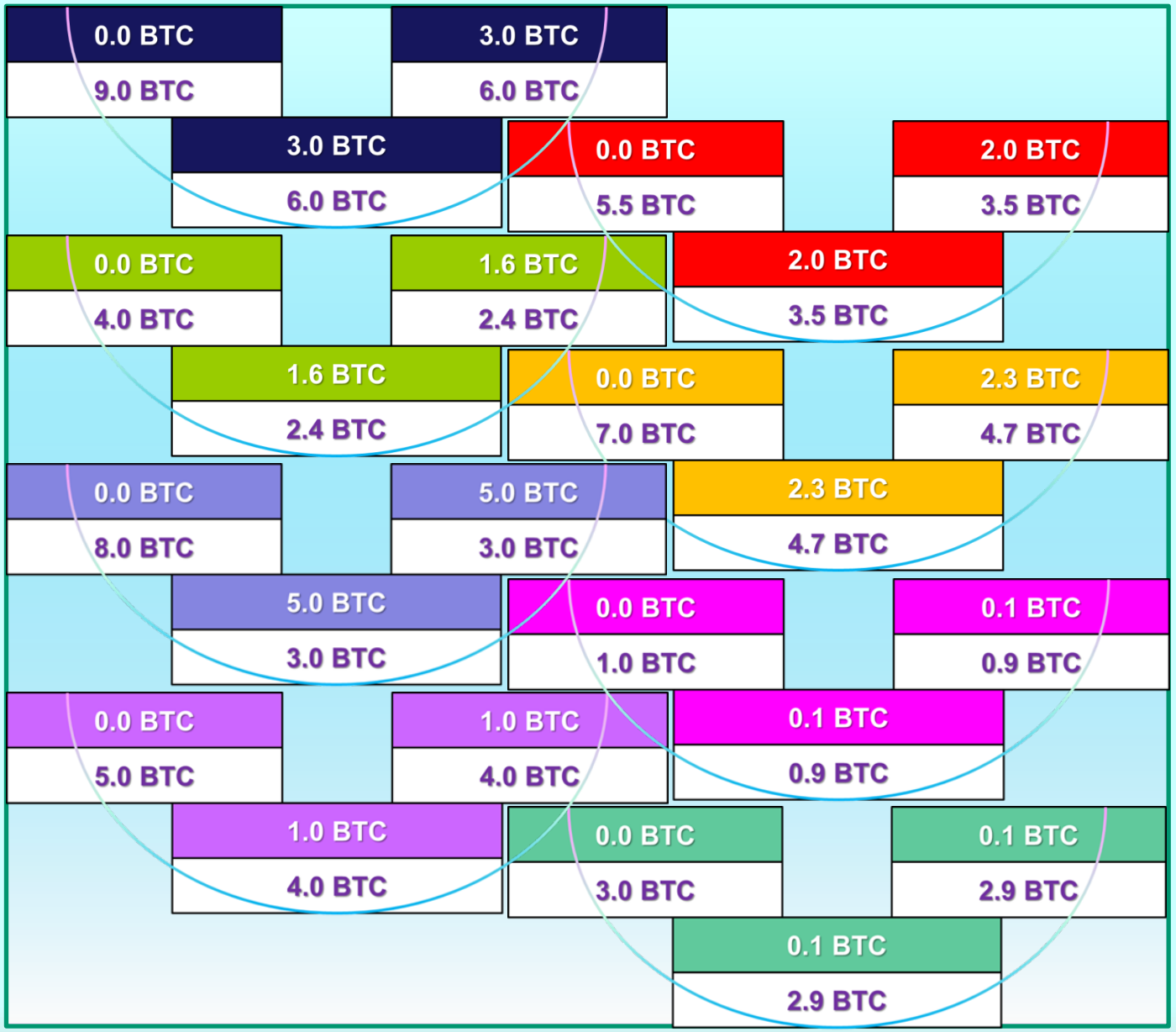
中央集権型


銀 行
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
1.0 BTC
4.0 BTC

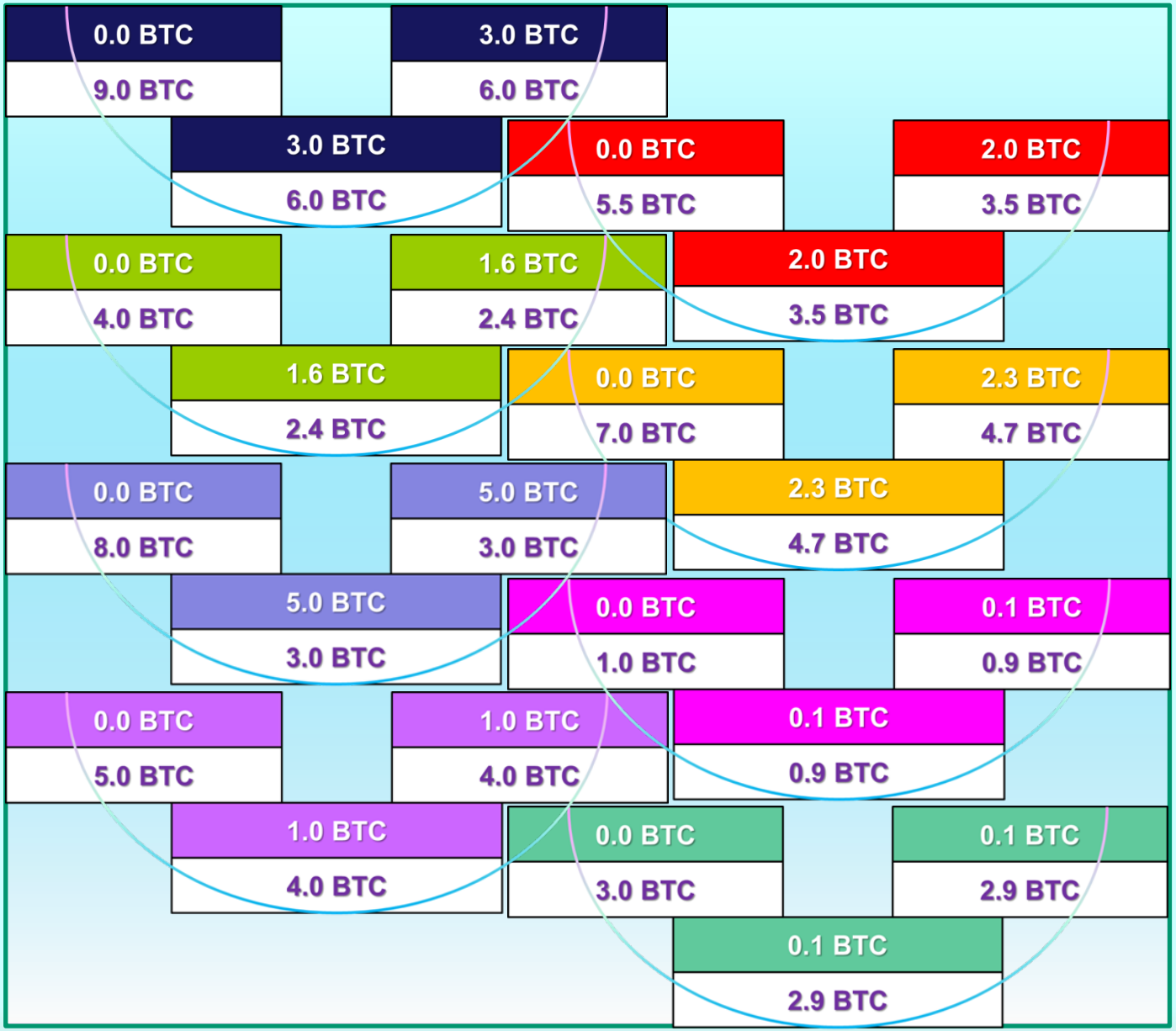

0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
1.0 BTC
4.0 BTC


0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC
採集
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
1.0 BTC
4.0 BTC

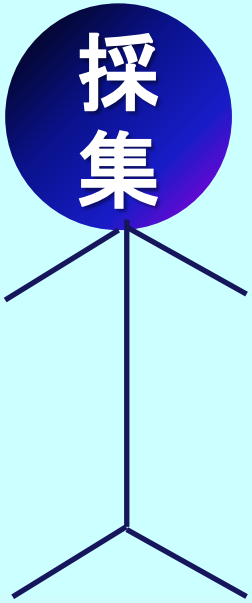
篭（ブロック）にまとめる

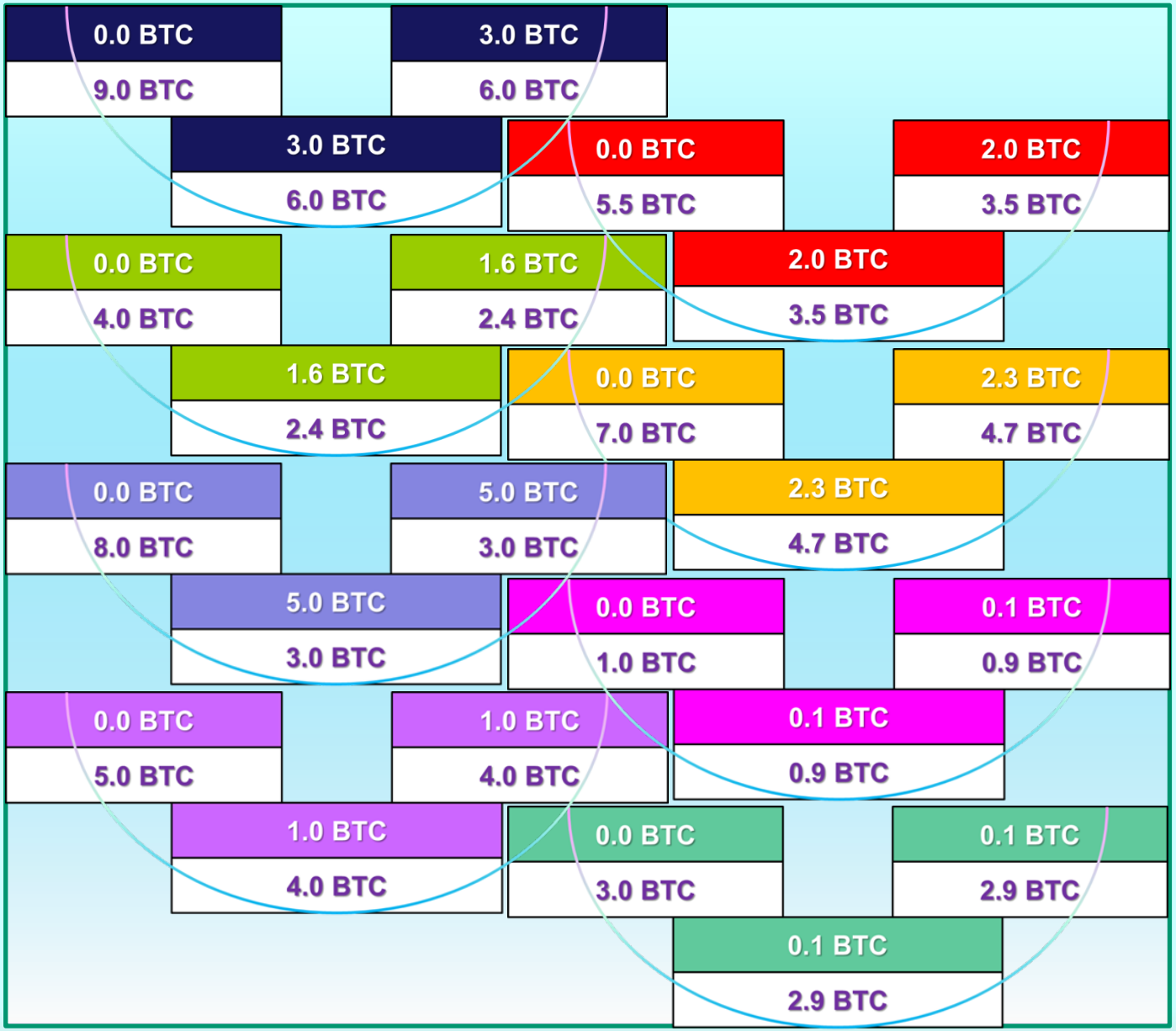

0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

採集


0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

計算問題


採集


0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

計算競争

採掘

0.0 BTC 9.0 BTC	3.0 BTC 6.0 BTC			
	3.0 BTC 6.0 BTC	0.0 BTC 5.5 BTC	2.0 BTC 3.5 BTC	
0.0 BTC 4.0 BTC	1.6 BTC 2.4 BTC	2.0 BTC 3.5 BTC		
	1.6 BTC 2.4 BTC	0.0 BTC 7.0 BTC	2.3 BTC 4.7 BTC	
0.0 BTC 8.0 BTC	5.0 BTC 3.0 BTC	2.3 BTC 4.7 BTC		
	5.0 BTC 3.0 BTC	0.0 BTC 1.0 BTC	0.1 BTC 0.9 BTC	
0.0 BTC 5.0 BTC	1.0 BTC 4.0 BTC	0.1 BTC 0.9 BTC		
	1.0 BTC 4.0 BTC	0.0 BTC 3.0 BTC	0.1 BTC 2.9 BTC	
		0.1 BTC 2.9 BTC		

正解発見

正解発見

ブロック

0.0 BTC 9.0 BTC	3.0 BTC 6.0 BTC		
3.0 BTC 6.0 BTC	0.0 BTC 5.5 BTC	2.0 BTC 3.5 BTC	
0.0 BTC 4.0 BTC	1.6 BTC 2.4 BTC	2.0 BTC 3.5 BTC	
1.6 BTC 2.4 BTC	0.0 BTC 7.0 BTC	2.3 BTC 4.7 BTC	
0.0 BTC 8.0 BTC	5.0 BTC 3.0 BTC	2.3 BTC 4.7 BTC	
5.0 BTC 3.0 BTC	0.0 BTC 1.0 BTC	0.1 BTC 0.9 BTC	
0.0 BTC 5.0 BTC	1.0 BTC 4.0 BTC	0.1 BTC 0.9 BTC	
1.0 BTC 4.0 BTC	0.0 BTC 3.0 BTC	0.1 BTC 2.9 BTC	
		0.1 BTC 2.9 BTC	

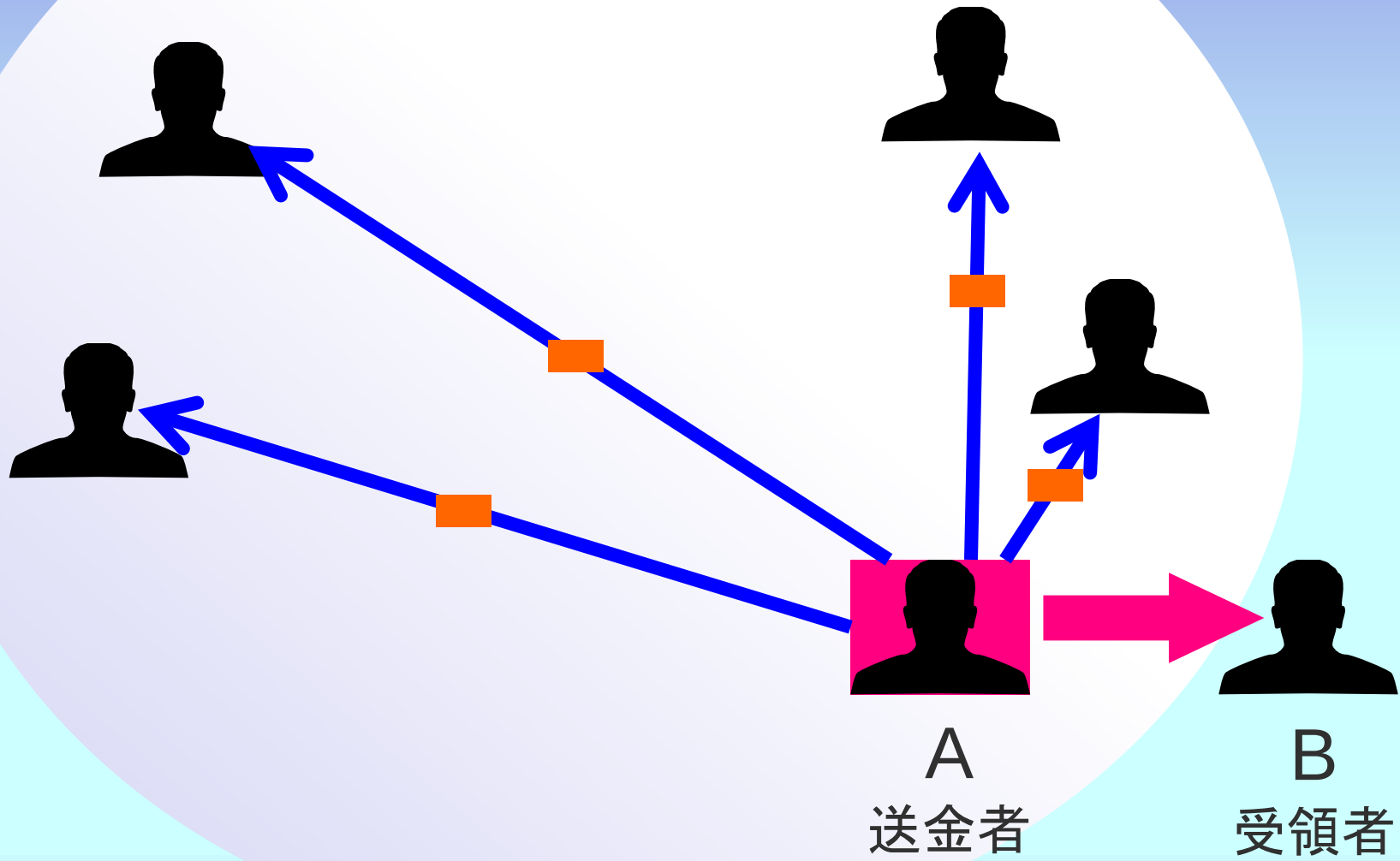
何のために採掘するのか

AがBに5.0BTC
支払った

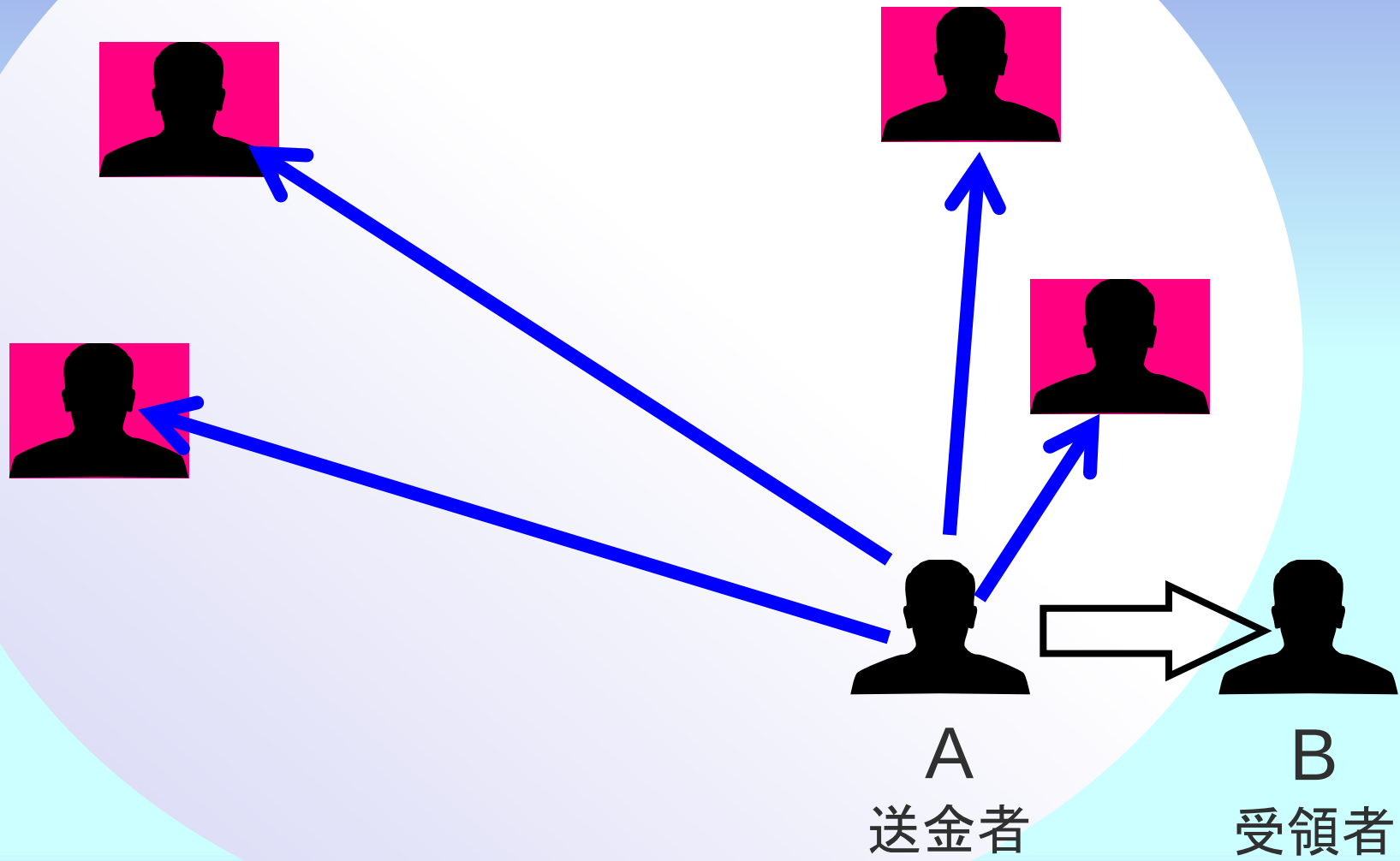
A
送金者

B
受領者

◆取引記録をバケツリレー



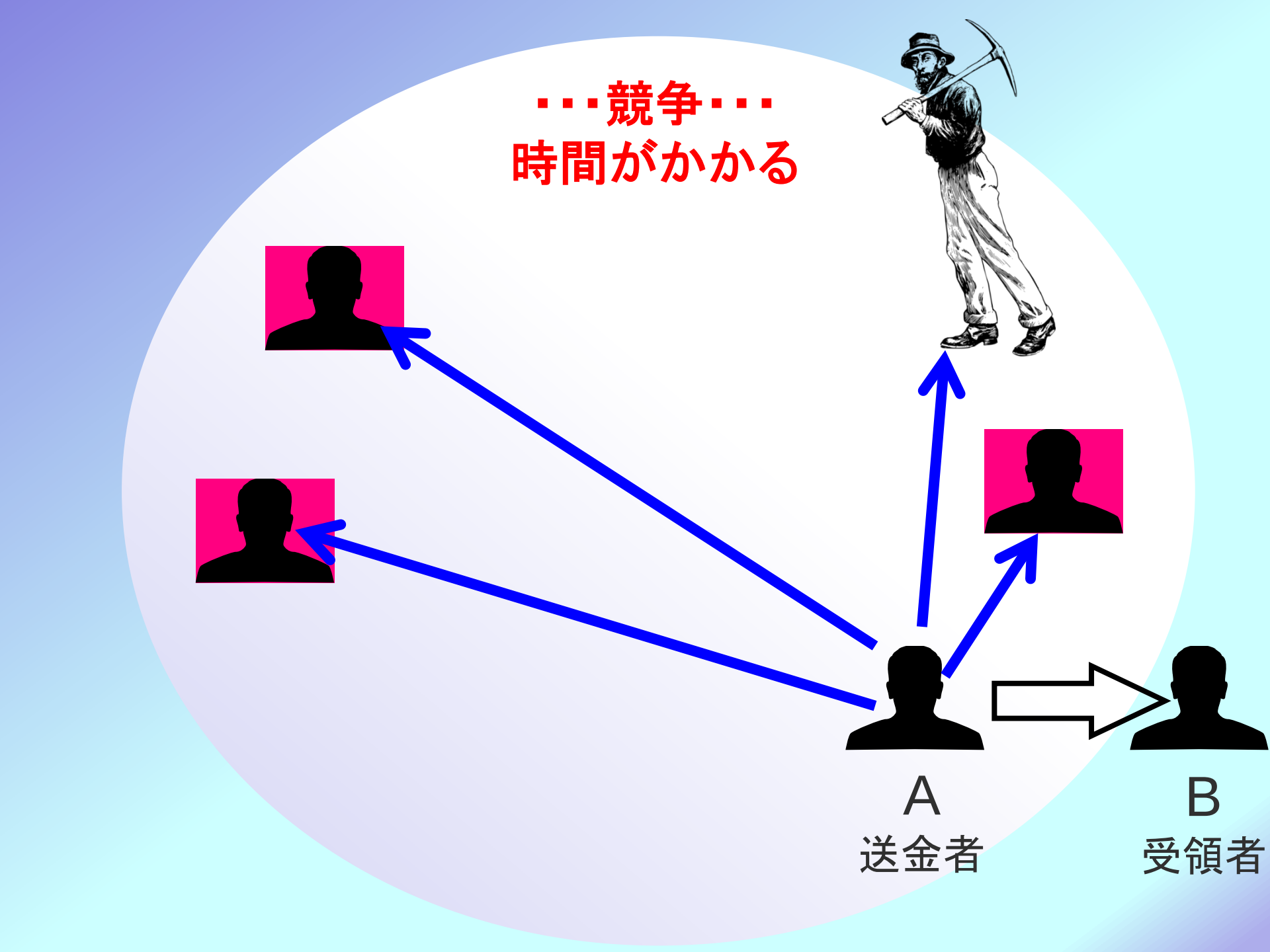
競い合って計算する



採掘者が計算競争

A
送金者

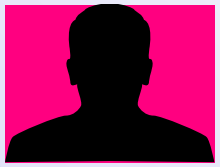
B
受領者


・・・競争・・・
時間がかかる
A
送金者
B
受領者

・・・正解発見・・・
時間がかかった

A
送金者

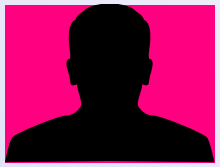
B
受領者



疲れた

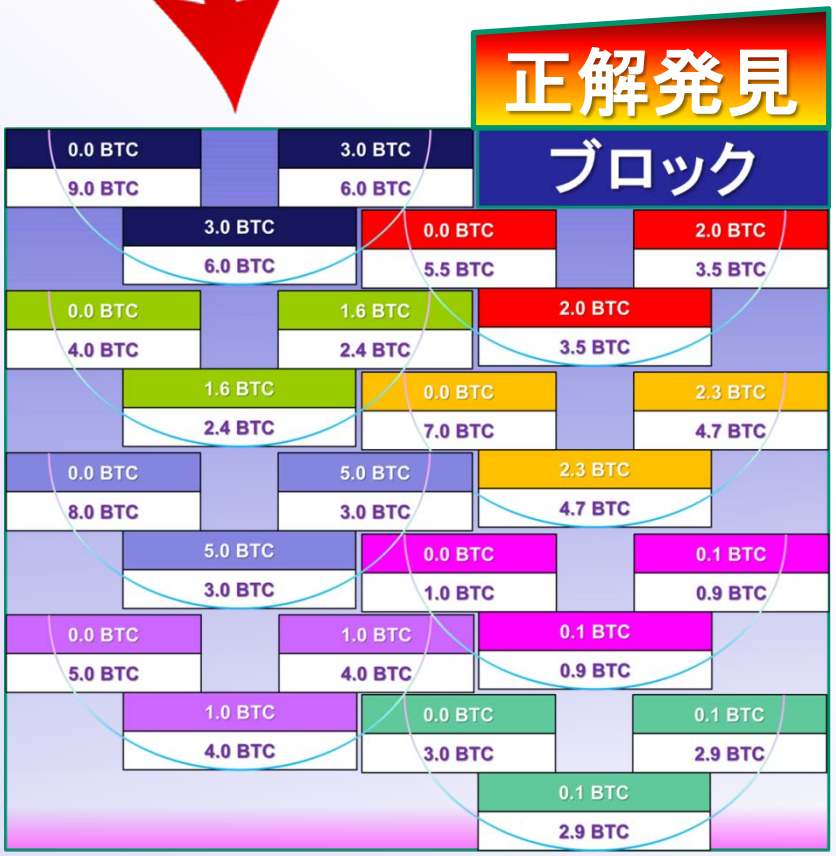
正解発見
ブロック
0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

時間をかけた証拠



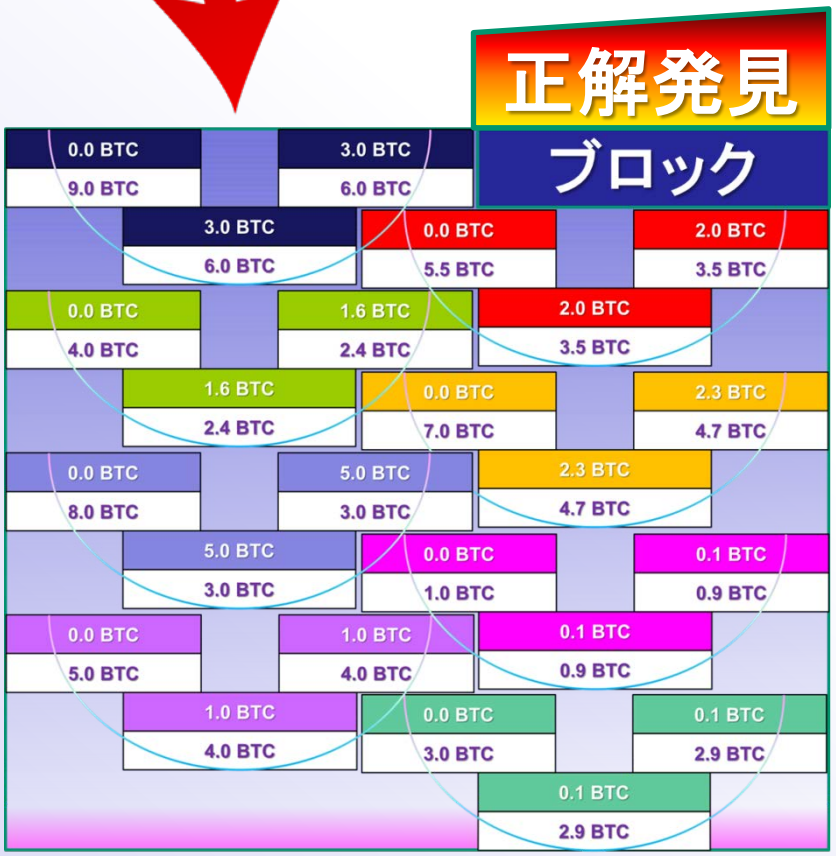
正解発見
ブロック
0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

偽造には遙かに長い時間

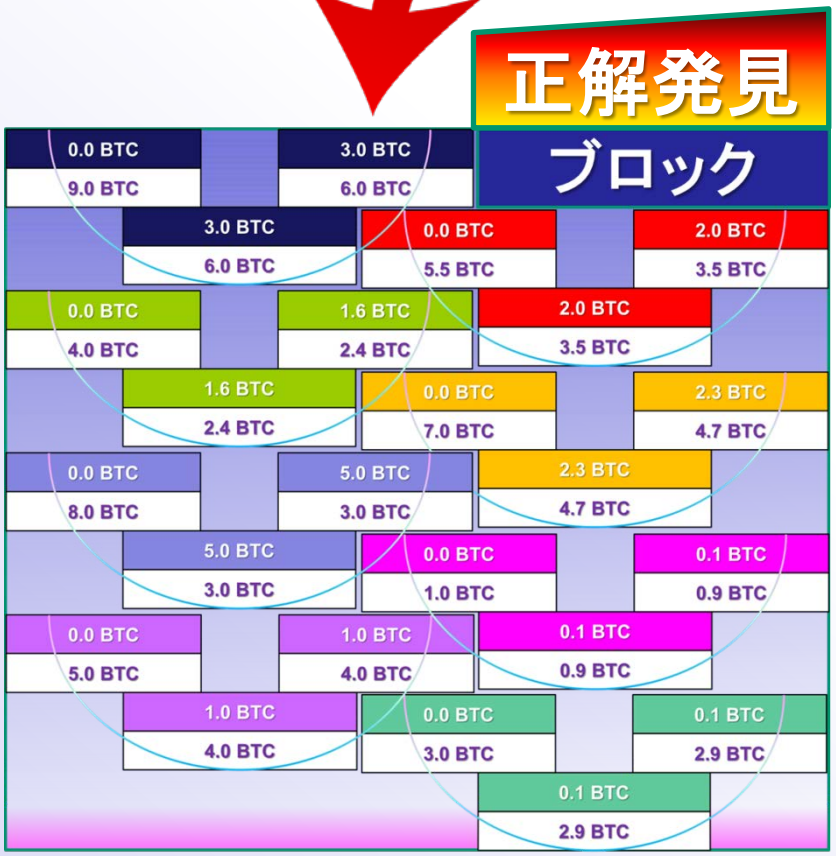


割に合わない・・・

偽造には遙かに長い時間

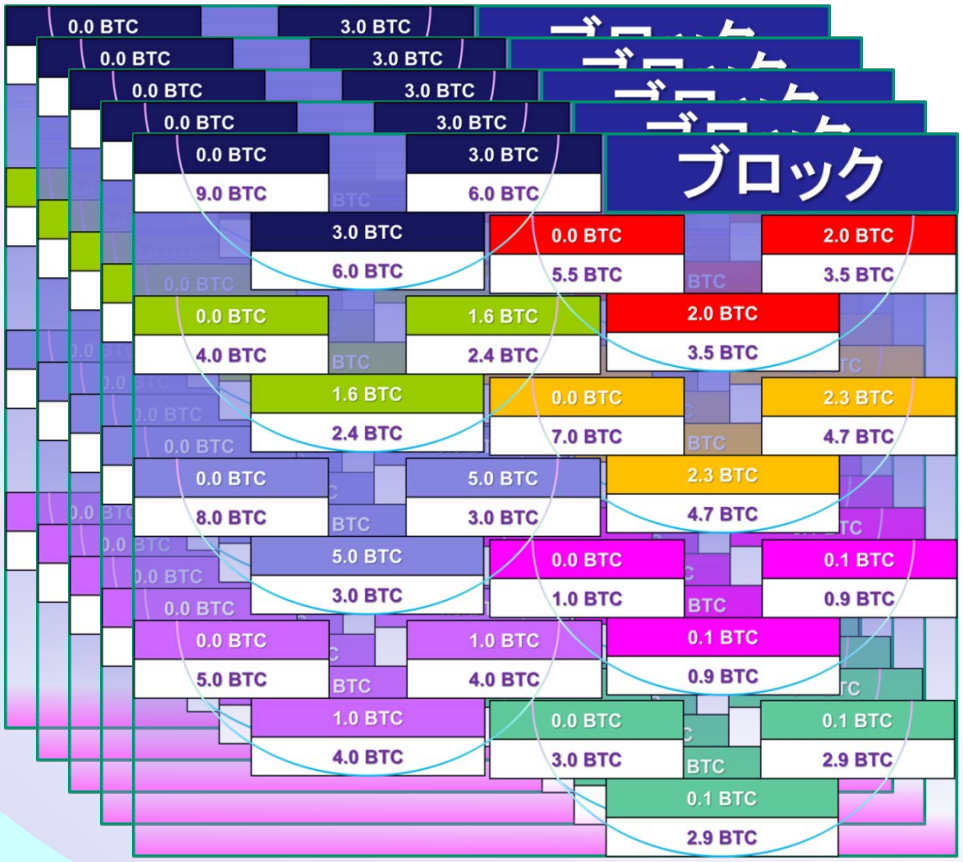


正式に登録しよう


正解発見
ブロック
0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

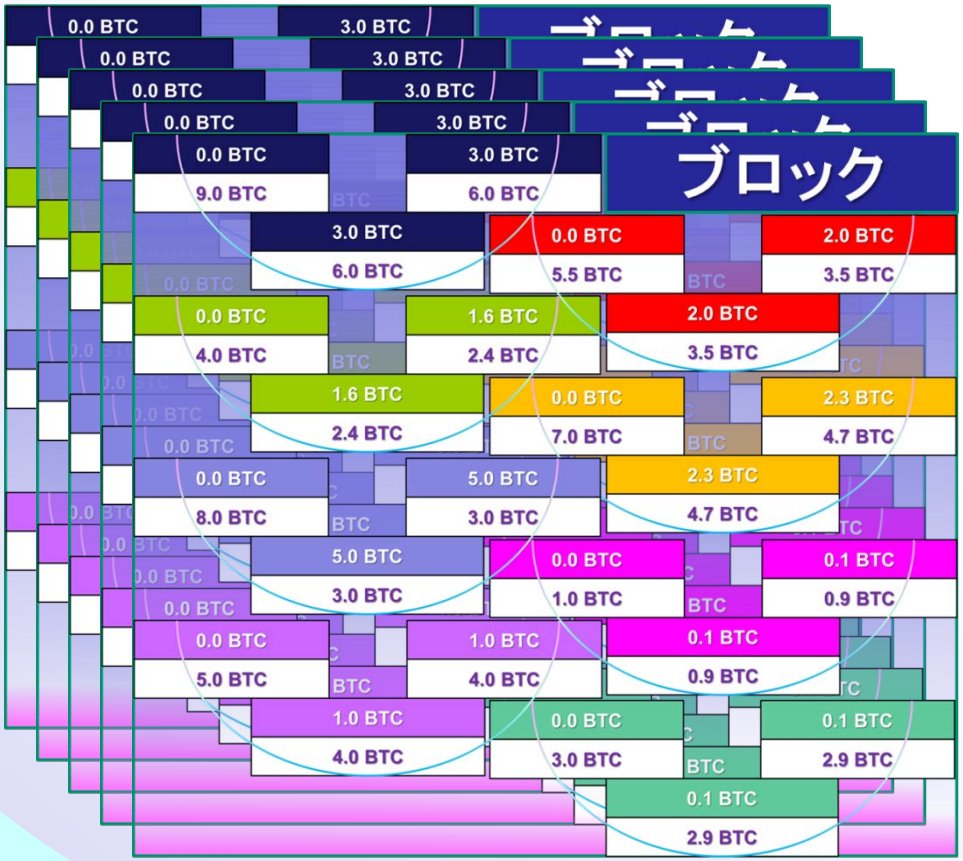
新しく追加したい

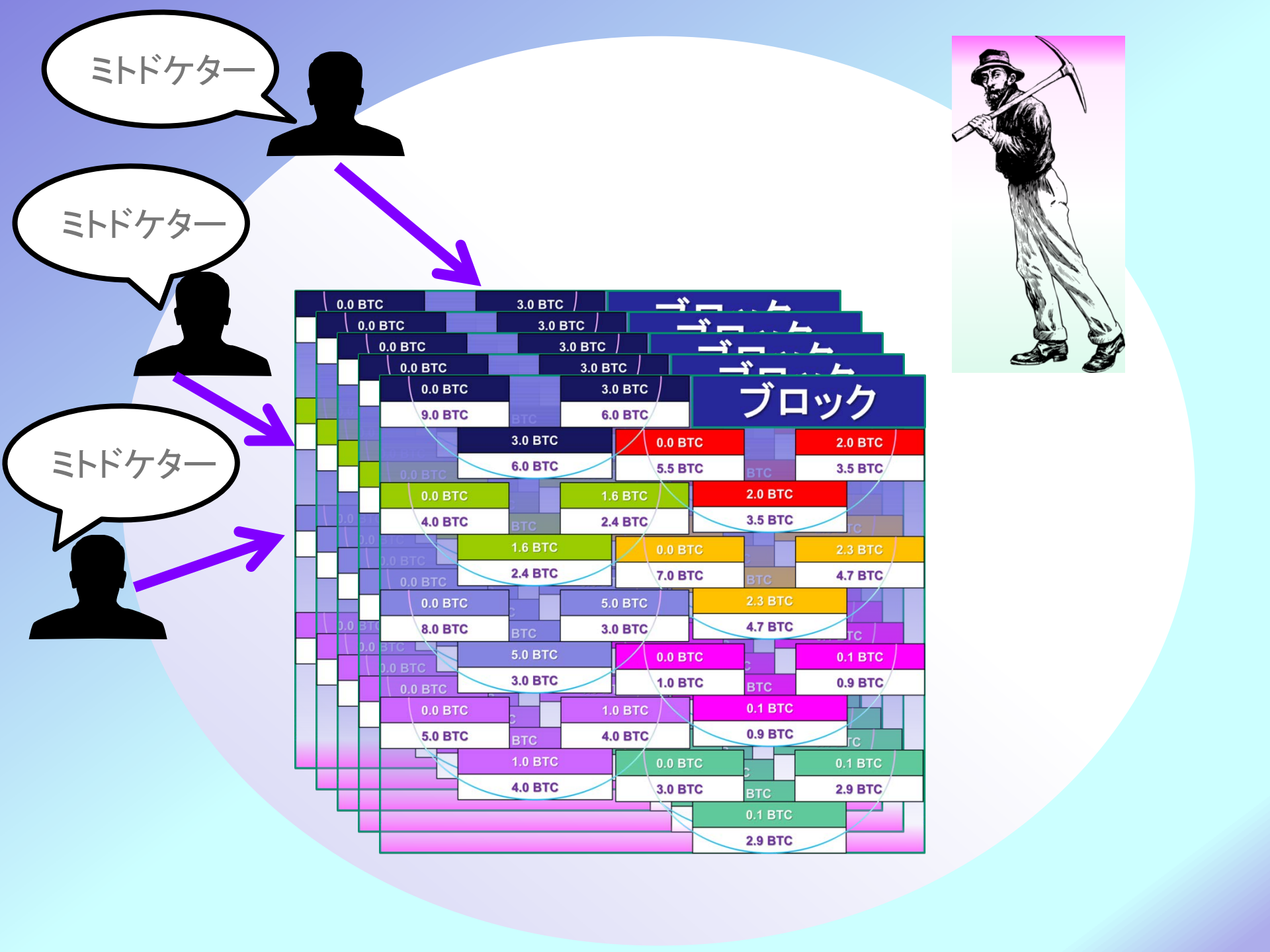
ビットコイン大福帳の一冊



いいですか皆さん？

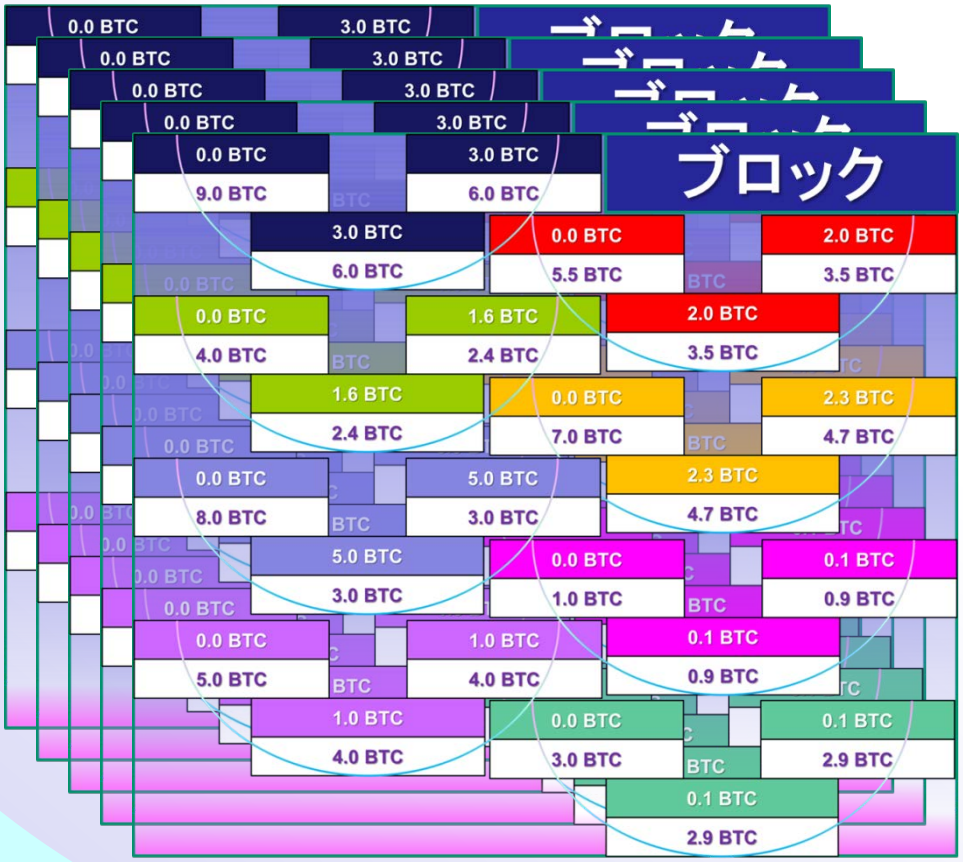
ビットコイン大福帳の一冊




ミトドケター
ミトドケター
ミトドケター
ブロック
0.0 BTC
3.0 BTC
9.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

無事に登録されました

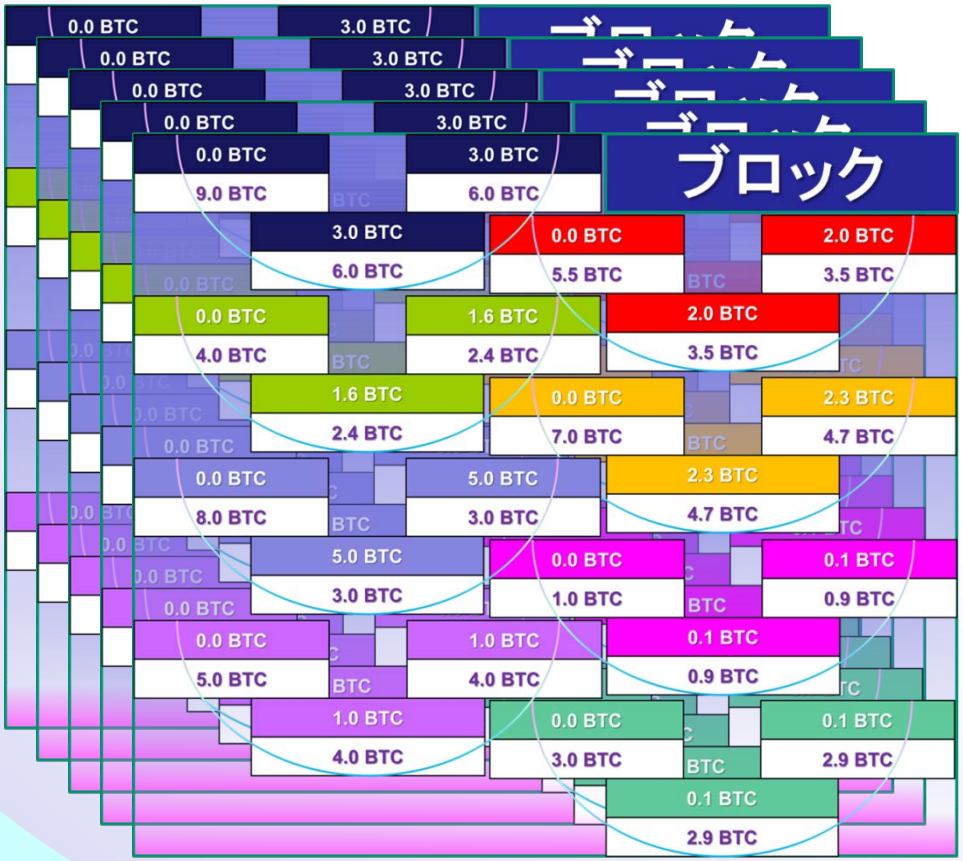
ビットコイン大福帳の一冊



作業の報酬

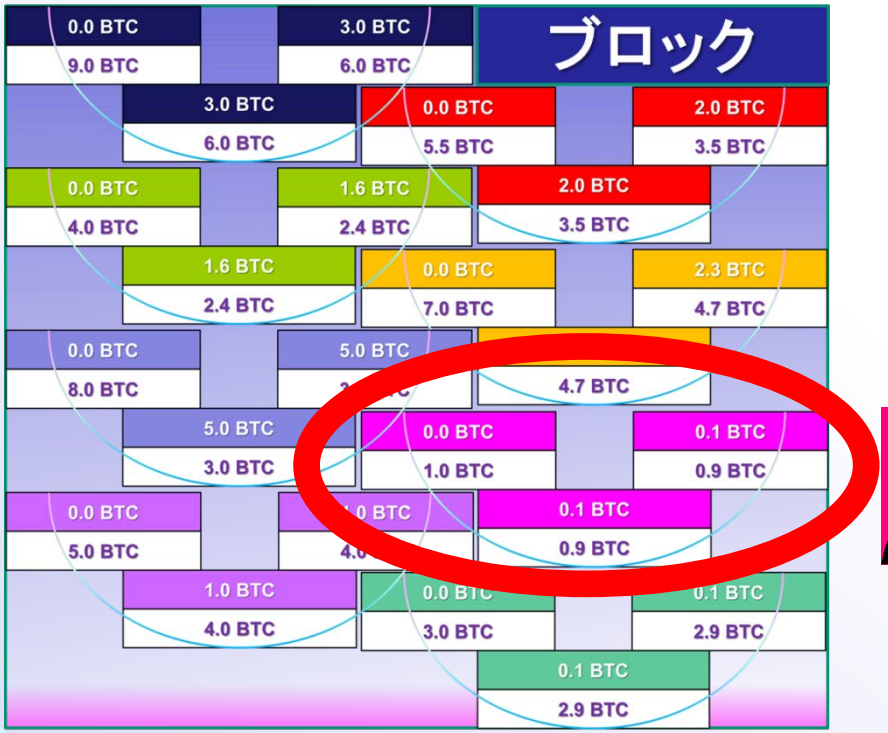
25BTC

うれしい

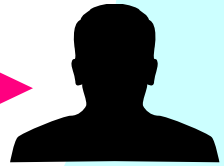


登録されると・・・

ビットコイン大福帳の一冊

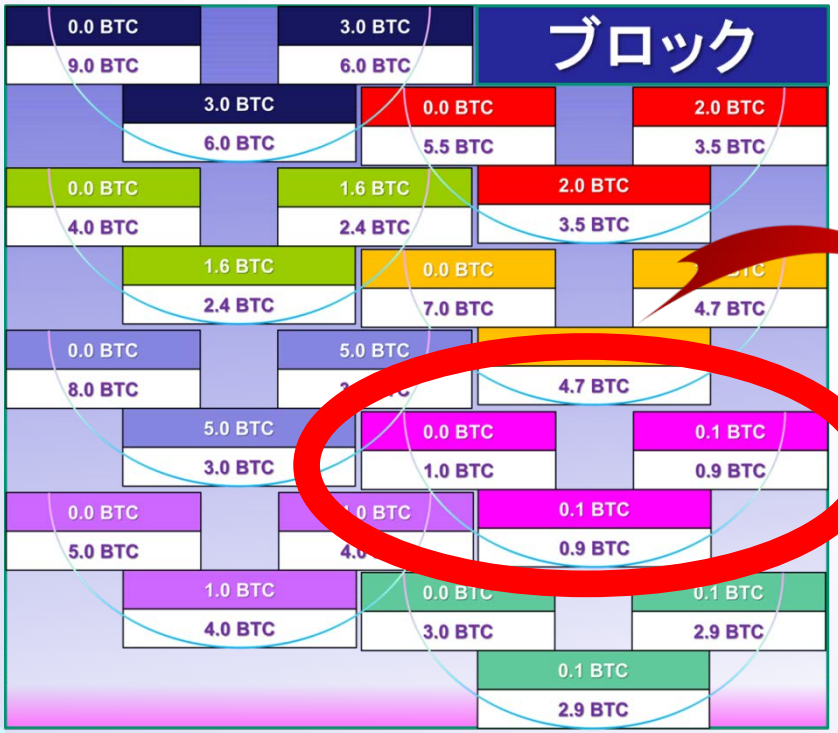


A
送金者



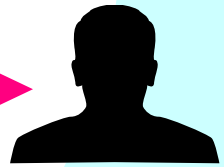
B
受領者

ビットコイン大福帳の一冊



取引が承認された

A
送金者



B
受領者

よかった

エコシステム

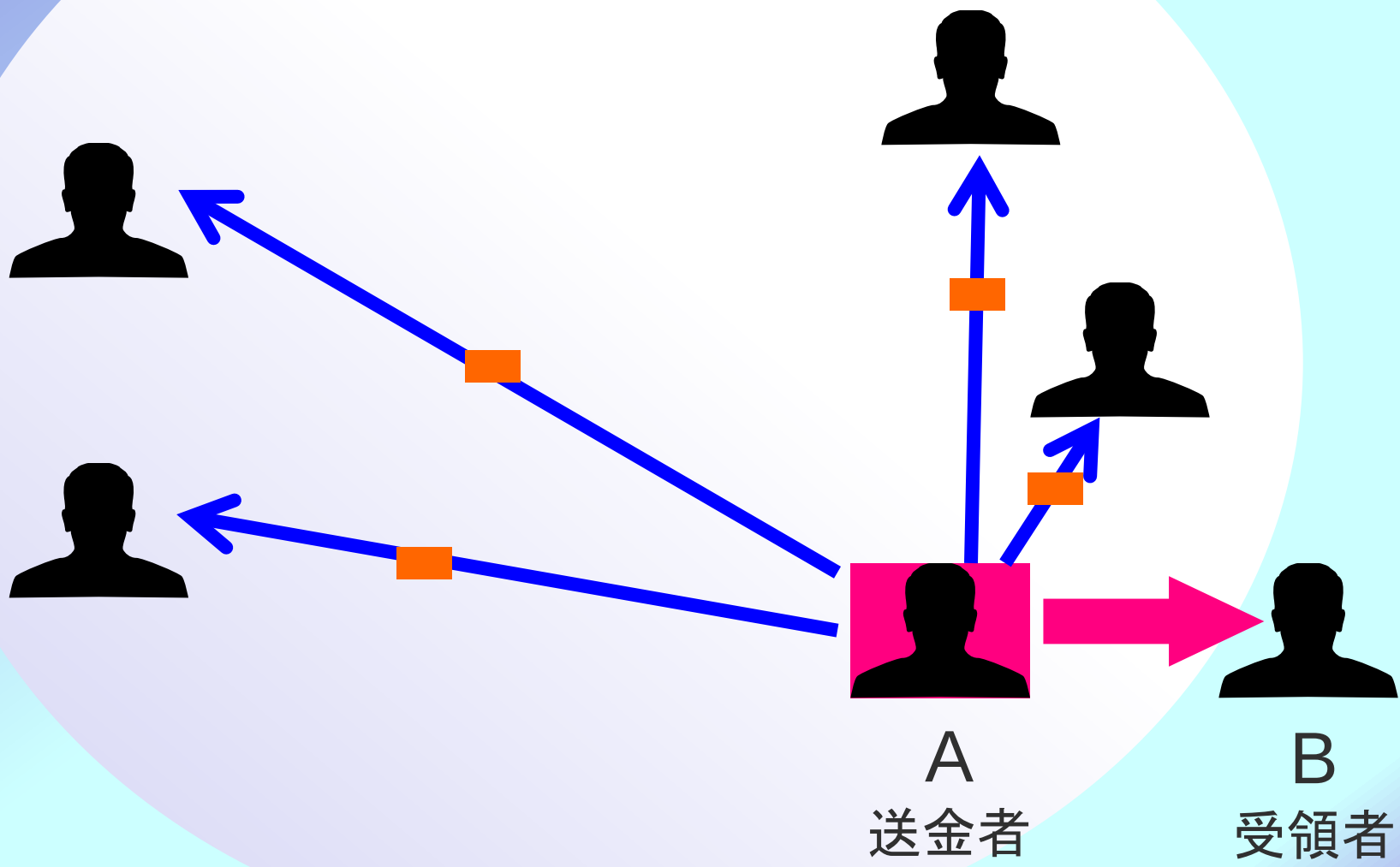
1.支払

AがBに5.0BTC
支払った

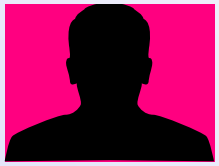
A
送金者

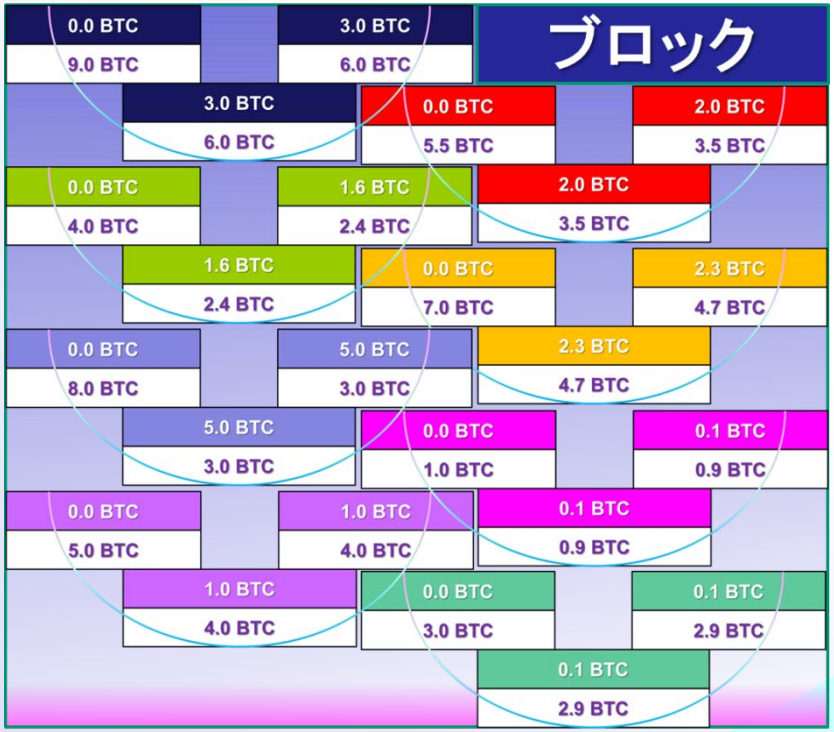
B
受領者

2.記録

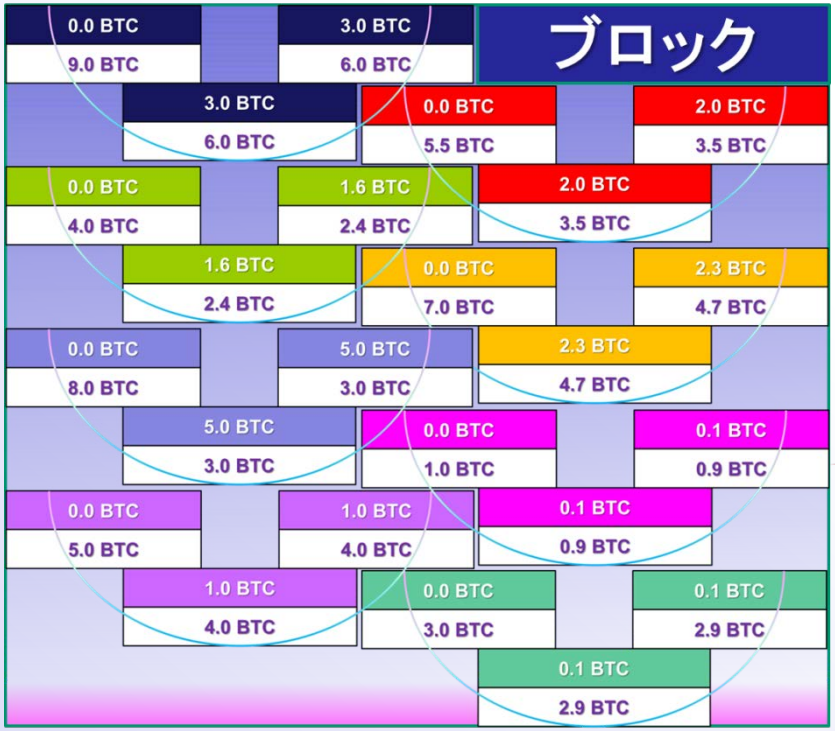


3.採掘



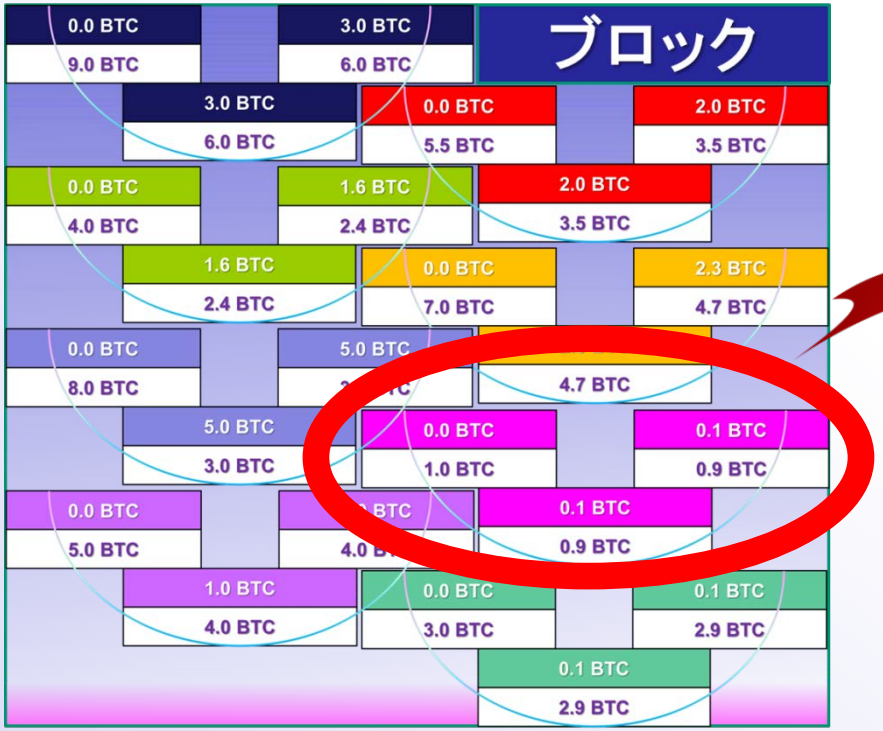

ブロック
0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

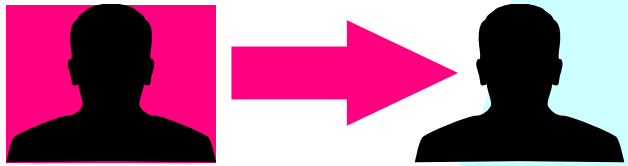
4.報酬


0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
ブロック
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
3.0 BTC
2.3 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC

25BTC

5.承認


0.0 BTC
9.0 BTC
3.0 BTC
6.0 BTC
ブロック
3.0 BTC
6.0 BTC
0.0 BTC
5.5 BTC
2.0 BTC
3.5 BTC
0.0 BTC
4.0 BTC
1.6 BTC
2.4 BTC
2.0 BTC
3.5 BTC
1.6 BTC
2.4 BTC
0.0 BTC
7.0 BTC
2.3 BTC
4.7 BTC
0.0 BTC
8.0 BTC
5.0 BTC
4.7 BTC
5.0 BTC
3.0 BTC
0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.0 BTC
5.0 BTC
0.1 BTC
0.9 BTC
1.0 BTC
4.0 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC



A B

6.発行

25BTC

インターネットの、
インターネットによる、
インターネットのための通貨

仮想通貨のリスク

MT.GOX

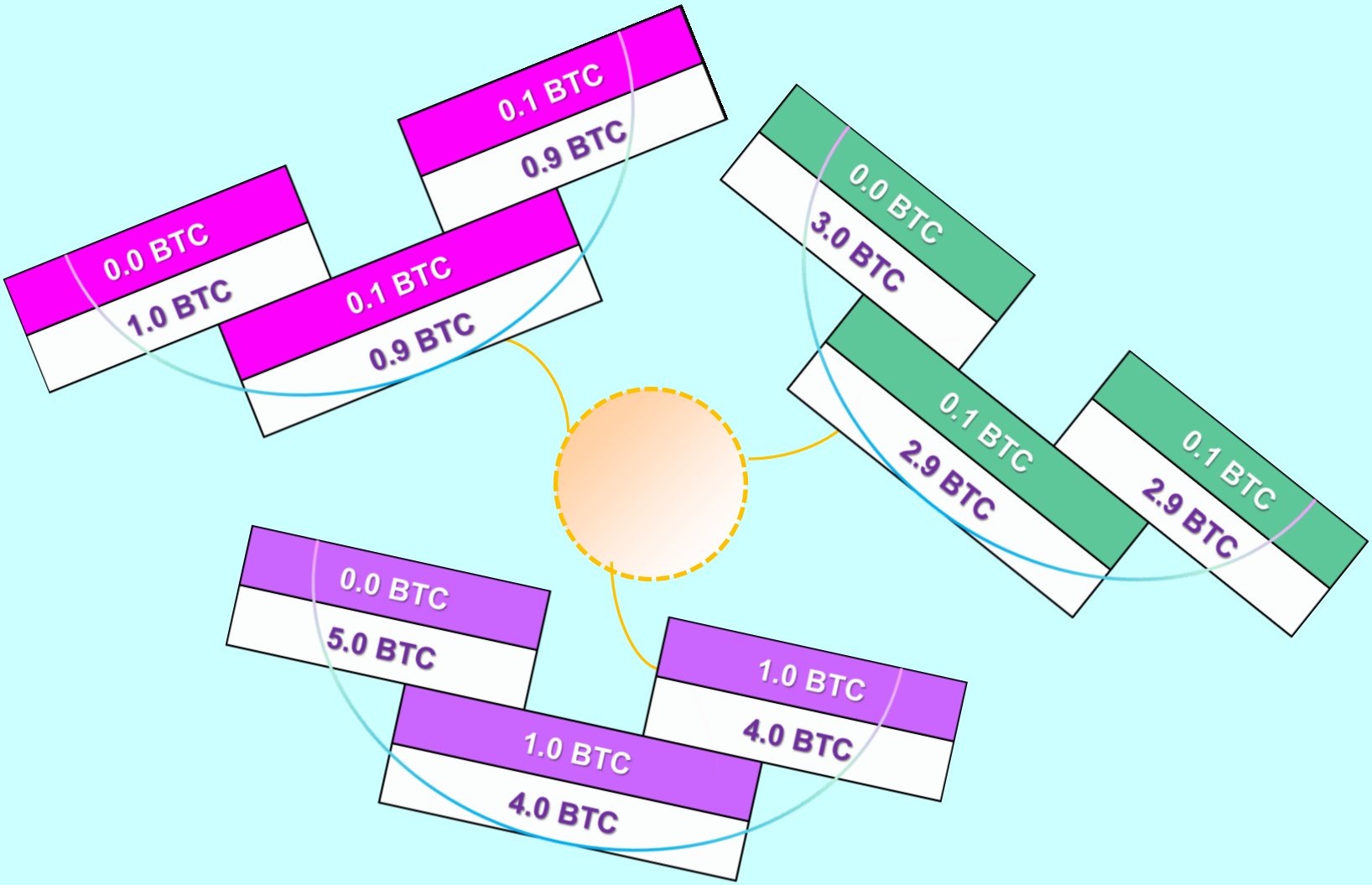
2014年2月28日

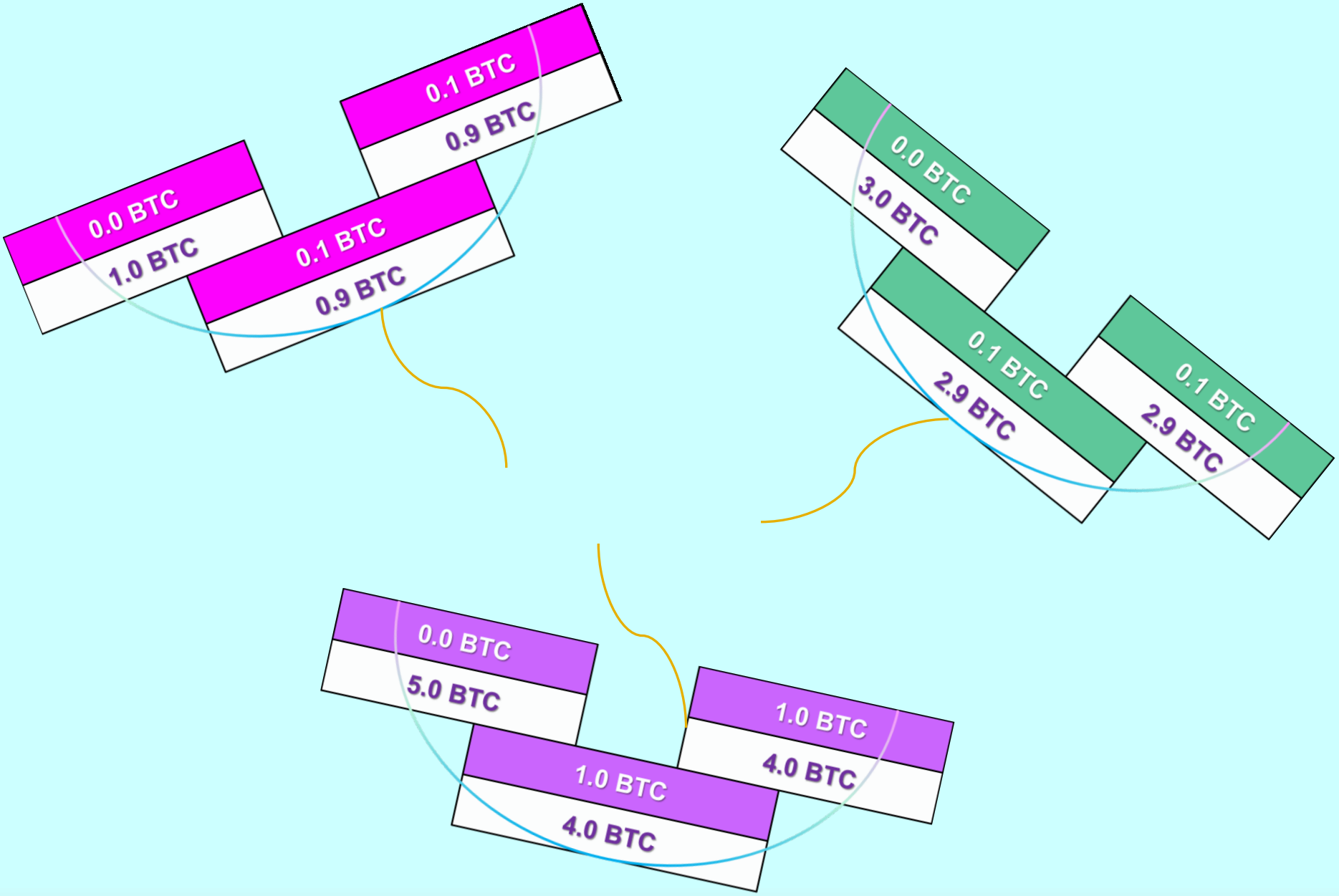
ykanazawa1999

預かった⇒消えた

消えたビットコイン

どこに消えたのか？

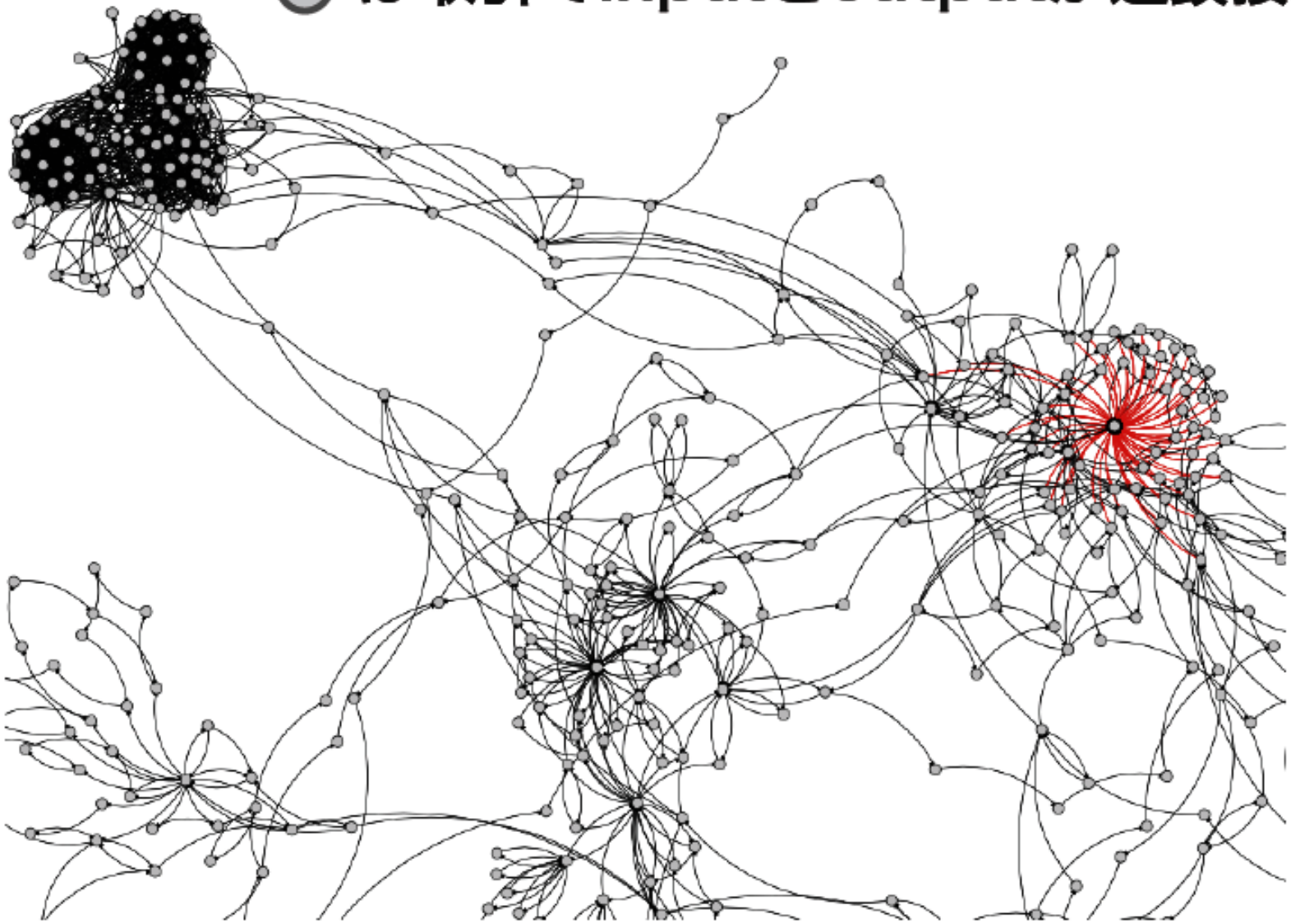

0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
1.0 BTC
4.0 BTC


0.0 BTC
1.0 BTC
0.1 BTC
0.9 BTC
0.1 BTC
0.9 BTC
0.0 BTC
3.0 BTC
0.1 BTC
2.9 BTC
0.1 BTC
2.9 BTC
0.0 BTC
5.0 BTC
1.0 BTC
4.0 BTC
1.0 BTC
4.0 BTC

匿名取引の追跡困難性

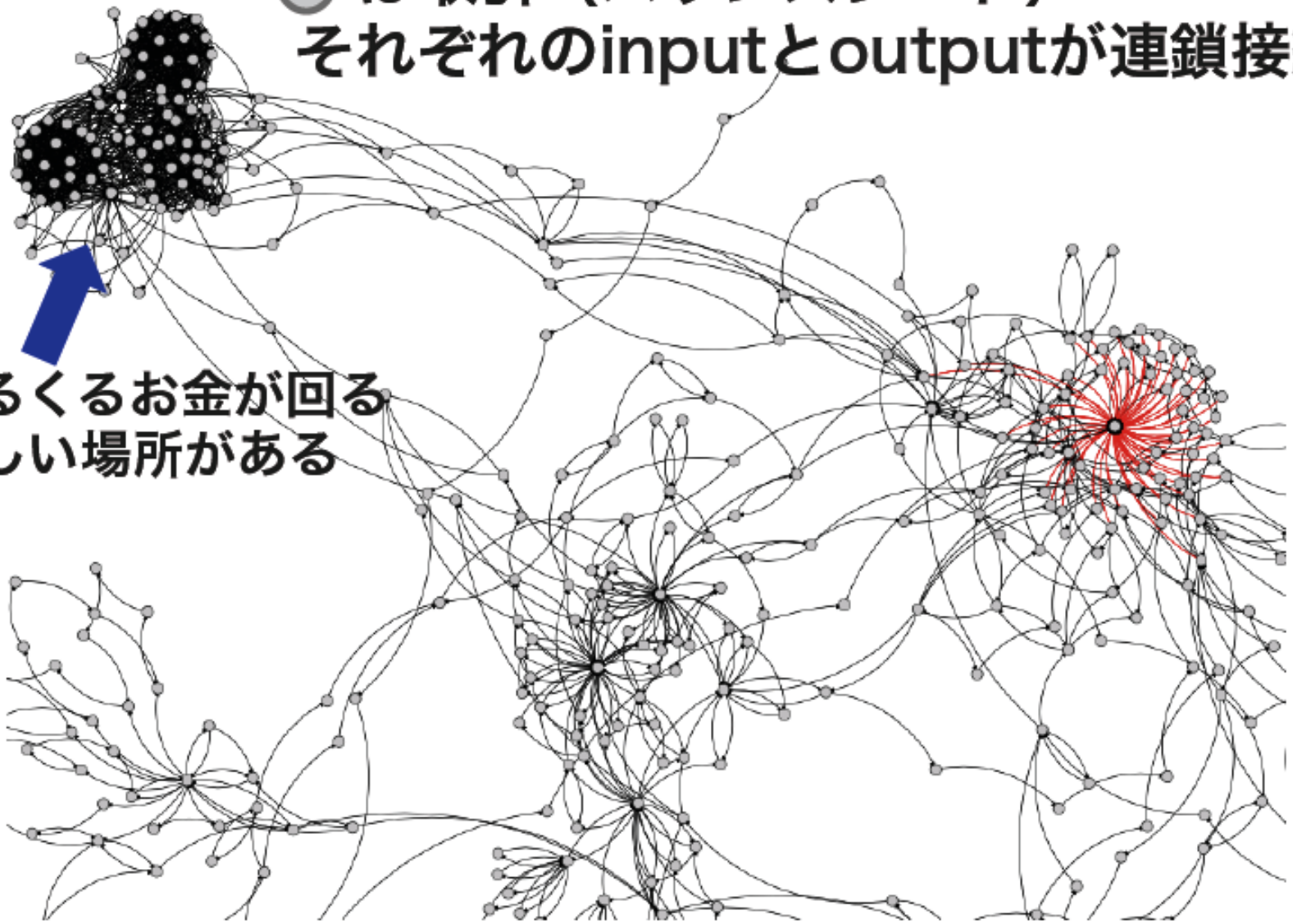
取引グラフの例

● は取引でinputとoutputが連鎖接続



取引グラフの例

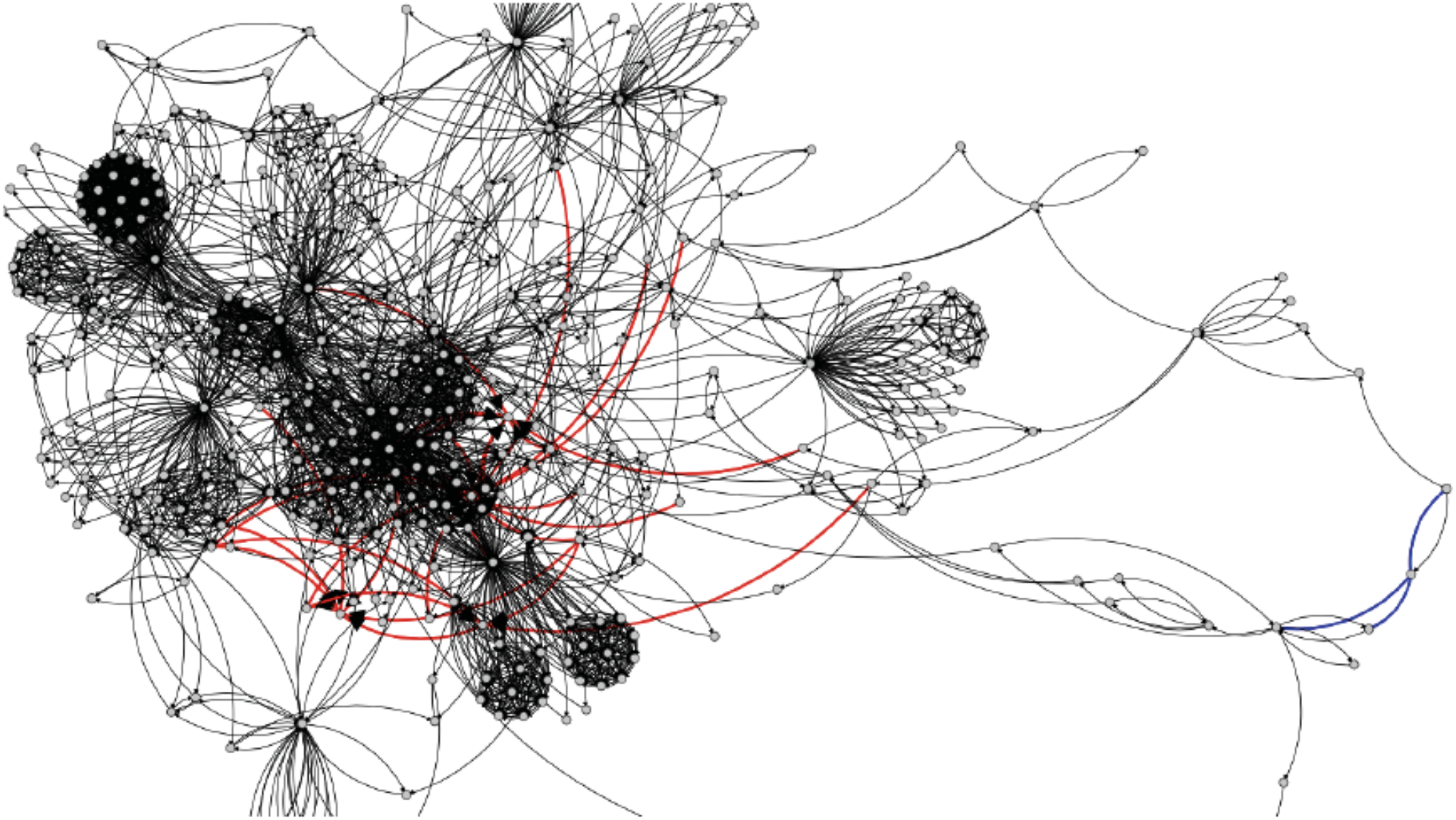
● は取引（バランスシート）
それぞれのinputとoutputが連鎖接続



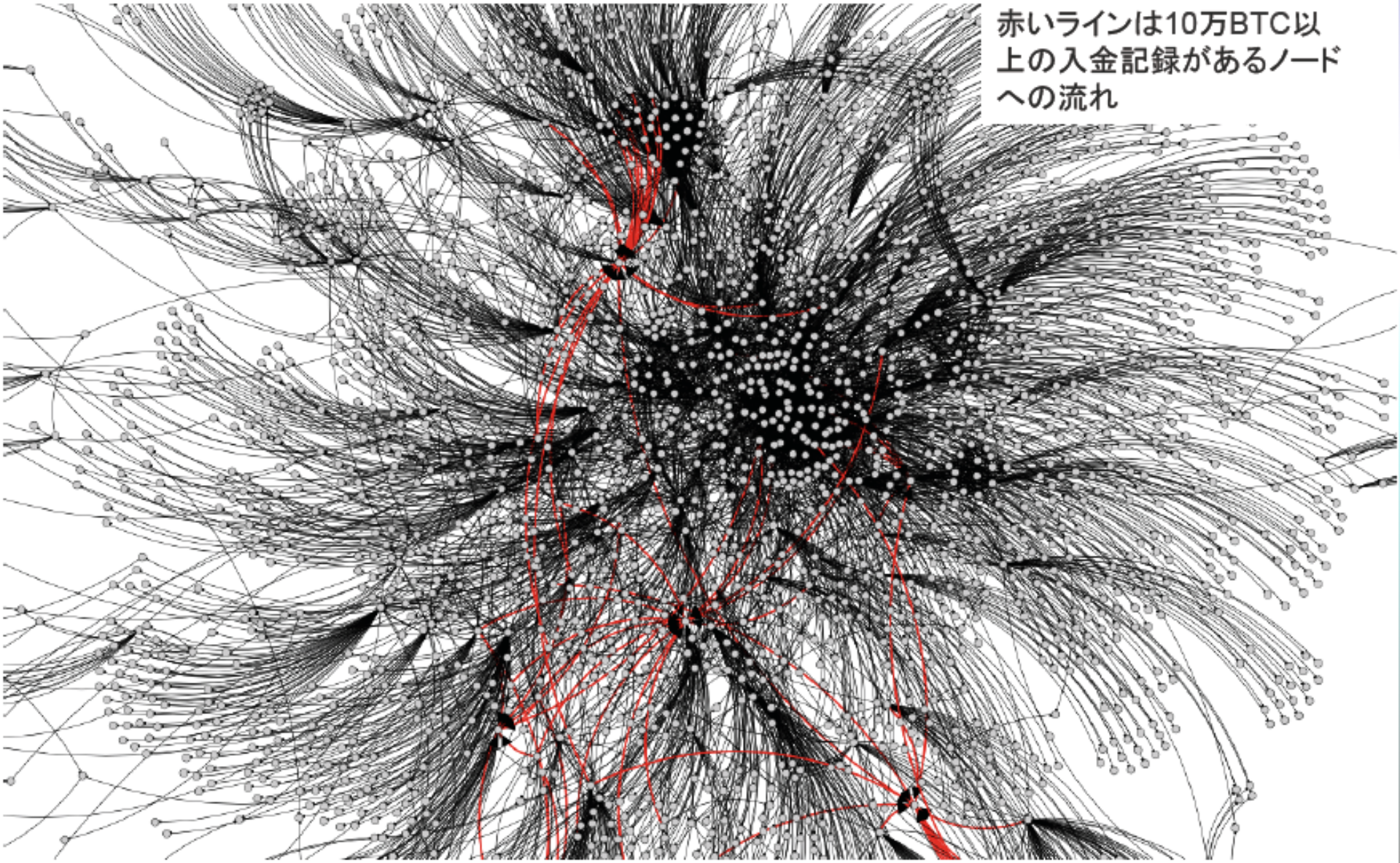
くるくるお金が回る
怪しい場所がある

仮名取引の追跡容易性

注目ノードからMt.Goxへの逆経路のみに枝刈り



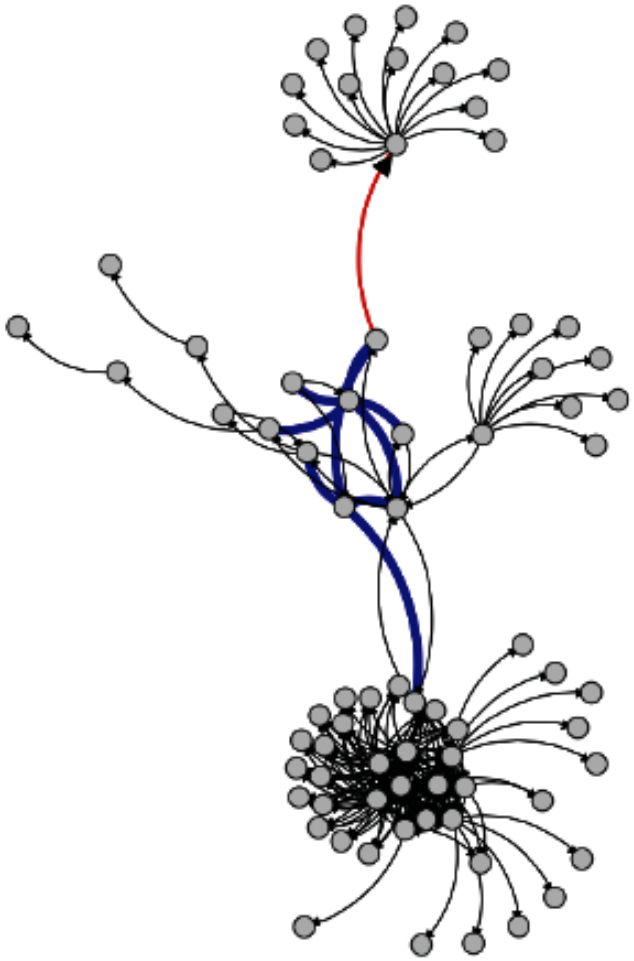
Mt.Gox -> 6ホップの トランザクショングラフ (6282ノード)



破綻時の自主ルール

flexcoin社のコイン盗難経路

2014年3月2日にこのアドレスに盗まれました



flexcoin the bitcoin bank

FAQ Bitcoin Bank Register Activate Login

Flexcoin is shutting down. (March 3 2014)

On March 2nd 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker made off with 896 BTC, dividing them into these two addresses:

1NDkewqpt45WYFEmqvCDDSf7DLMTNVggdu

1QFoC5JitGwpFKqRDd9QNHSoGN68dCNgy8

As Flexcoin does not have the resources, assets, or otherwise to come back from this loss, we are closing our doors immediately.

Users who put their coins into cold storage will be contacted by Flexcoin and asked to verify their identity. Once identified, cold storage coins will be transferred out free of charge. Cold storage coins were held offline and not within reach of the attacker. All other users will be directed to Flexcoin's **"Terms of service"** located at "Flexcoin.com/118.html" a document which was agreed on, upon signing up with Flexcoin.

Flexcoin will attempt to work with law enforcement to trace the source of the hack.

Updates will be posted on **twitter** as soon as they become available.

Update (March 4 2014)

During the investigation into stolen funds we have determined that the extent of the theft was enabled by a flaw within the front-end.

The attacker logged into the flexcoin front end from IP address 207.12.89.117 under a newly created username and deposited to address 1D6D3B3eB2wGZjZAwa2dqQ7M9v7AjwGLy

The coins were then left to sit until they had reached 6 confirmations.

The attacker then successfully exploited a flaw in the code which allows transfers between flexcoin users. By sending thousands of simultaneous requests, the attacker was able to "move" coins from one user account to another until the sending account was overdrawn, before balances were updated.

This was then repeated through multiple accounts, snowballing the amount, until the attacker withdrew the coins. (**Here** and **Here**)

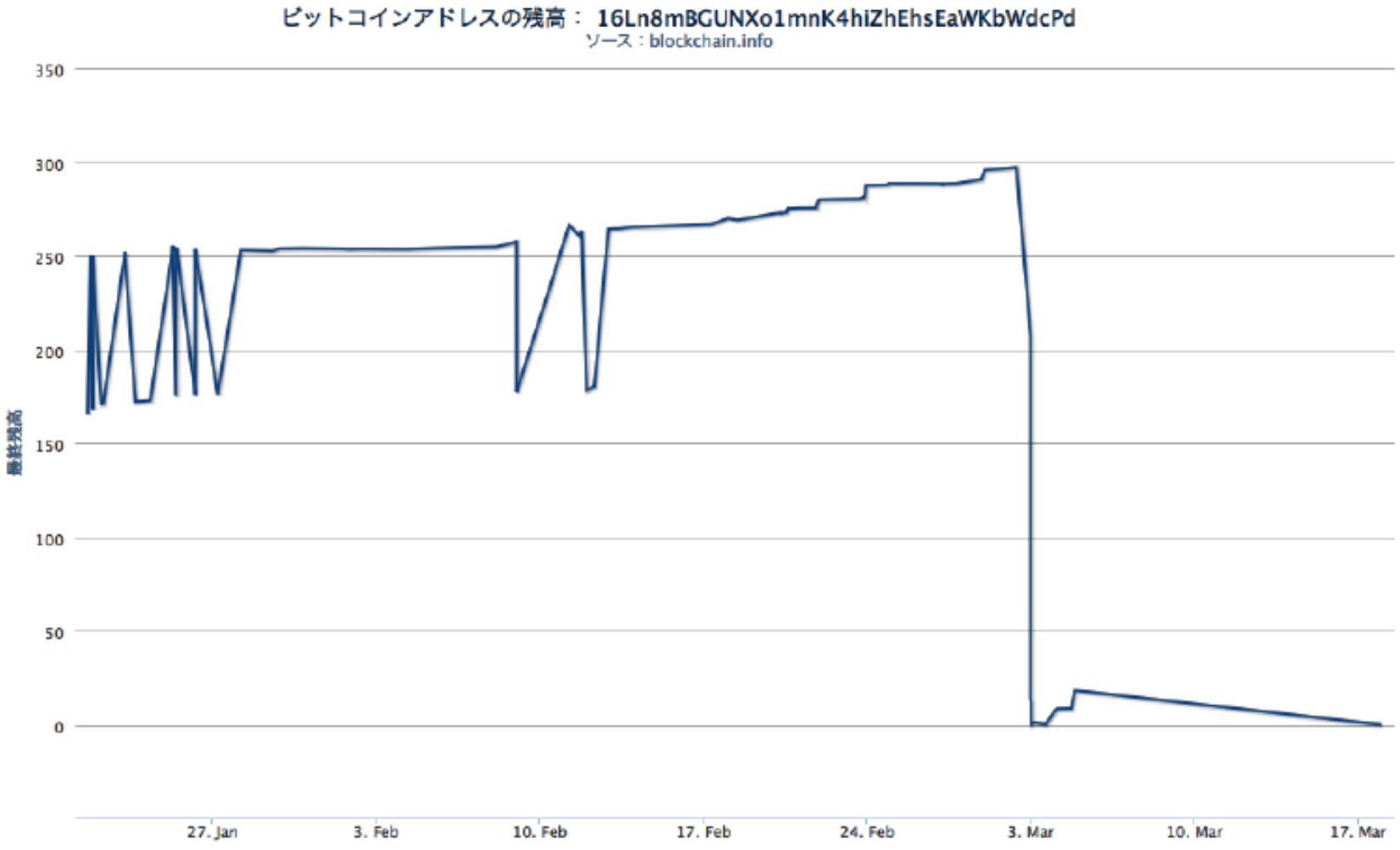
Flexcoin has made every attempt to keep our servers as secure as possible, including regular testing. In our ~3 years of existence we have successfully repelled thousands of attacks. But in the end, this was simply not enough.

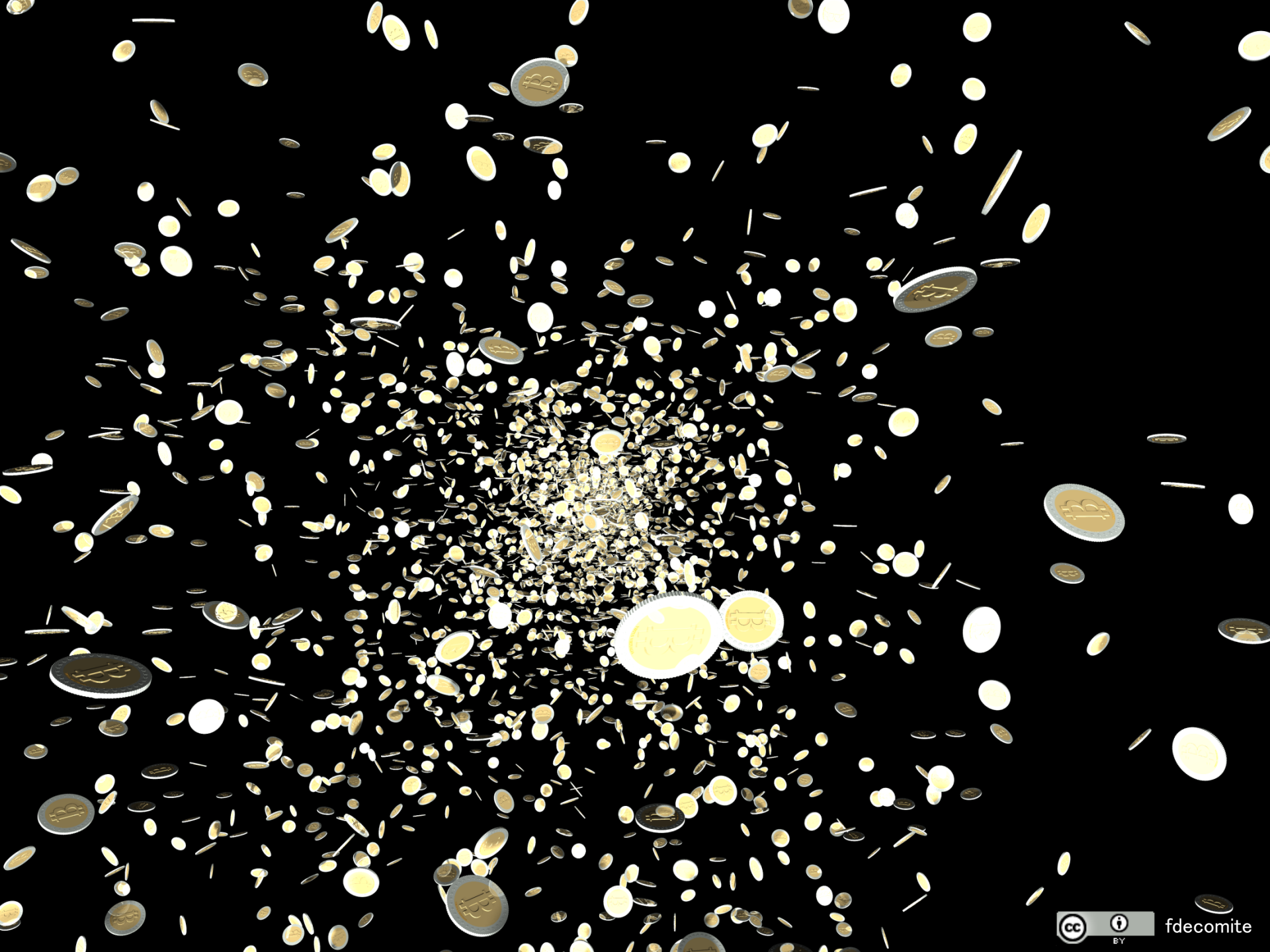
Having this be the demise of our small company, after the endless hours of work we've put in, was never our intent. We've failed our customers, our business, and ultimately the Bitcoin community.

Please direct any and all questions to admin(at)flexcoin(dot)com and we will reply to you as soon as possible.

http://www.slideshare.net/11ro_yamasaki/bitcoin-35192176

カナダflexcoin社の残高




fdecomite

貨幣発行自由化論
F. A. ハイエク著

1976

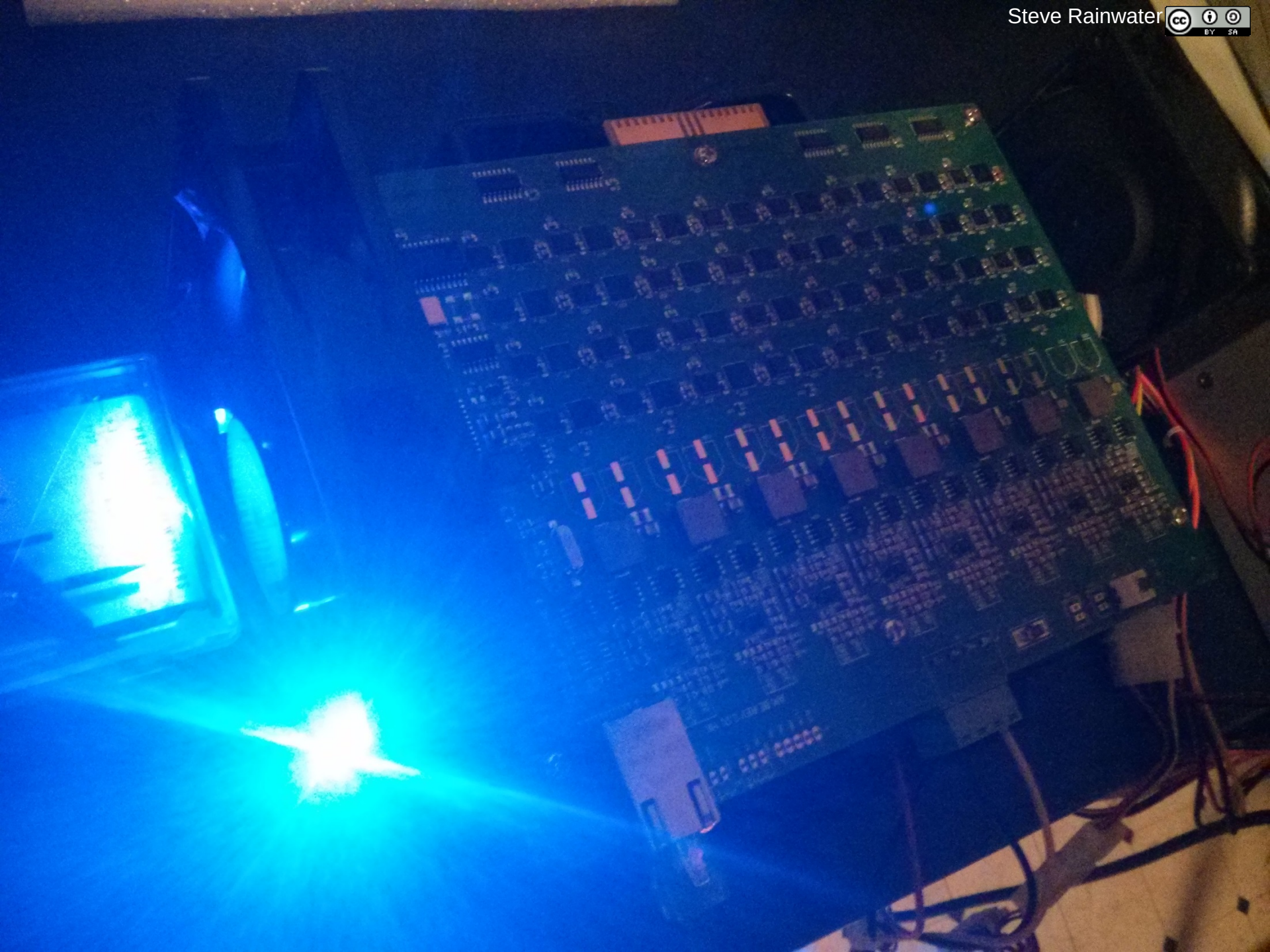
ジンバブエ通貨
100 Trillion Dollar

Steve Jurvetson

6. 発行

25BTC

Marko Ahtisaari


Steve Rainwater

分散型 ⇒ 独占型

信頼できる第三者機関
が存在しなくても
インターネット上を
流通する電子的価値

を、政府の力を借りずに実現する。

一人の大きな存在が
他を圧倒して
インターネット上を
支配する電子的価値

が、政府の規制なしに現実化する。

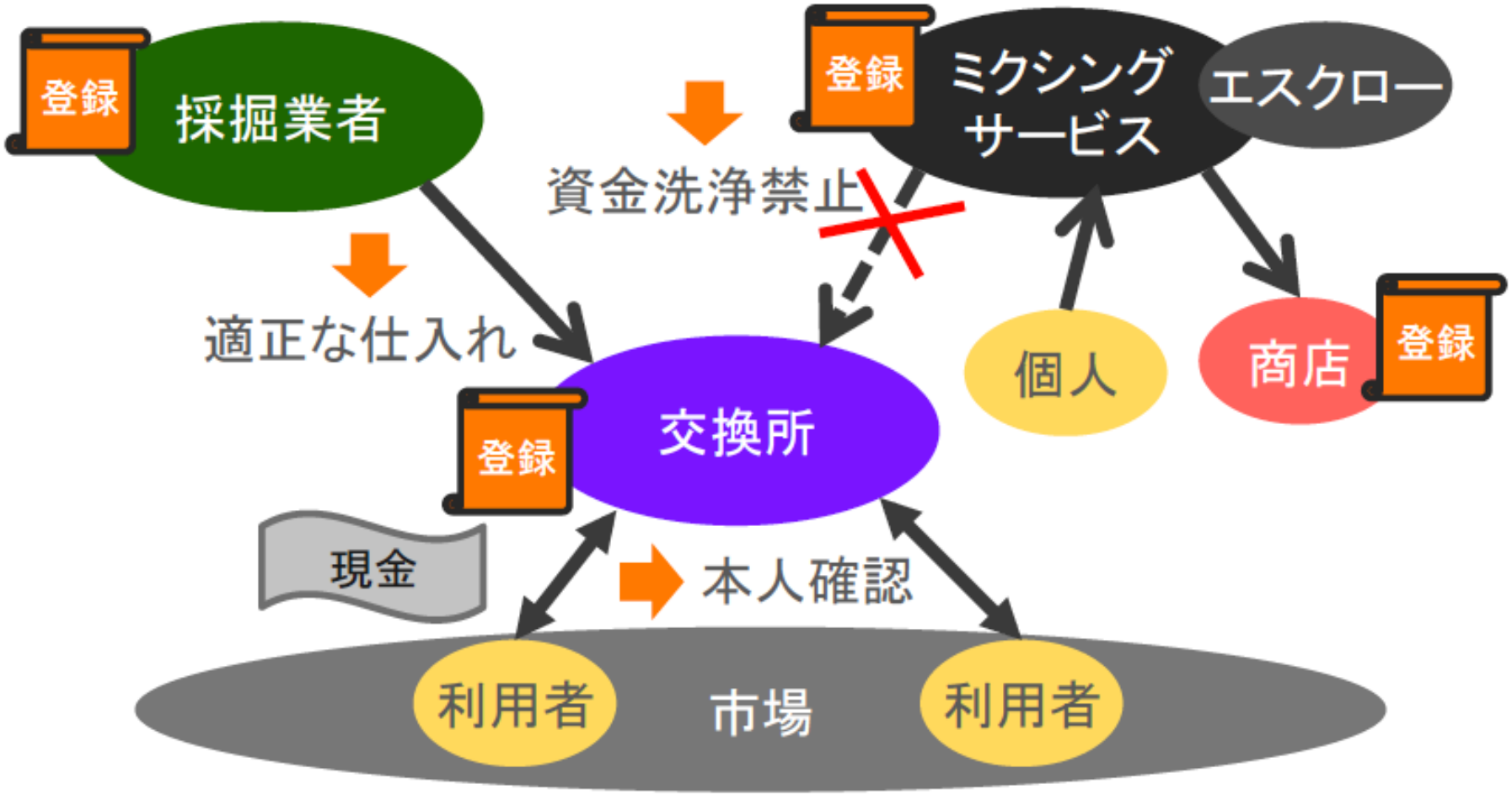
Adam Lang

仮想通貨は規制できるか

自主規制と共同規制

Bitcoinエコシステムの秩序

犯罪予防、利用者保護のための政府の関与
制度、規制



仮想通貨とはなんだったのか

21世紀のゴールドラッシュ

mlhradio （左上）

Tim Gillin（右上）

Mark Stevens（左）

マイニング風景

Archives New Zealand（左上）

Prayitno（右上）

Londahln（左）

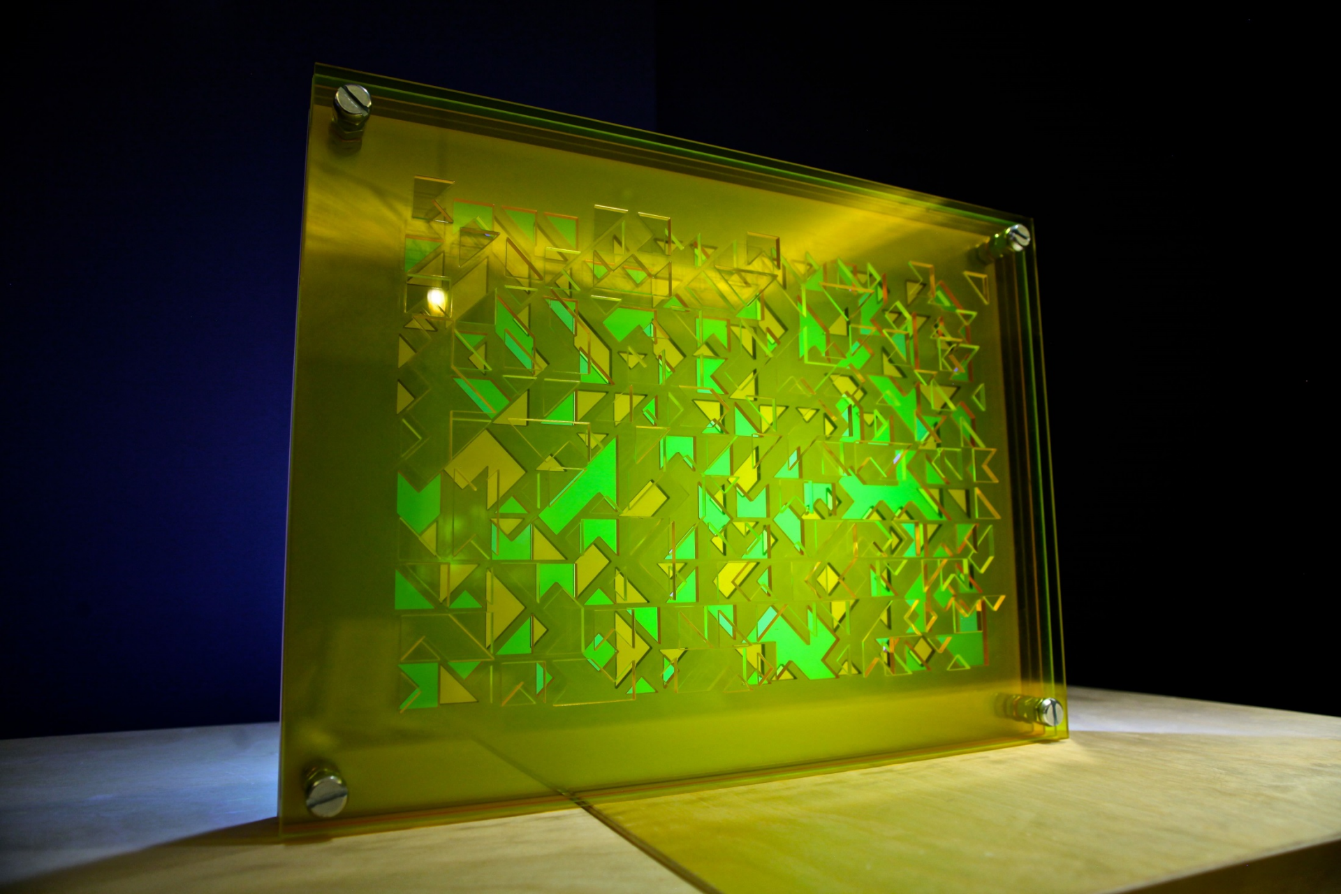
ステージコーチ画像
現金輸送・貨客兼用駅馬車

Ken Teegardin（左上）

sburke2478（右上）

Rojer（左）

駅馬車をシンボルマークに採用する米国の銀行



立体的に表現されたワンタイムパスワード

Stef Lewandowski

詳しい情報はこちらをご覧下さい

「ビットコイン」って何ですか？
「ビットコイン」創設の目的は
マイナビニュース
http://news.mynavi.jp/articles/2014/04/17/bitcoinokada/

Bitcoinにみる、分散型仮想通貨の仕組みと課題
～国立情報学研究所の記者説明会から～
Internet Watch
http://internet.watch.impress.co.jp/docs/news/20140520_649202.html

詳しい情報はこちらをご覧下さい

仮想通貨 VS 国家 ― ビットコインの衝撃

クローズアップ現代

NHKオンライン

http://www.nhk.or.jp/gendai/kiroku/detail_3455.html

仮想通貨は規制できるか

視点・論点

NHKオンライン

http://www.nhk.or.jp/kaisetsu-blog/400/183620.html

NII Citizens Seminar / June 26th, 2014

国立情報学研究所

情報社会相関研究系

岡田 仁志

http://www.nii.ac.jp/faculty/society/okada_hitoshi/