

*November 18<sup>th</sup>, 2015*

# 分散型仮想通貨の特性に適した レジリエントな制度設計

国立情報学研究所

情報社会相関研究系

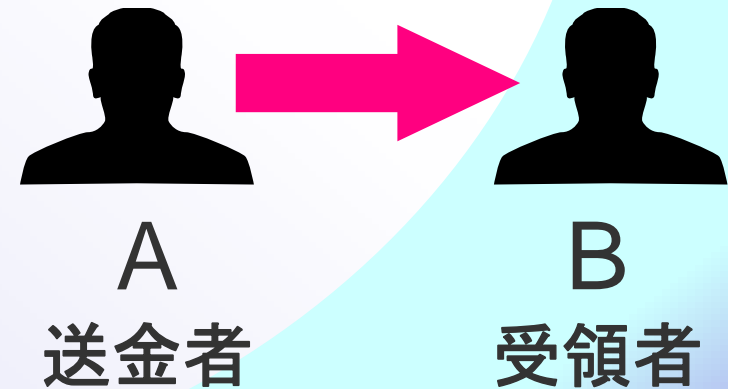
岡田 仁志

# ビットコインのエコシステム

# 1. 支払

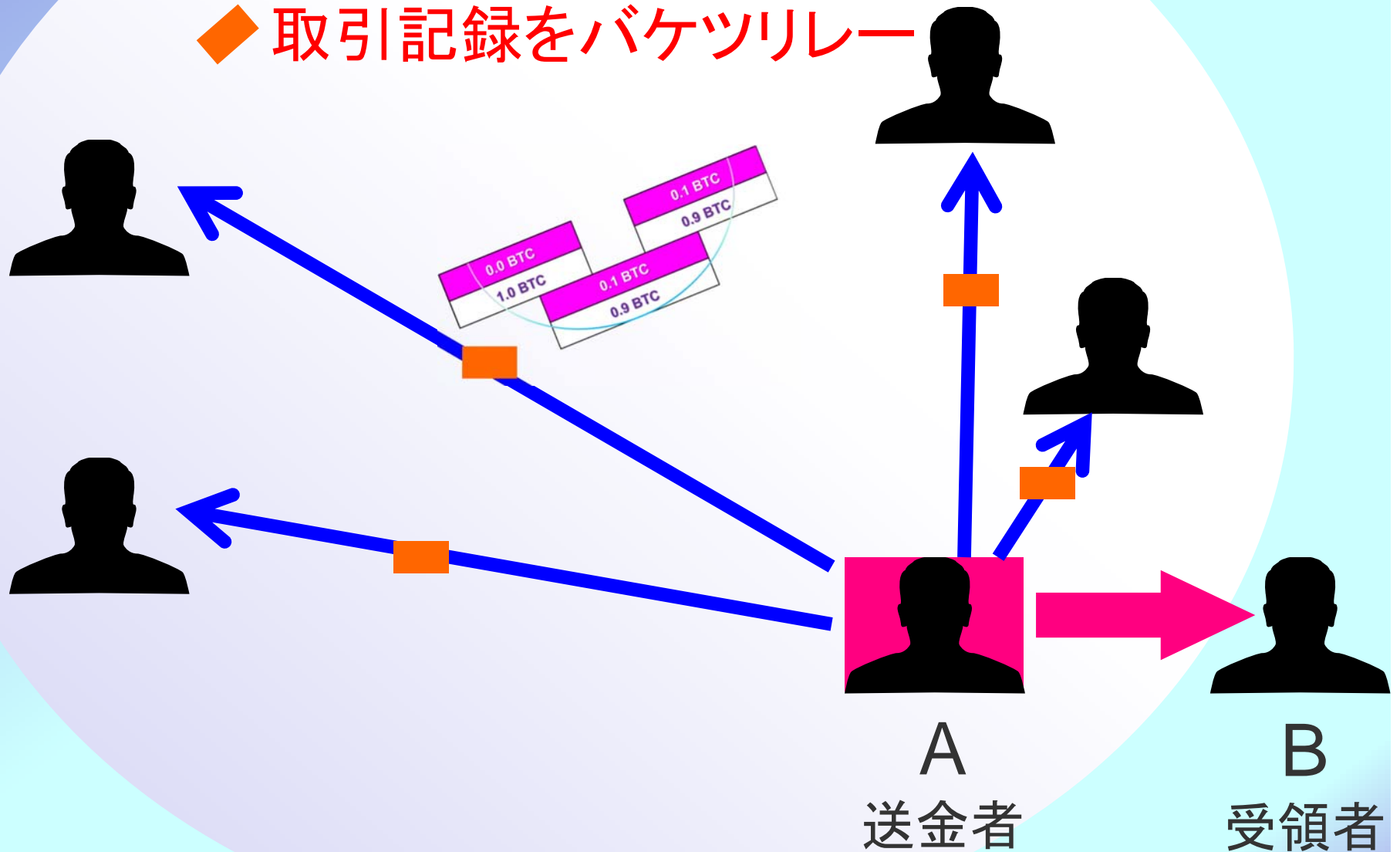
◆ 個から個への分散的な行為

AがBに0.1BTC  
支払った



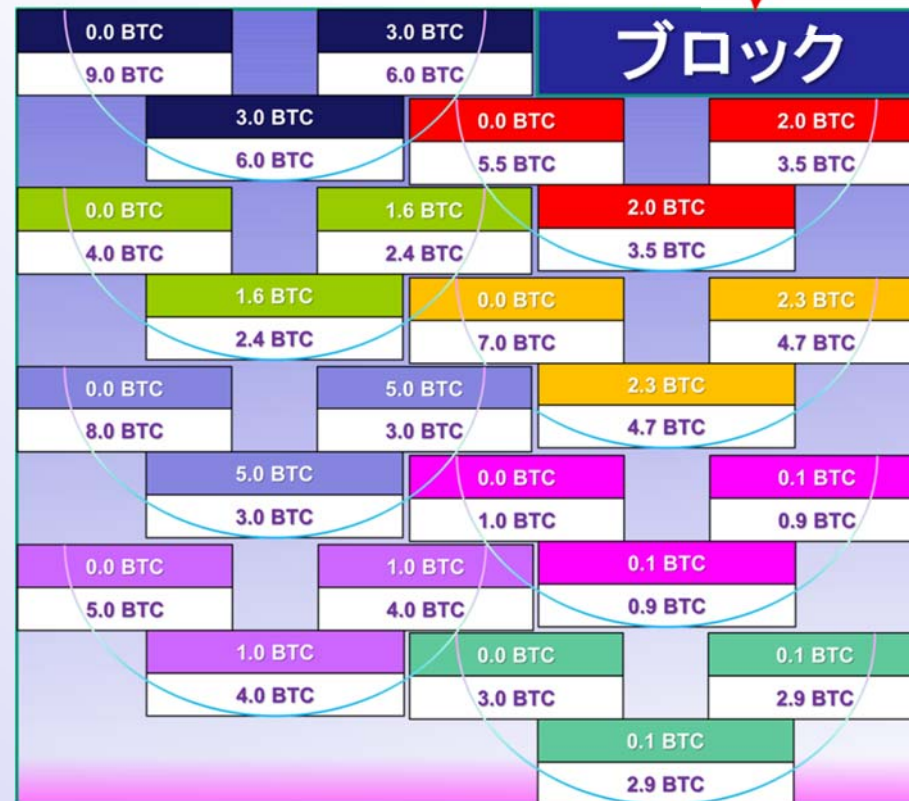
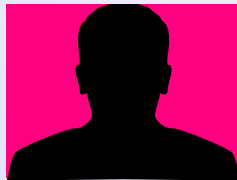
# 2.記録

◆取引記録をバケツリレー



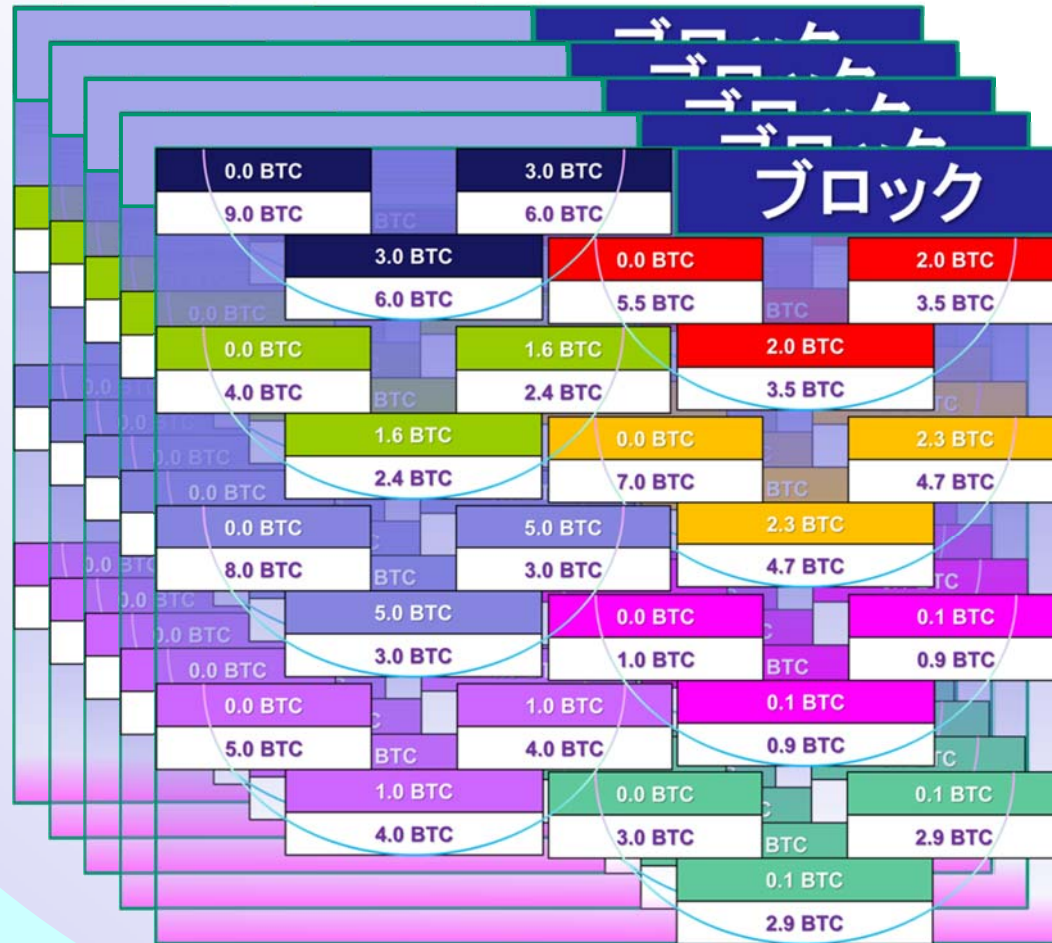
# 3. 採掘

◆ ブロックを競争的に生成



# 4.報酬

◆ ビットコイン大福帳の一冊に登録



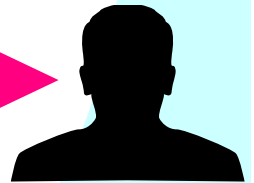
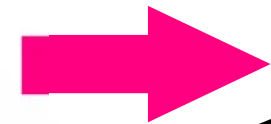
25BTC

# 5.承認

◆ ブロックに含まれる取引を正統化



A



B

# 6.発行

◆ 25BTCを、流通に載せる。



25BTC





# 集中と分散の振り子

# Bitcoin型採掘

◆ 誰でもマイニングに参加できる



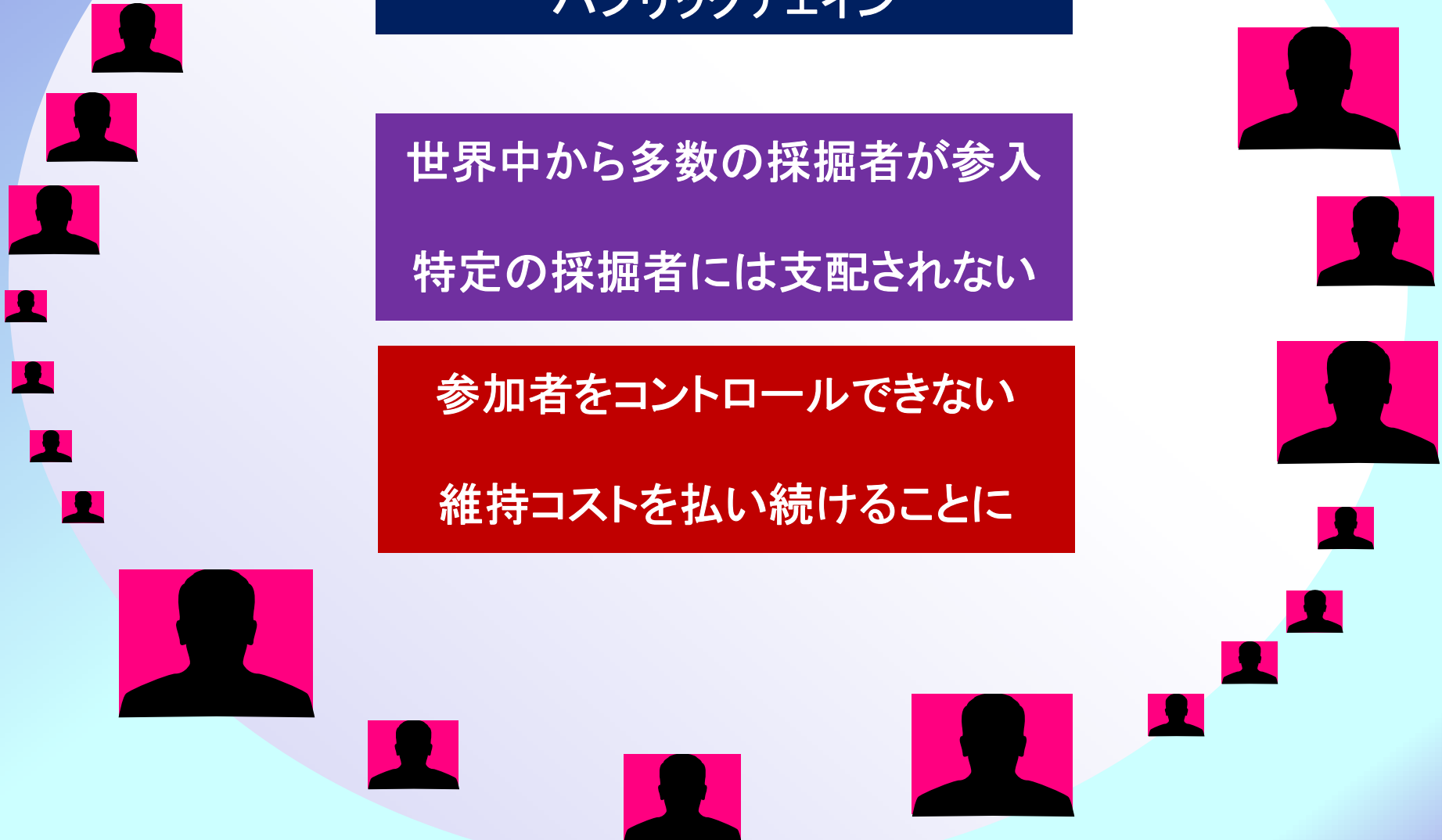
# Bitcoin型採掘

◆ 誰でもマイニングに参加できる

パブリックチェーン

世界中から多数の採掘者が参入  
特定の採掘者には支配されない

参加者をコントロールできない  
維持コストを払い続けることに

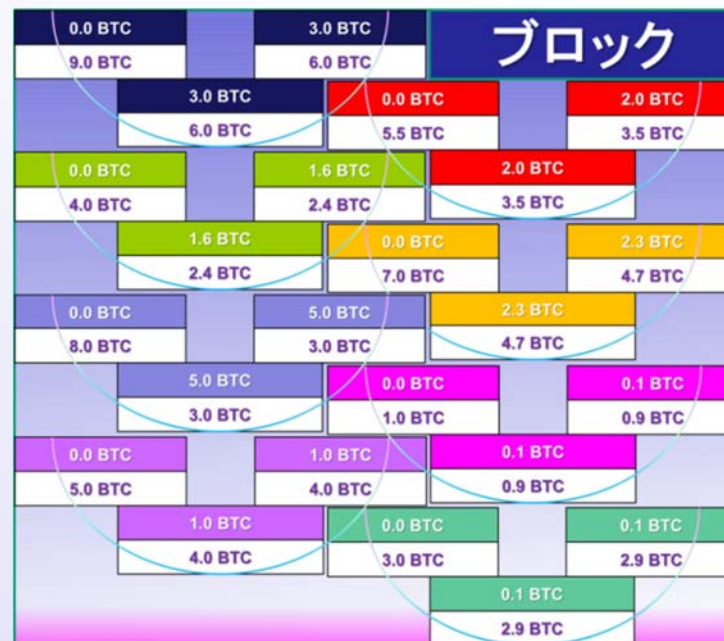
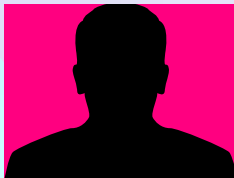
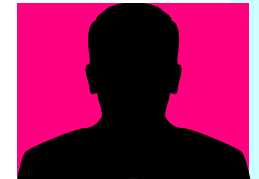
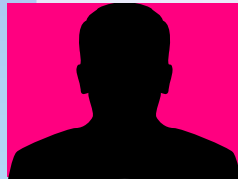


# コンソーシアム型

◆ 会員だけが採掘権を得る。



プライベートチェーン



# コンソーシアム型

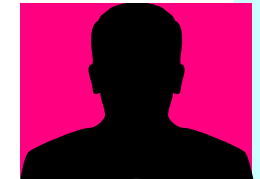
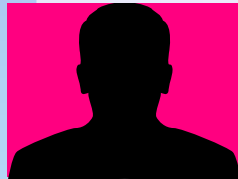
◆ 会員だけが採掘権を得る。



プライベートチェーン

信頼できる提携企業だけが参加

正体不明の参加者は存在しない



参加者が少数に限定される

「結託」による改ざんのリスク



# コンソーシアム型

◆ 会員だけが採掘権を得る。

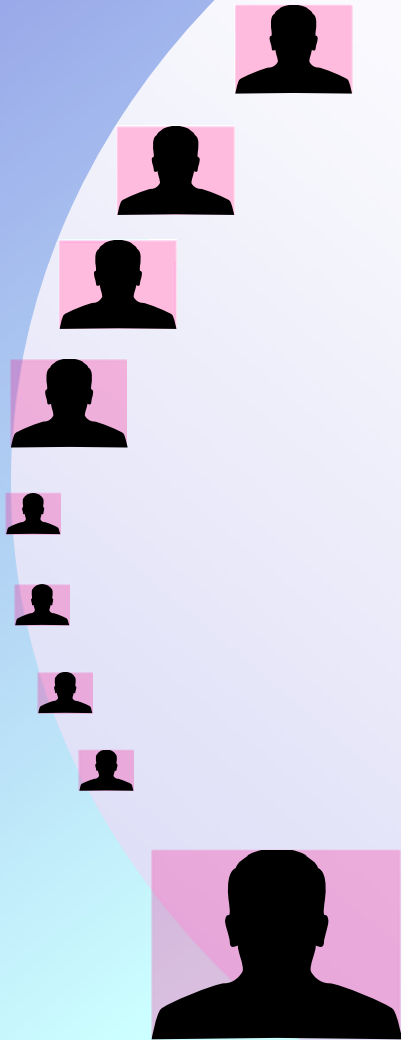
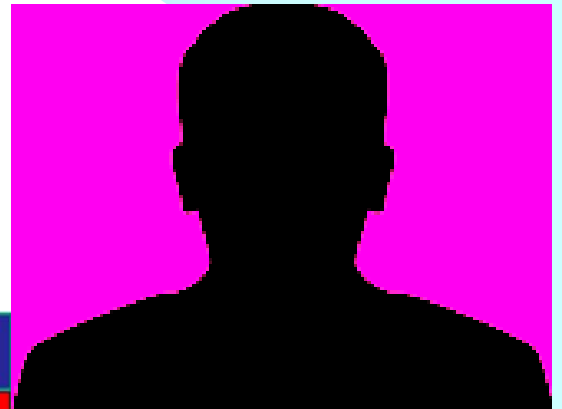
プライベートチェーン

信頼できる提携企業だけが参加  
正体不明の参加者は存在しない

採掘権を一般に開放する方式も

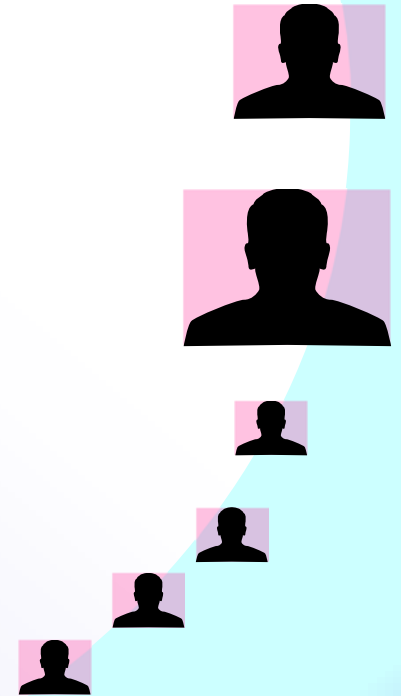
許可制 ⇔ 公開制

# 寡占型

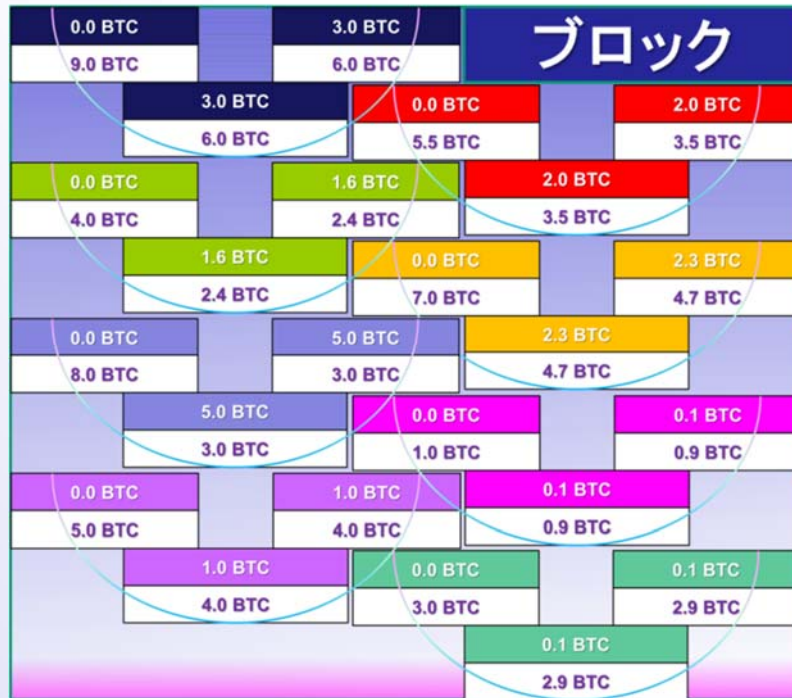


ブロック

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



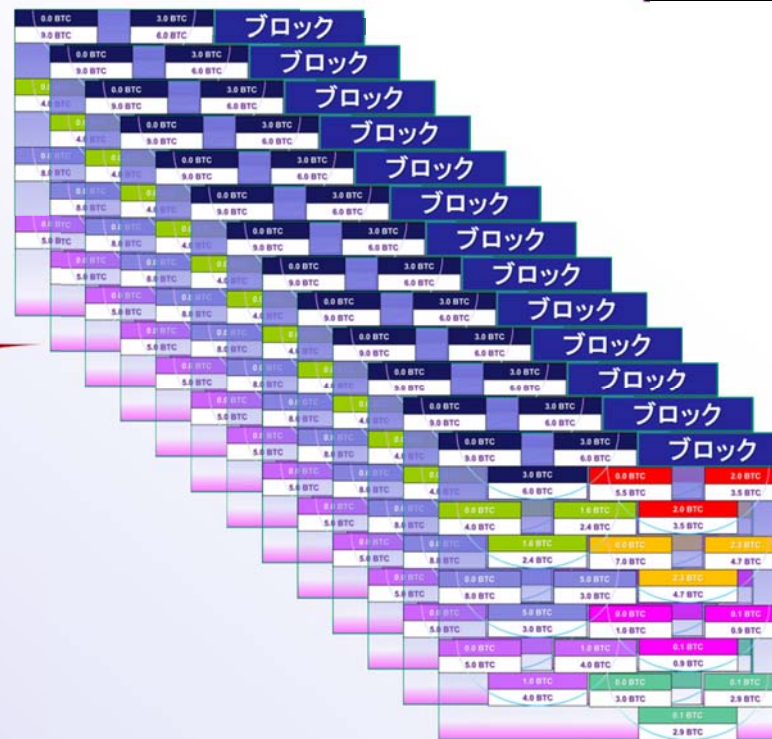
# 独占型





# 独占型

100% POS



V.C.

# プライベートチェーン

無数の「マイナー」が計算競争を行う代わりに、信頼できる1人または少数が、ブロックチェーンの「記録」の正しさの検証に関する責任を担う。

反社会的勢力の参加を防ぐことができる。

# パブリックチェーン

無数の「マイナー」達が計算競争を行うことで、ブロックチェーンの「記録」の正しさを不可逆に固定させる。

代表的なものとして、ビットコインがあげられる。

# サイドチェーン

何らかの仮想通貨を基軸通貨であると理解し、これに対してペグする二次的な仮想通貨。

債権債務関係を独自に定義できるメリットと、ブロックチェーンの記録の正しさを基軸通貨に依存できるメリットを兼ね備える。

# Sovereign Block Chain

イングランド銀行の「Old Money, New Money」と題する報告書は、仮想通貨時代の銀行の役割については歴史に遡って考察する。

仮想通貨の将来像として、民間の信用に依存した自由発行の世界と、国家を後ろ盾とした、ソブリン・デジタル・カレンシーの両方を論じる。

*Internet Week / November 18<sup>th</sup>, 2015*

国立情報学研究所  
情報社会相関研究系准教授  
岡田 仁志