

経済産業省・Fintech研究会資料

株式会社Orb

取締役COO 妹尾賢俊

チーフサイエンティスト 齊藤賢爾

2015年11月30日



orb

目次

1. ブロックチェーンとその特長
2. なぜ金融機関がブロックチェーンに注目するか
3. ブロックチェーンをめぐる金融機関等の動向
4. ブロックチェーンの主たる類型(管理者基準)
5. ブロックチェーンの主たる類型(CAP基準)
6. 「ビットコイン」ブロックチェーンの問題点
7. 金融システムに求められるブロックチェーンとは
8. ブロックチェーンを活用するにあたって

自己紹介

妹尾 賢俊(せのお ただとし)

株式会社Orb 共同創業者 兼 取締役COO

三菱東京UFJ銀行 勤務(1997-2007)

maneo株式会社 共同創業者 兼 代表取締役CEO(2007-2013)

齊藤 賢爾(さいとう けんじ) Ph.D.

株式会社Orb チーフサイエンティスト

慶應義塾大学SFC研究所 上席所員

P2P暗号通貨「i-WAT」開発。IPA未踏スーパークリエイター(2007年度)

ブロックチェーンとその特長

権利移転などの記録を公的に維持するデータベースであり、「公告」のプラットフォーム

【登記簿・官報との違い】

- 登記簿・官報は法務局等の信頼できる機関の第三者認証を経てその真正性が担保される。かつ、その基となるデータベースは当該機関において保持・更新される。
- 一方、ブロックチェーンにおいては、権利移転取引などの第三者認証を行うのは、特定の機関ではなくネットワークの参加者全員(全ノード＝全端末)。かつ、ブロックチェーンのデータベースは全ノードが同一のコピーを保持し、新たな記録が追加される度に全ノードのコピーが更新される。

【特長】

- 全ノードがコピーを保持しているため、一部ノードが壊れても、システム全体の稼働には影響がなく安定している。
- 一部ノードが壊れても、それを更新するだけで済むためメンテナンスコストが低い。
- 多数のノードが参加して取引内容を検証しているため、改ざんされる可能性が低い。

なぜ金融機関がブロックチェーンに注目するか

ブロックチェーンを使えば、安定的に稼働しかつ改ざん耐性を持つデータベース上で、権利や価値の移転取引を、低コストで運用できると考えているから。

権利や価値の移転取引は金融取引そのものではあるが、金融取引に限定されるわけではなく、応用範囲は広い。

ブロックチェーン技術：価値移転取引を分散ネットワーク上で改ざん困難な形で認証する技術

現在の主たる用途：ビットコイン等の仮想通貨（価値保蔵、交換・支払）

金融分野で期待される応用例

送金・決済	法定通貨での送金・決済網
株式・社債	発行体による直接発行、 相対取引での流通
信託	配当、名義書換の自動化 暦年贈与信託の自動化

金融分野以外で期待される応用例

登記	所有権移転登記 (不動産、自動車等)
文書・公証	タイムスタンプ付存在証明
IoT	予約条件に従い、動作実行 (IBM Adept)

ブロックチェーンをめぐる金融機関等の動向

	名称	取組み	時期
銀行等	R3CEV	30金融機関が参加する分散型台帳を活用した金融プラットフォームの研究開発	2015年9月
	Citi	ブロックチェーン技術をベースにしたデジタル通貨関連システムCiticoinsを実験中	2015年7月
	USAA	バックオフィス業務効率化のためのブロックチェーン研究チーム立ち上げ	2015年5月
	BNY Mellon	社内で社員向け報奨プログラムとして独自コイン発行を行う等、同技術を実験中	2015年4月
	Deutsche Bank	8領域をターゲットにブロックチェーン技術調査に着手	2015年7月
	Barclays	ブロックチェーン関連ベンチャーSafello社(スウェーデン)と協働開始	2015年6月
	BNP Paribas	ポストレード処理効率化のためにブロックチェーン技術を実証中	2015年7月
	ING Bank	セキュリティ向上目的でブロックチェーン認証を実験	2015年7月
	UBS	ブロックチェーン研究ラボをロンドンに開設、スマート債券、リーガソン開催	2015年4月
	DBS	IBMと共同でブロックチェーン技術に関するハッカソン開催	2015年5月
証券他	NASDAQ	未公開株式市場プラットフォーム「Inq」、Chain.comと協働	2015年6月
	SWIFT	ブロックチェーンを使った送金ネットワーク研究	2015年7月
	VISA	ブロックチェーンの研究着手(米、印、シンガポール3拠点)	2015年8月
中銀等	イングランド中央銀行	ビットコインフォーラムメンバーに	2015年5月
	欧州銀行協会(EBA)	ブロックチェーン関連レポート公開	2015年5月
	FRB他主要中央銀行	ブロックチェーンを使った通貨のデジタル化と決済ネットワークの構築に関してIBMと非公式協議	2015年3月
	シンガポール金融管理局	FinTechハブとなるべく225Mドルの投資計画表明	2015年7月

ブロックチェーンの主たる類型（管理者基準）

森・濱田松本法律事務所 増島雅和弁護士作成の表を当方にてアレンジ

	パブリック型	プライベート型	コンソーシアム型
管理者の有無	なし	あり・単独	あり・相互に信頼関係にある複数の主体
ノード参加	自由 (Permission less)	管理者による許可制 (Permissioned)	管理者による許可制 (Permissioned)
認証に求められる合意形成の厳格さ	厳格 (例: 作業証明)	必ずしも厳格でなくてもよい (管理者次第)	必ずしも厳格でなくてもよい (管理者次第)
認証時間 ^(注)	遅い	早くできる	早くできる
一定時間内に処理できる取引量 ^(注)	少ない	多くできる	多くできる

↑
ビットコイン

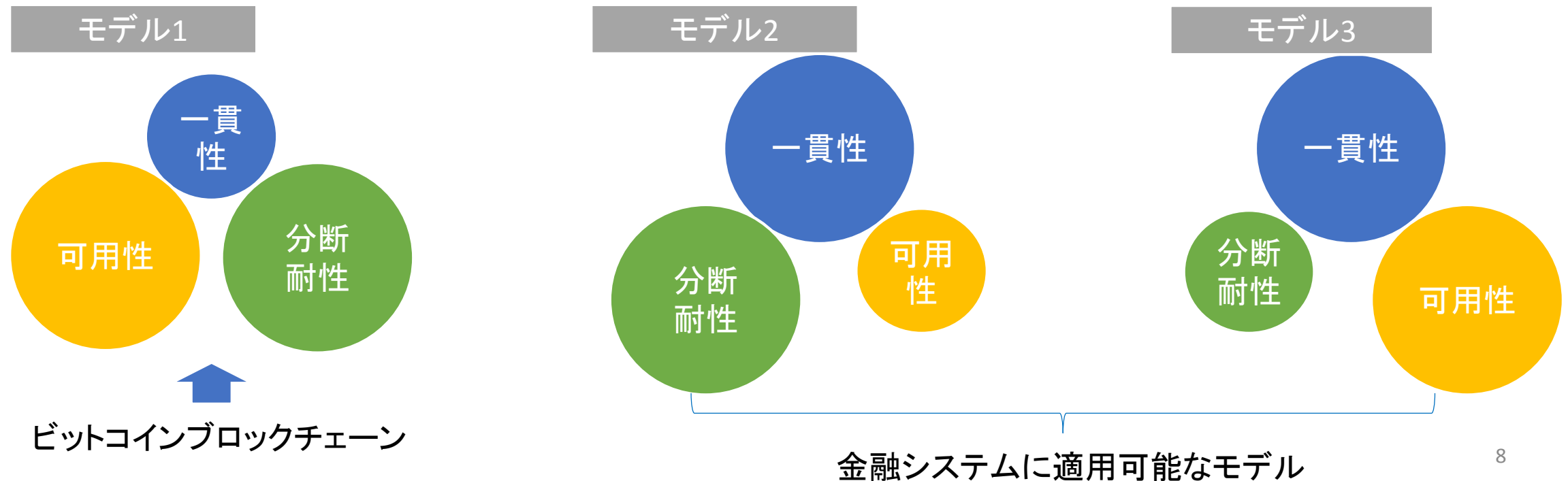
↑
金融機関による利用が想定されるモデル

(注) 認証時間と取引量は、パブリック型とプライベート型・コンソーシアム型を同一環境で比較し、かつ、プライベート型・コンソーシアム型の合意形成の厳格さがパブリック型に比較して緩和された場合の相対的なもの。

ブロックチェーンの主たる類型(CAP基準)

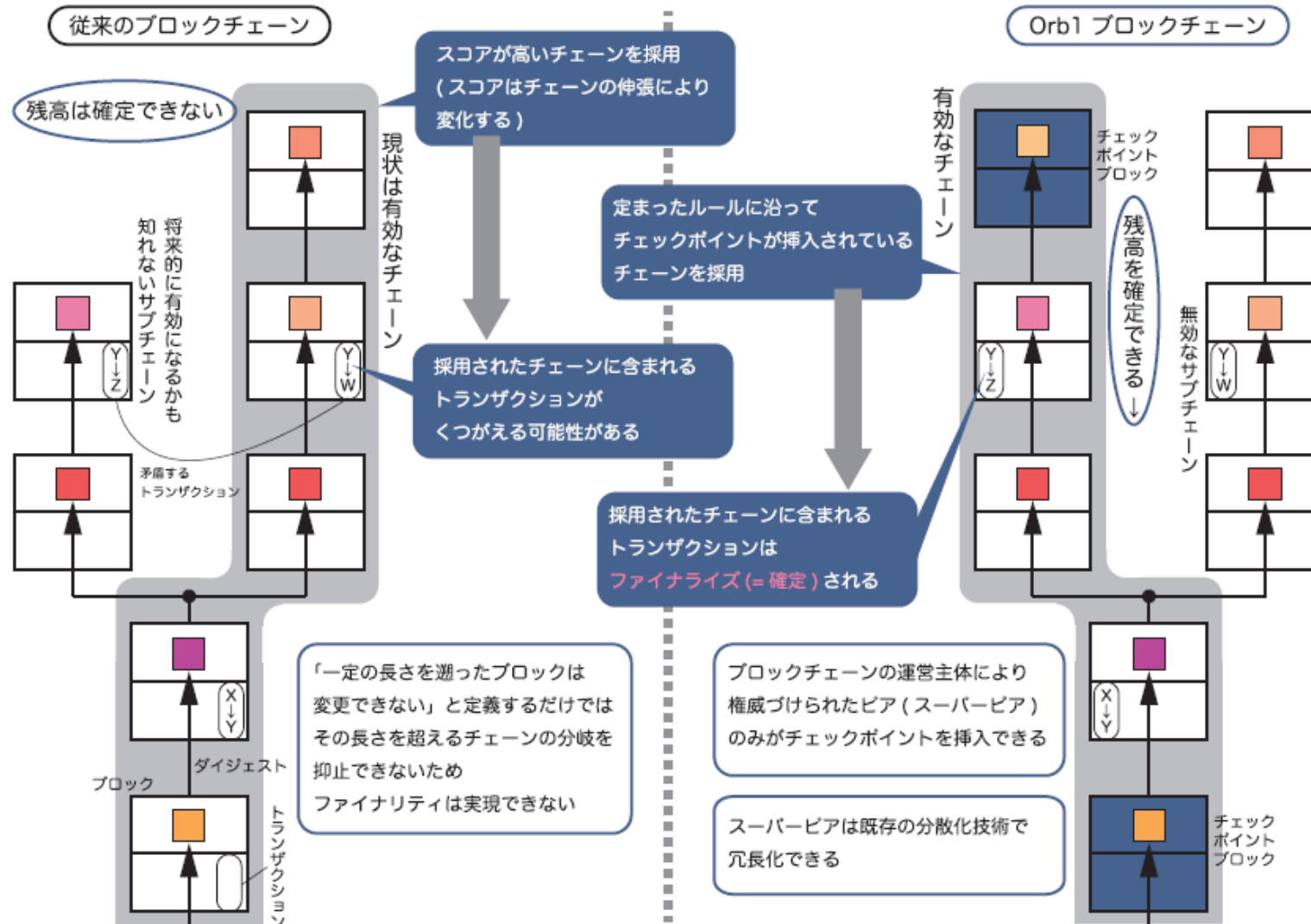
ノード間でデータの複製・共有を行うシステムの場合(ブロックチェーンもその一つ)、以下の3つのモデルから一つを選ばなければならない(以下の3つの性質を同時に満たすことはできない)。

- 一貫性(Consistency): 合意したデータを全てのノードにおいて同時に参照でき、一度合意したデータが遡及的に変化しないこと
- 可用性(Availability): 一部のノードが故障しても、他のノードが生存している限り応答し続けること
- 分断耐性(Partition tolerance): ノード間のネットワークが(障害等で)分断されても、システムが動くこと

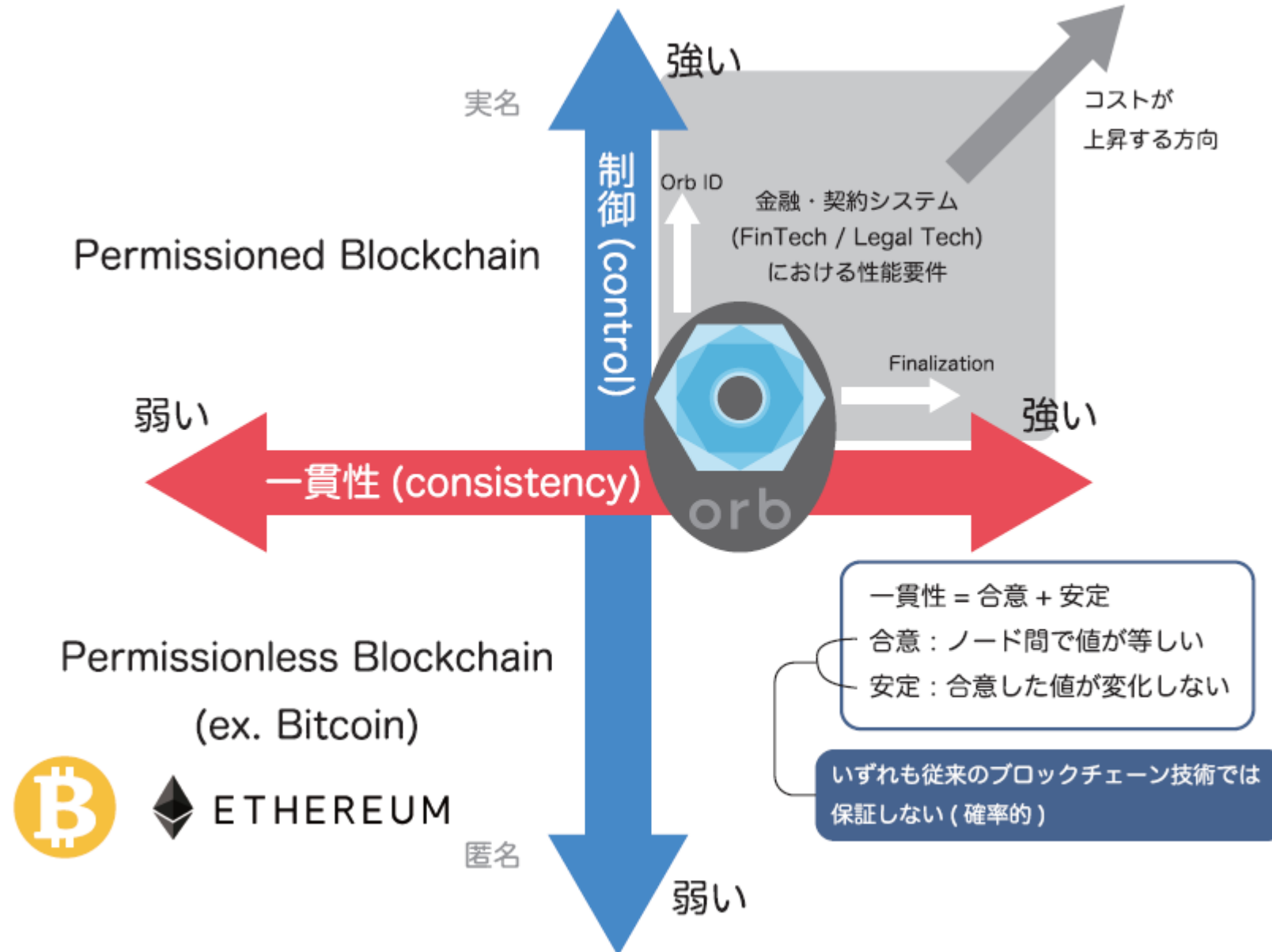


「ビットコイン」ブロックチェーンの問題点

一貫性がない(=データが確定しない) → 金融システムに使えるのか？



金融システムに求められるブロックチェーンとは



ブロックチェーンを活用するにあたって

ブロックチェーン(あるいは分散型台帳)は様々な分野でもの応用可能性が高い技術であることは確か。

ただし、活用にあたっては「何をしたいのか」を明確にすることが大事。

「何をしたいのか」が決まれば、

- ・一貫性(データ確定性)
- ・可用性
- ・分断耐性
- ・コスト(構築・運用コスト)

といった要件のバランスを考慮してシステムの設計可能性を検討できる。