

暗号通貨・ブロックチェーン技術と その応用可能性

田中 圭介

東京工業大学 情報理工学院

サイバーセキュリティ研究センター

蔵前技術士会 第175回例会・講演会

東工大蔵前会館ロイヤルブルーホール

2018年9月10日

ビットコイン



- Satoshi Nakamoto (2008) が提案
- 信頼できる第三者を置かずに実現可能な暗号通貨
 - 非中央集権的に実現
- 基礎となる技術はブロックチェーン・分散型台帳などと呼ばれる
- 暗号理論、分散システム理論、ゲーム理論を技術背景としてもつ

Satoshi Nakamoto 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

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

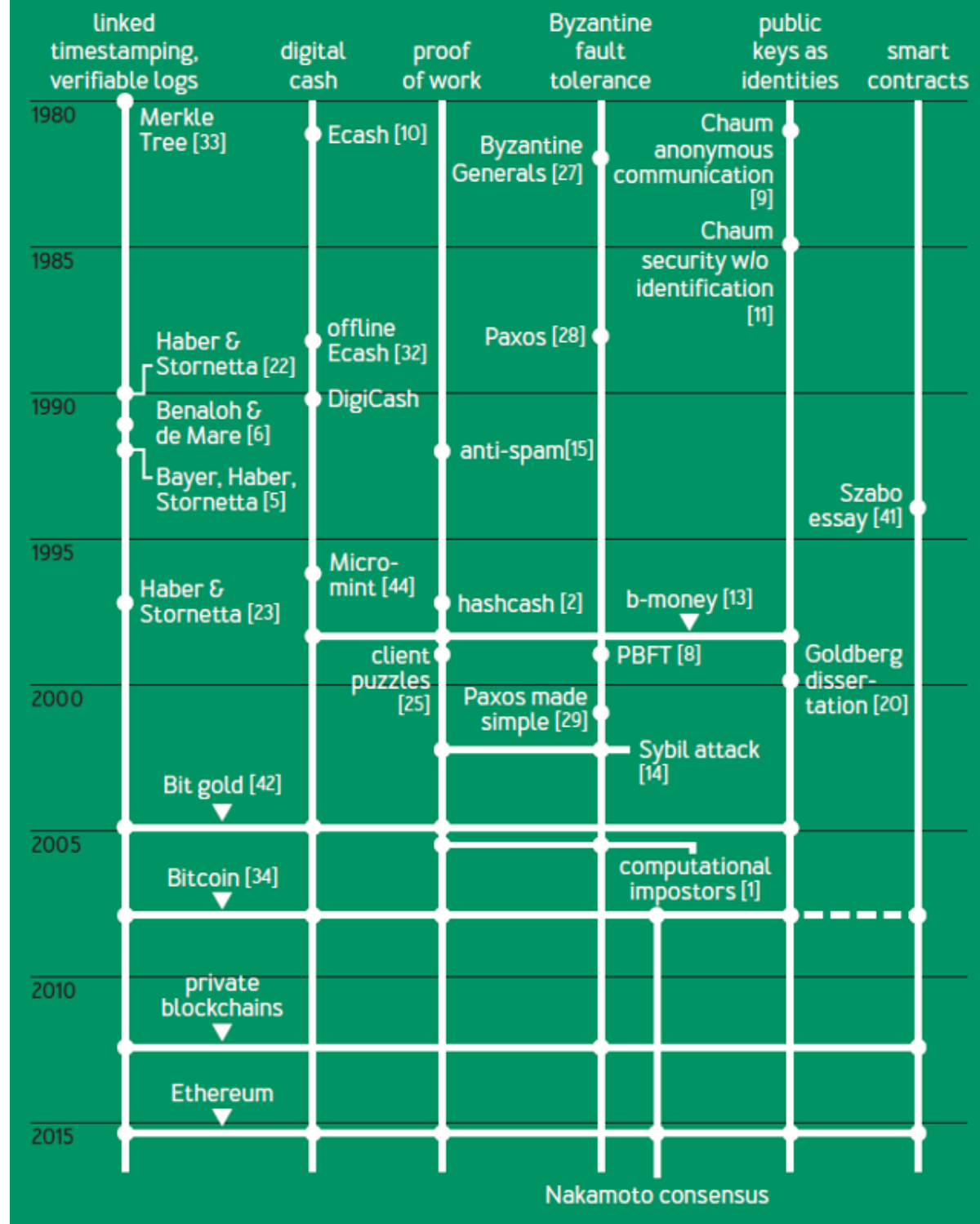
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot

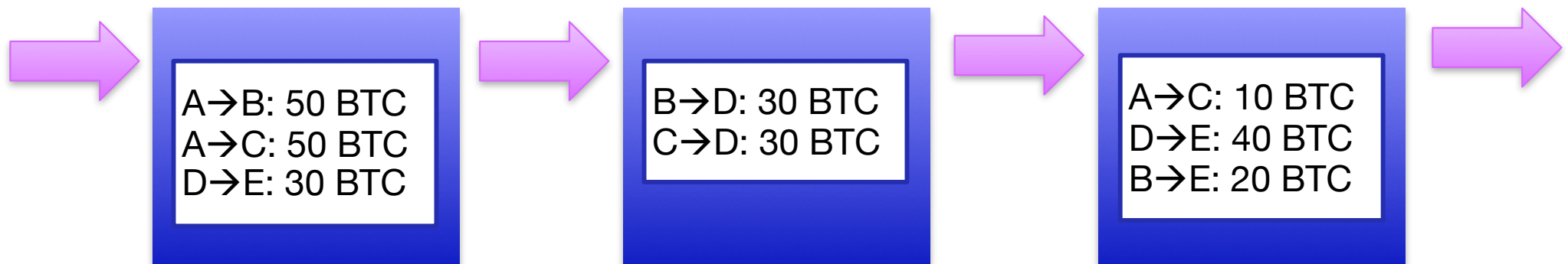
暗号通貨の 学術的背景

A. Narayanan
and J. Clark,
“Bitcoin’s
Academic
Pedigree”,
ACM Queue
Magazine:
August/2017



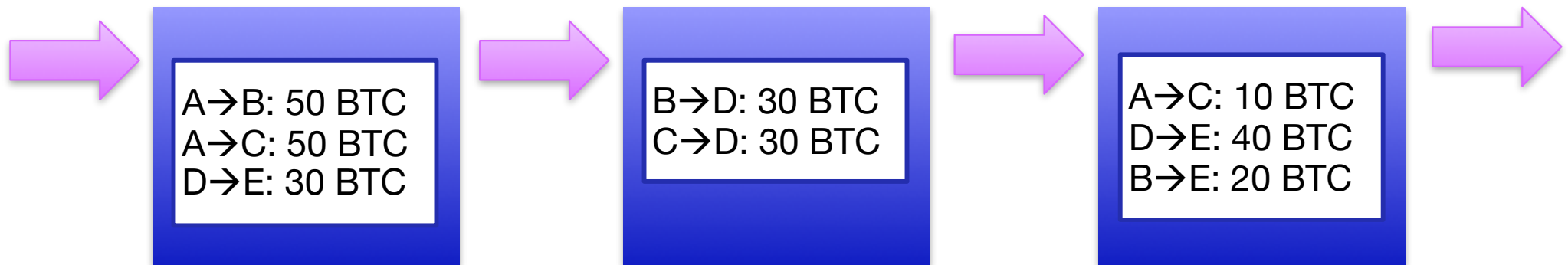
ブロックチェーン・分散型台帳の概要

- 各参加者がある種の計算 (Proof-of-Work) を行い続けることで、情報（台帳）を共有する技術
 - 台帳 = 追記専用のログ
 - ビットコインでは、取引（トランザクション）情報を台帳に記載
 - 追記の際に、二重支払い等の送金に関わる不正をチェック
 - 送金者の電子署名が必要なため、送金偽造は困難
- 信頼できる第三者を必要としない
- 一般的には低コスト
- 公開鍵と特定個人との結びつきは保証されていない



チェーンを1ブロック伸ばす手順

- 手に入れたトランザクションを組み込んでブロックの中身をつくる
 - トランザクションの正当性も検証
- ブロックの中身が出来上がったらブロックをチェーンに接続するために **Proof-of-Work (PoW)** を行う (**マイニング**とも呼ばれる)
 - 少し時間の掛かるパズルを解く (答えの正しさは簡単に確認可能)
- PoWに成功したら結果を参加メンバーにブロードキャストする
- 6ブロック後に確定する
 - 分岐する可能性もある
 - もっとも長いチェーンが生き残る

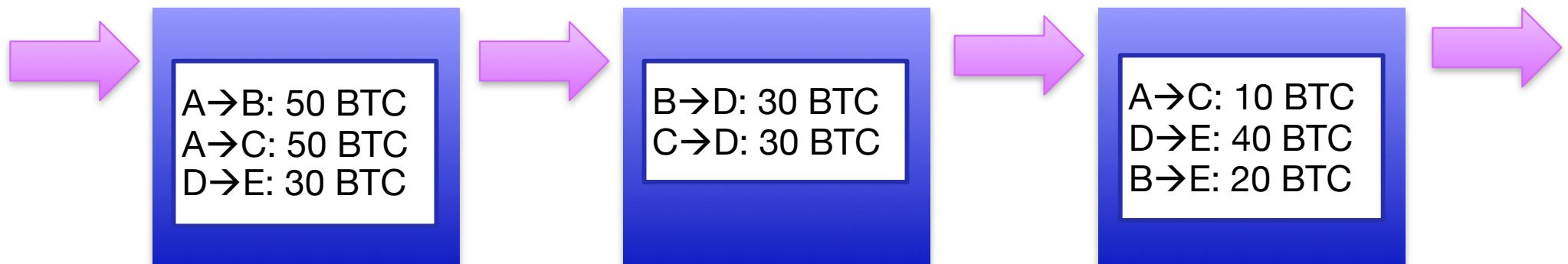


NakamotoプロトコルのProof of Workパート

- ランダムオラクル $H: \{0,1\}^* \rightarrow \{0,1\}^\kappa$ によるモデル化
- ブロック $b = (h_{-1}, n, \vec{m}, h)$
 - h_{-1} : 直前ブロックへのポインタ, n : ノンス, \vec{m} : メッセージ系列, h : 現在のブロックへのポインタ
- 困難性パラメータ p : 定数 $D_p = p(\kappa)2^\kappa$ が定まる
 - $\forall (h, b), \Pr_n[H(h, n, b) < D_p] = p(\kappa)$
- $b = (h_{-1}, n, \vec{m}, h)$ が valid w.r.t. $b_{-1} = (h'_{-1}, n', \vec{m}', h')$
 \Leftrightarrow (1) $h_{-1} = h'$ (2) $h = H(h_{-1}, n, \vec{m})$ (3) $h < D_p$
- ブロックチェーン $BC = (b_0, b_1, \dots)$ が valid
 \Leftrightarrow (1) $b_0 = (0, 0, \perp, H(0, 0, \perp))$ (2) $\forall i, b_i$ が valid w.r.t. b_{i-1}
(3) ブロック内メッセージ系列が valid

Proof of Work で実際に行なっていること

- ハッシュ関数 (ランダムオラクル) H の入力
 - 前のブロックへのポインタ
 - 追加するブロックの中身 (署名つきトランザクションの集合)
 - 数 (ナンス)
- 出力が000000083729などの決められた閾値以下の数になるような数 (ナンス) を見つければ成功
- トランザクションについての署名が正しいことの検証
- トランザクション内容がこれまでと矛盾しないことの検証



ビットコインと報酬設定 (1)

- システム全体でおよそ10分に1回しかPoWに成功しない
- 前回分のマイニング計算履歴は、次回分のマイニング計算に生かせない
- マイニングの成功に対して報酬を与え、PoW を行うことのインセンティブを付与
- マイニングの報酬に加えて別途、個別取引の手数料も受け取る
 - 個別取引の手数料は取引毎に自由に決められる

マイニングの報酬設定 (2)

- 現在のマイニング報酬は12.5 BTC (1 BTC = 約850,000円)
- 4年に1度程度、報酬が半減する (21万ブロック毎)
 - 最初の報酬は50 BTC
 - 発行上限が決まっている
 - cf. イーサリアムやリップルには半減期が存在しない
- 安定した報酬は得られない
 - 多くのマイナーはマイニングプールに参加して安定した報酬を受け取ることを望む

マイニングプール

- 協力してマイニングを行うマイナーの集団
 - 安定した報酬を受け取ることが目的
 - cf. 資金のみ提供するタイプのマイナー集団もある
- 大規模なマイニングプールの危険性
 - ビットコインでは上位3つのプールが過半数を占める
 - 51%ルールに抵触する危険性
- 「51%ルール」とは
 - 計算資源の半数を不正者が占めると破綻の可能性
 - 不正者に都合のよい分岐が正しいチェーンとなる
- マイニングプール内で利益を得る戦略もある

マイニング報酬が少なくなったときには

- マイニング報酬と取引報酬のバランス
 - マイニング報酬は4年で半減
- ある時点で取引手数料 100 BTC 分の取引が確定せずに残っているとする
- 取引手数料 90 BTC 分の取引がチェーンの最後に記録され、10 BTC 分の取引が残っているとき
 - (1) そのチェーンの次に 10 BTC 分の取引をマイニングする
 - (2) 1 つ前に戻って枝分かれさせ 100 BTC 分の取引をマイニングするか
- マイナーにとって様々な戦略が存在してしまう
- 取引手数料が時間によって異なることの不安定性

暗号通貨のインセンティブ設定の課題 + a

- ビットコインにはブロック報酬と取引報酬がある
- インセンティブ設定、すなわち、報酬の設定方法・妥当性は未解明
- 暗号通貨・ブロックチェーン技術は様々な応用をもつ
 - 暗号通貨以外で利用するときの報酬は？
 - 暗号通貨と法定通貨をペッグしたときにシステムは動く？
- インフレとデフレの抑制効果は？
 - 通貨発行量は動的に決めるべき？
- Proof of Work 以外によるブロックの更新
 - 例: Proof of Stakes (「所有量」によるマイニング権利の獲得)
- 匿名性の確保
 - ビットコインは取引内容をすべて公開・共有
- システムが正しく実装されていることの検証は？

ブロックチェーンの活用例

■ ブロックチェーン技術活用のユースケース

金融系 <ul style="list-style-type: none"> 決済 (SETL、FactoryBanking) 為替・送金・貯蓄等 (Ripple、Stellar) 証券取引 (Overstock、Symbiont、BitShares、Mirror、Hedgy) bitcoin取引 (itbit、Coinffeine) ソーシャルバンキング (ROSCA) 移民向け送金 (Toast) 新興国向け送金 (Bitpesa) イスラム向け送金/シャリア遵法 (Abra、Blossoms) 	ポイント／リワード <ul style="list-style-type: none"> ギフトカード交換 (GyftBlock) アーティスト向けリワード (PopChest) プリペイドカード (BuyAnyCoin) リワードトークン (Ribbit Rewards) 	資産管理 <ul style="list-style-type: none"> bitcoinによる資産管理 (Uphold(旧Bitreserve)) 土地登記等の公証 (Factom) 	商流管理 <ul style="list-style-type: none"> サプライチェーン (Skuchain) トラッキング管理 (Provenance) マーケットプレイス (OpenBazaar) 金保管 (Bitgold) ダイヤモンドの所有権 (Everledger) デジタルアセット管理・移転 (Colu) 	公共 <ul style="list-style-type: none"> 市政予算の可視化 (Mayors Chain) 投票 (Neutral Voting Bloc) バーチャル国家/宇宙開発 (BitNation/Spacechain) ベーシックインカム (GroupCurrency)
		ストレージ <ul style="list-style-type: none"> データの保管 (Stroj、BigchainDB) 		
	資金調達 <ul style="list-style-type: none"> アーティストエクイティ取引 (PeerTracks) クラウドファンディング (Swarm) 	認証 <ul style="list-style-type: none"> デジタルID (ShoCard、OneName) アート作品所有権/真贋証明 (Ascribe/VeriSart) 薬品の真贋証明 (Block Verify) 		医療 <ul style="list-style-type: none"> 医療情報 (BitHealth)
	コミュニケーション <ul style="list-style-type: none"> SNS (Synereo、Reveal) メッセージ、取引 (Getgems、Sendchat) 	シェアリング <ul style="list-style-type: none"> ライドシェアリング (La'ZooZ) 	コンテンツ <ul style="list-style-type: none"> ストリーミング (Streamium) ゲーム (Spells of Genesis、Voxelnauts) 	IoT <ul style="list-style-type: none"> IoT (Adept、Filament) マイニング電球 (BitFury) マイニングチップ (21 Inc.)
			将来予測 <ul style="list-style-type: none"> 未来予測、市場予測 (Augur) 	

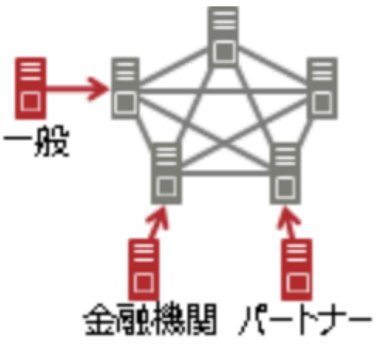
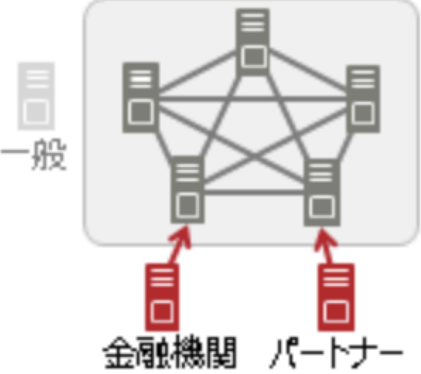
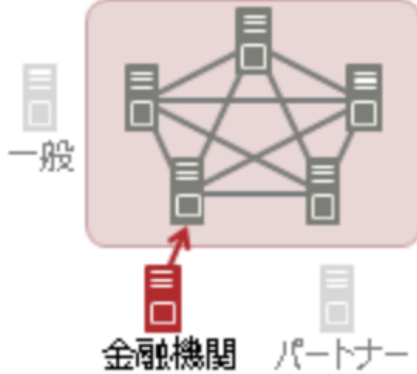
出典：経済産業省 商務情報政策局 情報経済課「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備 (ブロックチェーン技術を利用したサービスに関する国内外動向調査) 報告書概要資料」

ブロックチェーン技術の展開が有望な事例とその市場規模



出典：経済産業省 商務情報政策局 情報経済課「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備 (ブロックチェーン技術を利用したサービスに関する国内外動向調査) 報告書概要資料」

コンソーシアム型とプライベート型

	パブリック	コンソーシアム	プライベート
			
管理者の有無	なし	あり (複数企業)	あり (単独)
BCN (※1) 参加者	不特定多数 (Permission less)	特定複数 (Permissioned)	組織内 (Permissioned)
合意形成の仕組み	PoW / PoS (※2) など (厳格な承認が必要)	特定者間のコンセンサス (厳格な承認は任意)	組織内承認 (厳格な承認は任意)
利用モデル	ビットコイン	金融機関などによる利用が想定されるモデル	

※1 **BCN**: ブロックチェーンネットワーク ※2 **PoW** : Proof of Work / **PoS** : Proof of Stake

「富士通ホームページ金融ソリューション-ブロックチェーン技術の取り組み」から

コンソーシアム型とプライベート型 (2)

管理主体による一般的なブロックチェーンプラットフォームの分類

出所) IBM公開資料を一部加工

	パブリック型	コンソーシアム型	プライベート型
管理主体	なし	複数組織	単一組織
参加者	自由	許可制	
	不特定、悪意のある参加者を含む	参加者の身元が判明しており、信頼できる者で構成される	
コンセンサス方式 (合意形成方式)	Proof of Work(注1)型等	PBFT(注2)型等	
	ブロック確定(注3)しない 電力消費が多い	ブロック確定する 軽量、高速、低消費電力	
トランザクション 処理時間	長い(10分など)	短い(数秒など)	
ユースケース	仮想通貨等	銀行間送金、証券取引等ビジネスネットワーク 等	
実装例	Bitcoin、Ethereum 等	Ripple、Hyperledger Fabric 等	

- (注1) Proof of Work : 一般的に「単純だが手間がかかる、ただし本当にそれを行ったことの検証は簡単な、特定の作業をあえて行わせることにより、悪意のないことを確認する(不正を行う動機を低減させる)」という仕組みのこと。ビットコインにおいては、ネットワーク参加者が与えられた条件に合致する値が得られるまで計算を続け、求める値を得られた参加者がブロックの生成権限を得る、という仕組みによって、参加者間の合意を形成する方式
- (注2) PBFT (= プラクティカル・ビザンチン・フォールト・トレラント) : コアノードにブロックの生成権限を集中させ、コアノードによる合議制において、トランザクションの承認を行う方式
- (注3) ブロック確定 : ブロック生成においてフォーク(分岐)等が生じることで、生成されたブロックが後に否認される可能性がある状態となることがあるが、そのような可能性が無くなった状態。実際のビットコインの取引では、6回程度の後続ブロック生成が行われたことをもって、「取引が正当なものと認められた」(=ファイナリティが得られた)とみなしている。厳密には、どれだけブロックが連なったとしても、フォークする確率がゼロにはならないため、トランザクションが取り消されるリスクも非常に小さな確率で残る。

インセンティブ設計と暗号理論に関する他の話題

- ゲーム理論と暗号プロトコルの安全性
 - 秘密分散
 - 紛失通信
 - ビットコミットメント
 - 一般的なマルチパーティ計算
- ゲーム理論と計算量理論
 - 合理証明 (Rational Proofs)

暗号理論における攻撃者の分類

- 悪意のある攻撃者 (Malicious)
 - プロトコルの記述に従わない
 - 可能なリソースはすべて用いる。リスクも考慮しない
- 合理的な攻撃者 (Rational)
 - 攻撃検知リスクを考慮する。リソースは必要なだけ用いる
- 正直だが好奇心はもつ者 (Honest-but-curious)
 - プロトコルの記述に従うが秘密は盗み見る
- 正直者 (Honest)
 - プロトコルの記述に従う。秘密も盗み見ない

東工大における取り組み事例

- Input Output HK社との「暗号通貨・ブロックチェーン基礎技術」に関する研究 (2017年1月-) と修士課程向け授業の実施 (2018年4月-)
- 三菱電機との「電力取引」に関する研究 (2017年4月-)
- (株)日本クラウドキャピタルとの「未公開株式の管理と取引」に関する研究 (2017年4月-)
- 金融関連5社と法律専門家、技術専門家による「金融関連分野におけるブロックチェーン技術実務適用研究会」に参加 (2018年5月-)
- ブロックチェーンロック(株)と「スマートロックの管理」に関する研究 (2017年10月-)