IBM Blockchain Summit 2016　　2016.11.16

中央銀行から見たブロックチェーン技術の可能性とリスク

日本銀行 決済機構局
FinTechセンター長
岩下直行

本資料の内容や意見は発表者個人に属します。
日本銀行あるいは決済機構局の公式見解を示すものではありません。

1. Bitcoin, Blockchain and DLT

Bitcoinから始まったイノベーション

概念の発生順にみれば、

Bitcoin
→Blockchain
→DLT（Distributed Ledger Technology）

そこでまずは、Bitcoinの歴史を訪ねてみる。

2. Bitcoinの誕生前史

Satoshi Nakamoto論文 (2008年)

Bitcoin: A Peer-to-Peer Electronic Cash System

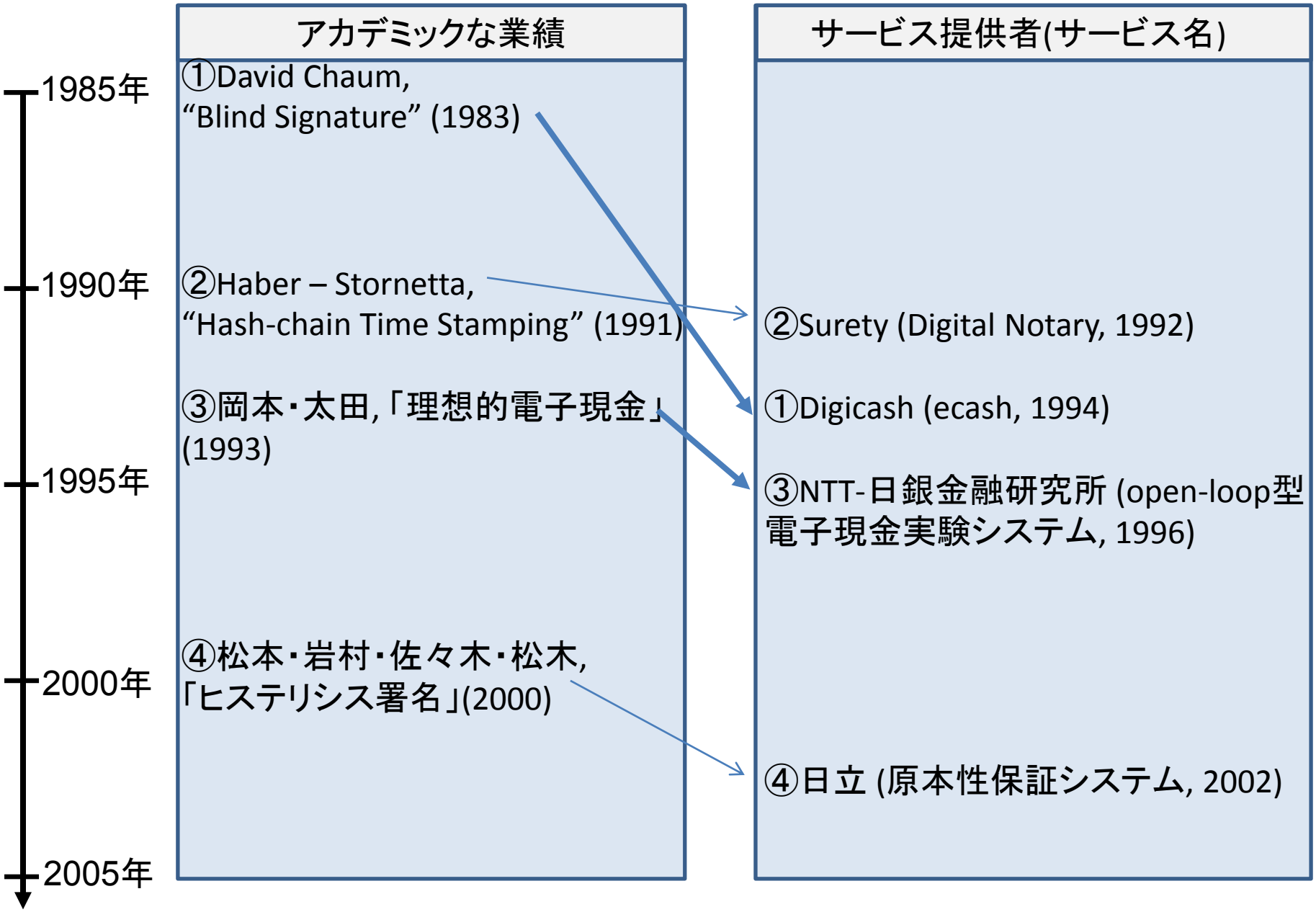
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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

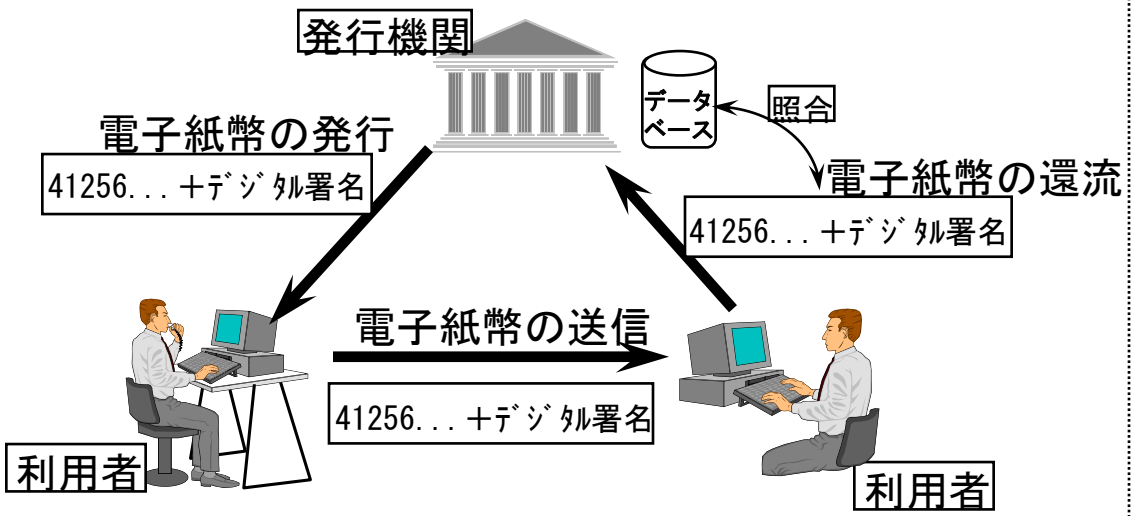
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

Bitcoinに先立って開発されていた主な技術



そもそも電子現金(Electronic Cash)とは

ユニークな番号等によって個別に特定可能なデジタル情報を一種の紙幣(＝電子紙幣)とみなし、これを送信することにより価値を移転する方式。



セキュリティの基本思想

発行機関は、還流した電子紙幣をデータベースの情報と突合チェックすることによって、その正当性を確認し、二重使用を防止する。

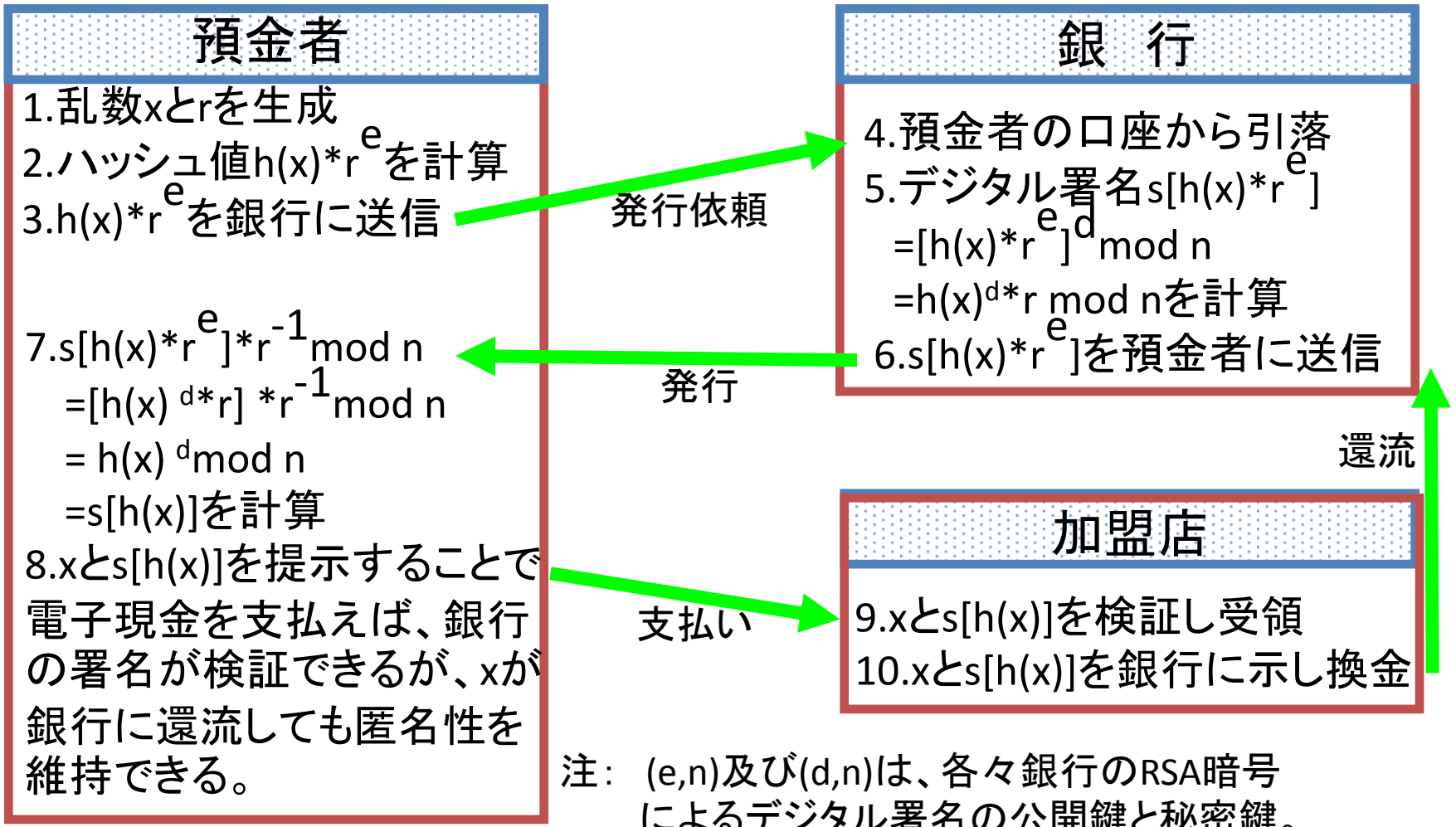
利用者は、相互に認証を行いながら電子紙幣を受け渡すことで価値を移転させる。

技術的特徴点

- ソフトウエアだけで実現することも、ICカード等のデバイスを利用することも可能。
- 送信してもデータは消えないため、発行機関がデータベースを構築し、二重使用をチェックする必要があるほか、利用者間の送受信等が複雑になり、システム構築・管理のコストが高くなりがち。
- 仮に電子紙幣の偽造が発生したとしても、発行機関に還流した時点で正当性がﾁｪｯｸされるため、偽造の事実が見逃されることはなく、ｼｽﾃﾑ全体が崩壊するリスクは小さい。
- 利用者のプライバシーを保護する観点から、偽造や二重使用が発覚した場合のみ実名の把握を可能とするような「制御された匿名性」の技術を利用することが可能。

① Digicash社のecash

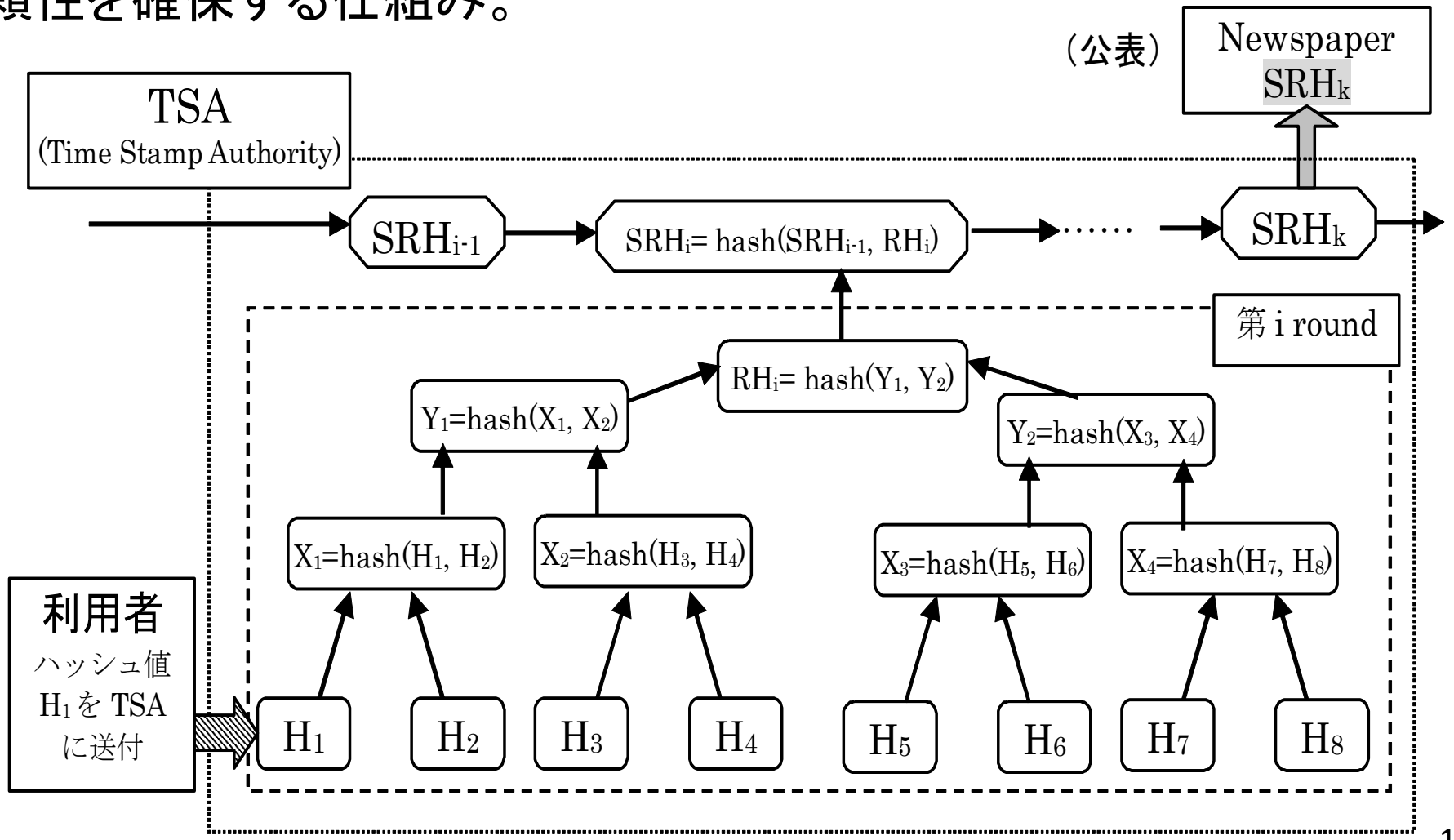
ecashは、David Chaumが発明したblind signatureと呼ばれる暗号技術により、取引の匿名性を実現したclosed-loop型電子現金。



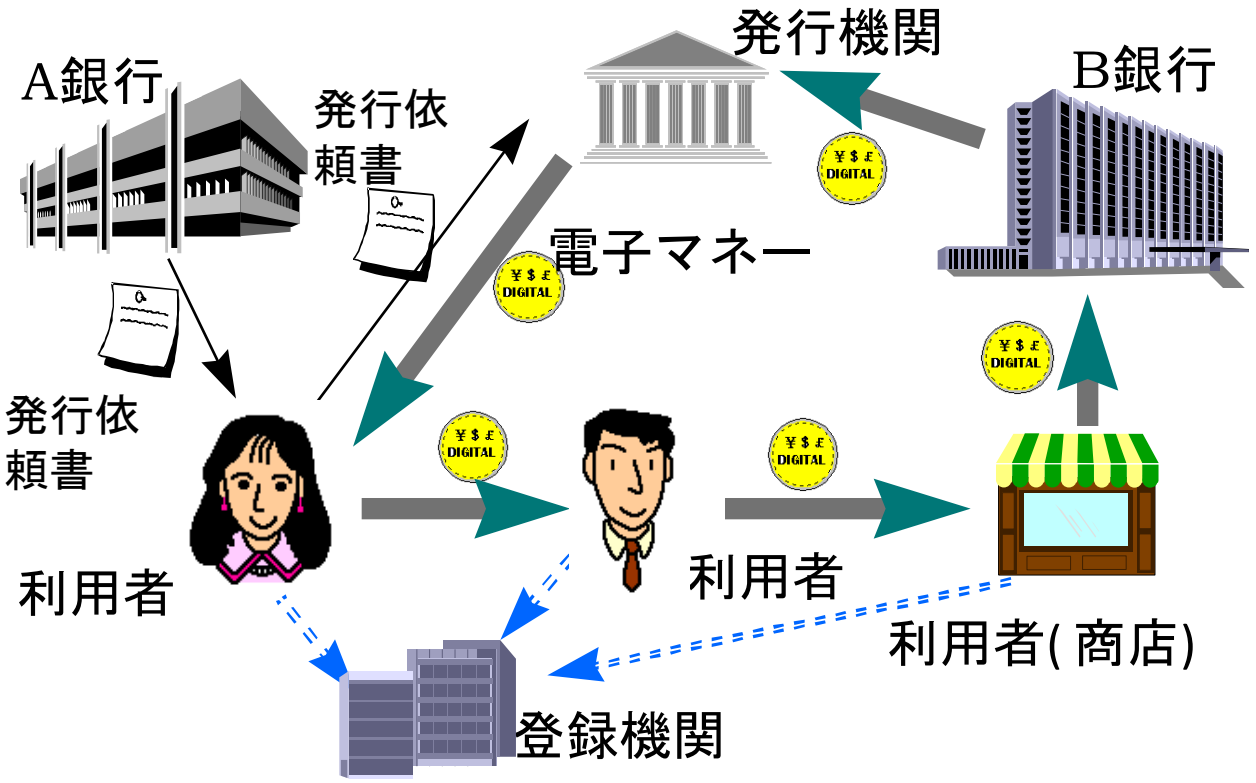
注：　(e,n)及び(d,n)は、各々銀行のRSA暗号によるデジタル署名の公開鍵と秘密鍵。
r^{-1}は、$r \cdot r^{-1} \bmod n = 1$となる正整数。

② Surety社のDigital Notary

Digital Notaryはハッシュ値を連鎖させることで電子的なタイムスタンプを実現するサービス。毎週ハッシュ値を新聞掲載することで信頼性を確保する仕組み。



③NTTと日銀金融研究所による電子現金実験システム



（利用環境）

・ コインを分割利用できる。ネットおよび商店店頭の双方で利用可能。

（セキュリティ対策の強化）

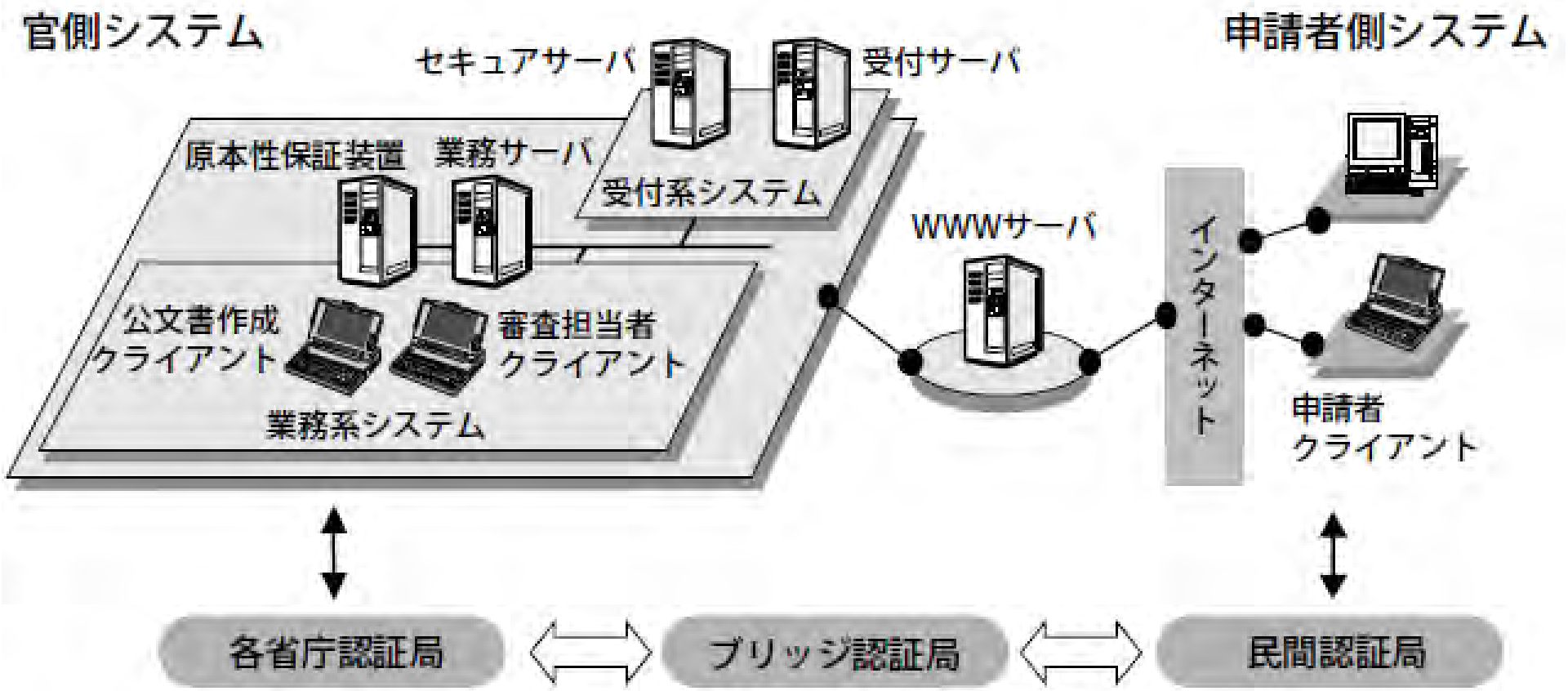
・ ICカードの耐偽造性による事前対策と、電子マネーへの属性情報の埋め込みによる事後対策の二重の対策を組み込み。

（現金のメリットの継承）

・ 利用者間での転々流通が可能（「open-loop型」）。
・ プライバシー保護の観点から、「取引の匿名性」を実現。

④日立の原本性保証システム
（経済産業省の汎用電子申請システムへの適用例）

原本性保証システムは、ヒステリシス署名を用いて電子文書の事後的な改竄を防止する仕組み。電子文書のデジタル署名を生成する際に、それ以前の署名等を署名生成記録として署名に埋め込み、すべての署名が相互に関連づけられることにより、署名生成者自身でも偽造が困難となる。



（出典）ニューメディア開発協会、『研究成果レポート』第7号、2002年7月

Bitcoinの誕生前史を読み解くと

- Bitcoinが考案される前から、Bitcoinの特徴である
  ① 乱数とデジタル署名を用いた電子現金、
  ② 分割可能性、open-loop性、匿名性の付与、
  ③ ハッシュ関数や署名のchainによる改竄防止、
  については、様々な技術が考案され、実装されていたことが分かる。
- しかし、システムリソースの不足やコスト、利便性の問題から、当時はそれらの技術が広く普及することはなかった。
- ecashは既存の通貨建てで発行された「電子マネー」的なものであったが、Chaumian digital cashと呼ばれる模倣プロジェクトの中には、独自の通貨単位を導入した、「仮想通貨」的なものもあった。それらは全て、特に注目されることもなく消滅している。

3. Bitcoinの誕生

2009年1月9日のメール

Bitcoin v0.1 released

Satoshi Nakamoto | Fri, 09 Jan 2009 17:05:49 -0800

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now. Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes

If you can keep a node running that accepts incoming connections, you'll really be helping the network a lot. Port 8333 on your firewall needs to be open to receive incoming connections.

Bitcoinの価格と利用者数の推移

Bitcoinの発掘の仕組み

Economist

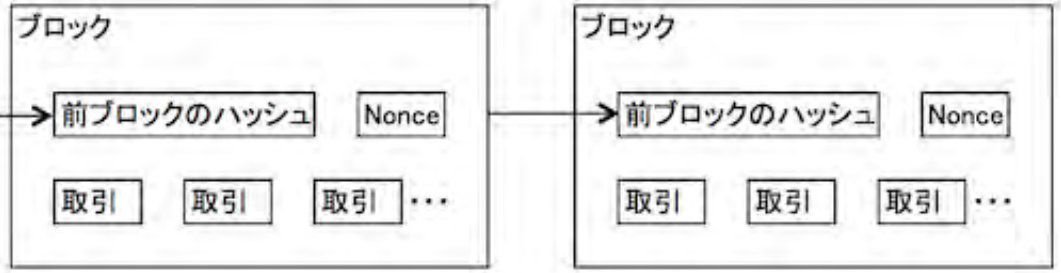
Bitcoin

The magic of mining

Minting the digital currency has become a big, ru

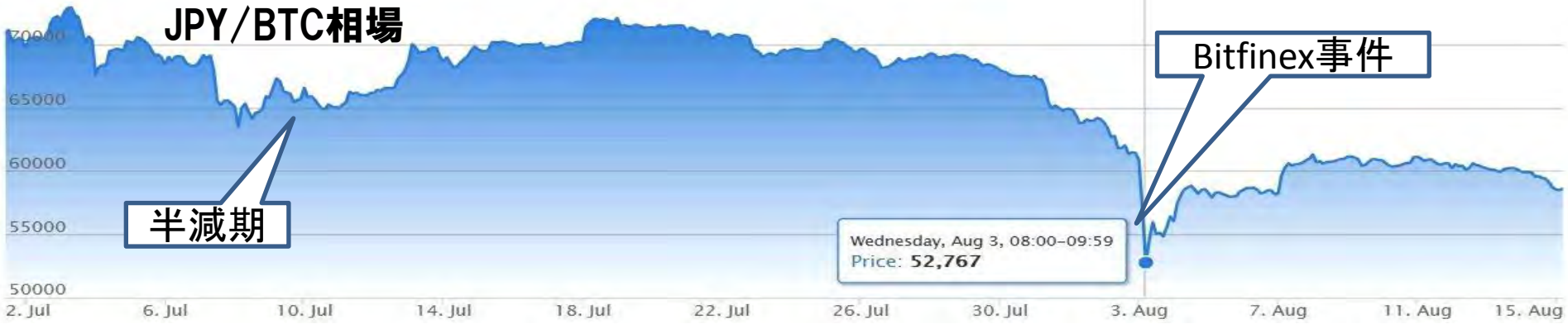
Jan 10th 2015 | BODEN, SWEDEN | From the print edition

Timekeeper



ビットコインは発行主体を持たず、インターネット上のP2Pネットワークで情報が共有される。誰でも利用者となることができ、ソースコードや取引履歴の検証を可能とすることで、信頼を確保。計算能力を提供してシステム全体の維持管理に貢献すること(＝発掘)に対し、一定の報酬が与えられる。この報酬を求めて、専門業者が膨大な計算能力を投入して「発掘」を進めている。

Bitcoinの半減期前後の相場変動



何故Bitcoinが「成功」したのか

① peer-to-peerによる分散コンピューティングの採用

— CPU、ストレージ、通信のコスト低下によって、一般ユーザーが保有するインターネット上のリソースだけで稼働可能になった。

② Proof of Work(PoW)を基準とした報酬付与によるインセンティブ付けで、ビザンチン障害耐性を獲得

— ①の結果生じる分散システム内の不整合を制御する手法を導入。これも安価なCPUリソースが普及したために可能となったもの。

③ 独自通貨単位(BTC)の採用による投資機会の提供

— 決済手段として用いるのであれば法定通貨建ての方が便利だが、交換価値を維持する費用が掛かる。システムを支えるマイニングの報酬の分だけ、仮想通貨を追加発行して賄うことで、外部からの費用投入なしにシステムを維持することが可能になった。

⇒ システム維持費用の「自給自足」が可能な仕組みを構築できたことが、現在の「成功」の一因と考えられる。

その「成功」は今後も続くだろうか

「デジタル通貨は特定の個人や機関の負債ではなく、当局による裏付けもない。さらに、本源的価値はゼロであり、結果的に、その価値は他の財・サービスないしソブリン通貨に後日交換されるという信頼にのみ由来する。したがって、デジタル通貨の保有者のほうがソブリン通貨の所有者よりも、価格変動・流動性リスクに起因するコストや損失に直面する可能性が高い。」

（BIS/CPMI　デジタル通貨報告書<2015>より）

4. BlockchainとDLT

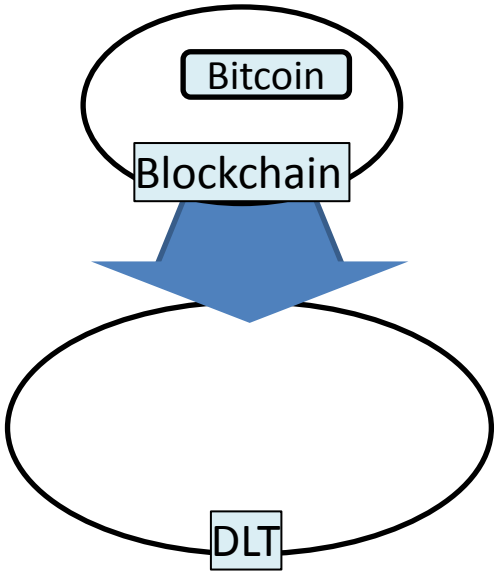
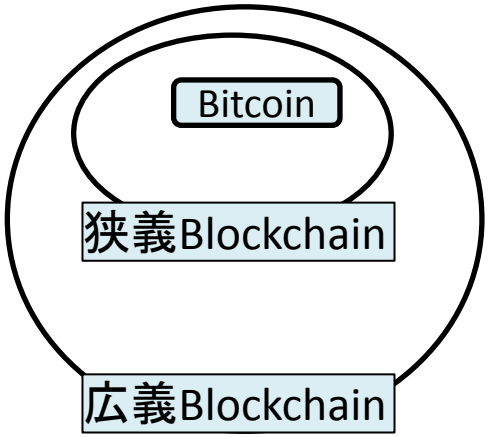
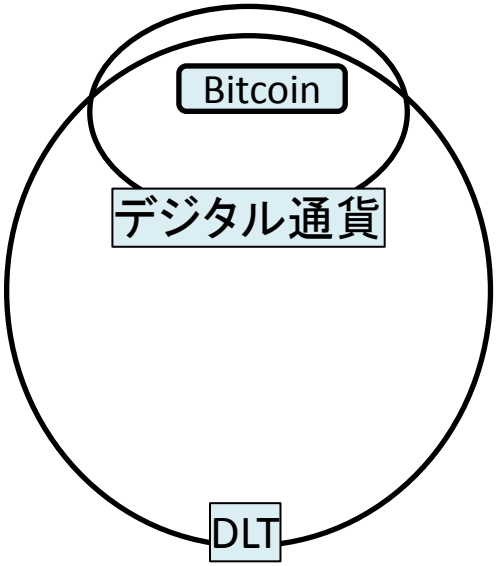
BlockchainとDLTの定義を巡って

Bitcoinが注目を集め、類似の技法で新たな仮想通貨が開発されるようになると、技術面に着目したそれらの総称として「Blockchain」という言葉が使われるようになった。また、その技術を仮想通貨以外にも適用することが提案されるようになると、Bitcoinそのものと深くリンクしたBlockchainという用語から、より汎用的な印象のあるDLT(Distributed Ledger Technology)という用語が使われるようになった。

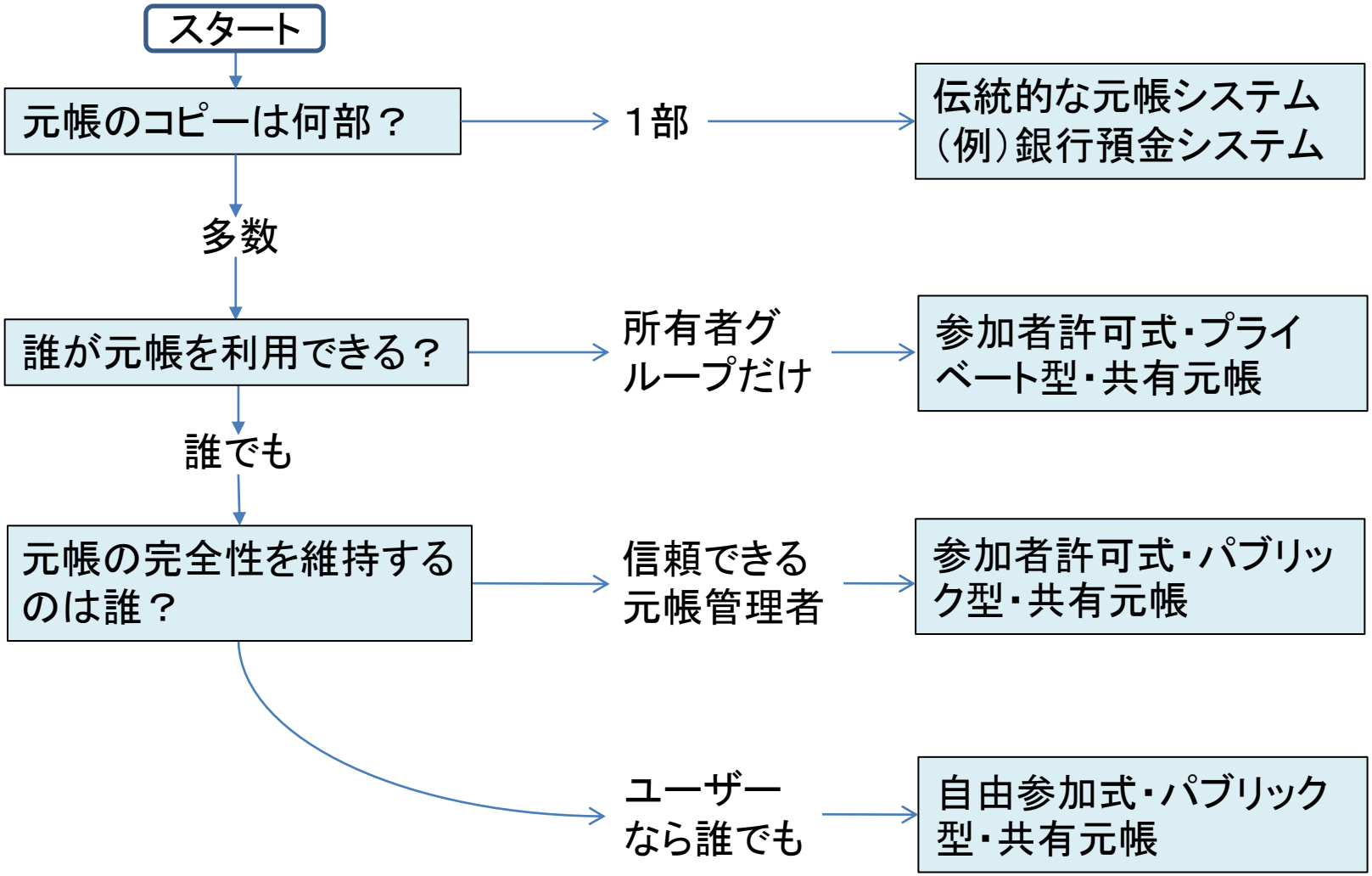
BlockchainとDLTについて、広く合意された定義があるわけではないが、日本ブロックチェーン協会（JBA）は、以下のような狭義・広義のBlockchainの定義を提唱している。

- ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装を「ブロックチェーン」と呼ぶ。
- 電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を「広義のブロックチェーン」と呼ぶ。

BlockchainとDLTを巡る様々な理解

英国政府レポート”Distributed Ledger Technology: beyond block chain” <2016>	日本ブロックチェーン協会（JBA）<2016>	BIS/CPMI デジタル通貨報告書<2015>
		
適用業務範囲がデジタル通貨からより一般的なものに拡大するところに注目して、DLTを広く捉えている。	ビザンチン耐性を持つものが狭義Blockchain。ビザンチン耐性を持たないが似たような構成をしていれば広義Blockchain。	DLTは「分散型の決済メカニズム履行を可能とする中心的イノベーションを描写する一般的な用語」として使われている。

英国政府「DLT: beyond block chain」の分類法



出典：“Distributed Ledger Technology: beyond block chain”,
A report by the UK Government Chief Scientific Adviser, 2016

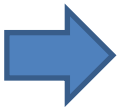
プライベートなブロックチェーンとパブリックなブロックチェーン

	プライベート型	コンソーシアム型	パブリック型
管理者	単独の機関	複数のパートナー	存在せず
ノード参加者	管理者による許可制	管理者による許可制	制限なし
合意形成	厳格ではないことが可能	厳格ではないことが可能	厳格であることが必要（PoW、PoS等）
取引速度	高速	高速	低速

現在、金融業界が実証実験のターゲットとしているブロックチェーン

Bitcoin、Ethereum等の仮想通貨の基盤に利用されている

とはいえ、現在の金融業界の「Bitcoinは危ないものだが、private/consortium型のブロックチェーンなら大丈夫」という考え方は二重の意味で問題がある。



①public型の可能性を放棄
②consortium型のブロックチェーンにおける合意形成問題

5. 主なユースケース

Blockchainの様々なユースケース

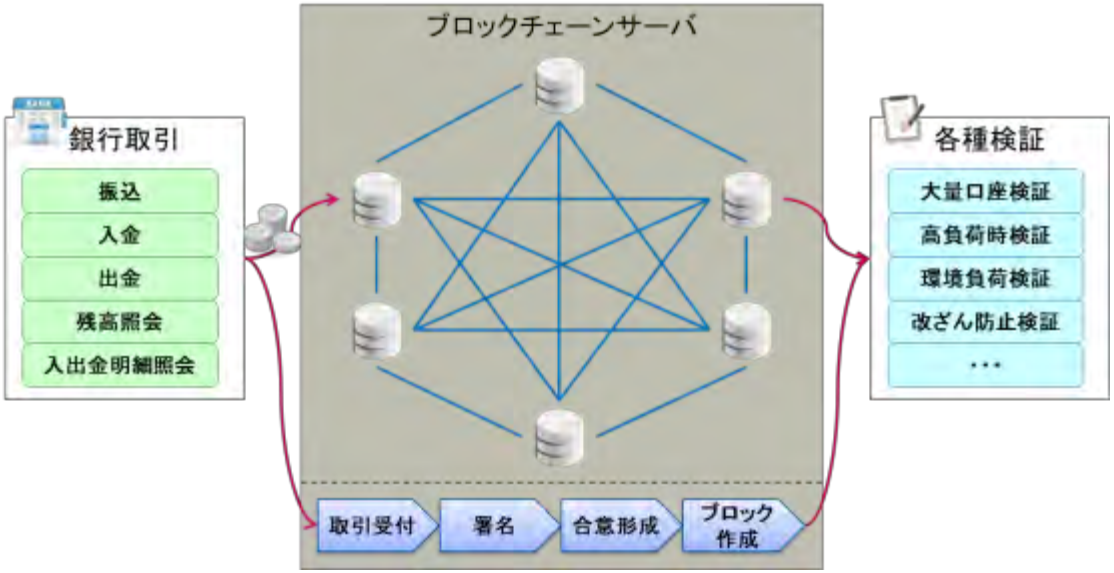
技術の使い方＼分野	金融	産業	行政	CivicTech
1. Bitcoinなどを仮想通貨としてそのまま使う	国際送金	貿易金融	社会保障支払の改善、国際援助の透明化	
2. Bitcoinなどの元帳機能のみを利用する	証券ポストトレード	サプライチェーン		学位認定、臨床試験の研究記録
3. オリジナルの分散元帳を構築する	銀行勘定系システムの構築、証券ポストトレード、小切手の電子化、KYC/AML	サプライチェーン	知財管理、ヘルスケア、消費税徴税事務の改善	土地登記、法人登記

住信SBIネット銀行の実証実験概要

■ 実験結果概要

銀行勘定系を想定した実証実験。

検証項目	内容
大量口座検証	当社口座数を想定した250万口座を作成
高負荷時検証	夜間バッチを想定した9万件の処理
環境負荷検証	意図的なノードダウンによる負荷検証
改竄防止検証	ハッキングプログラムを用いた検証



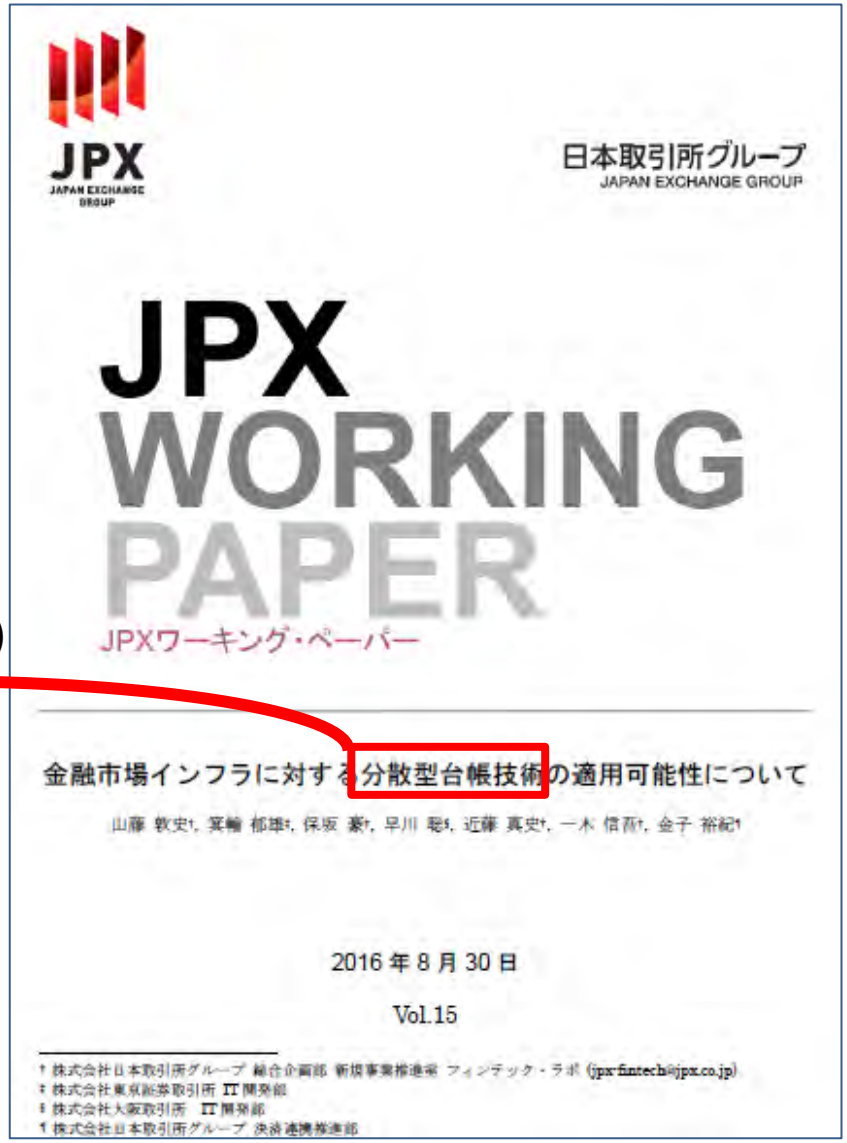
■ DR/BCP分野において効果。

■ 一方、周辺アプリケーション領域に課題。

（出典）2016.6.10　日本銀行金融高度化センターワークショップ提出資料

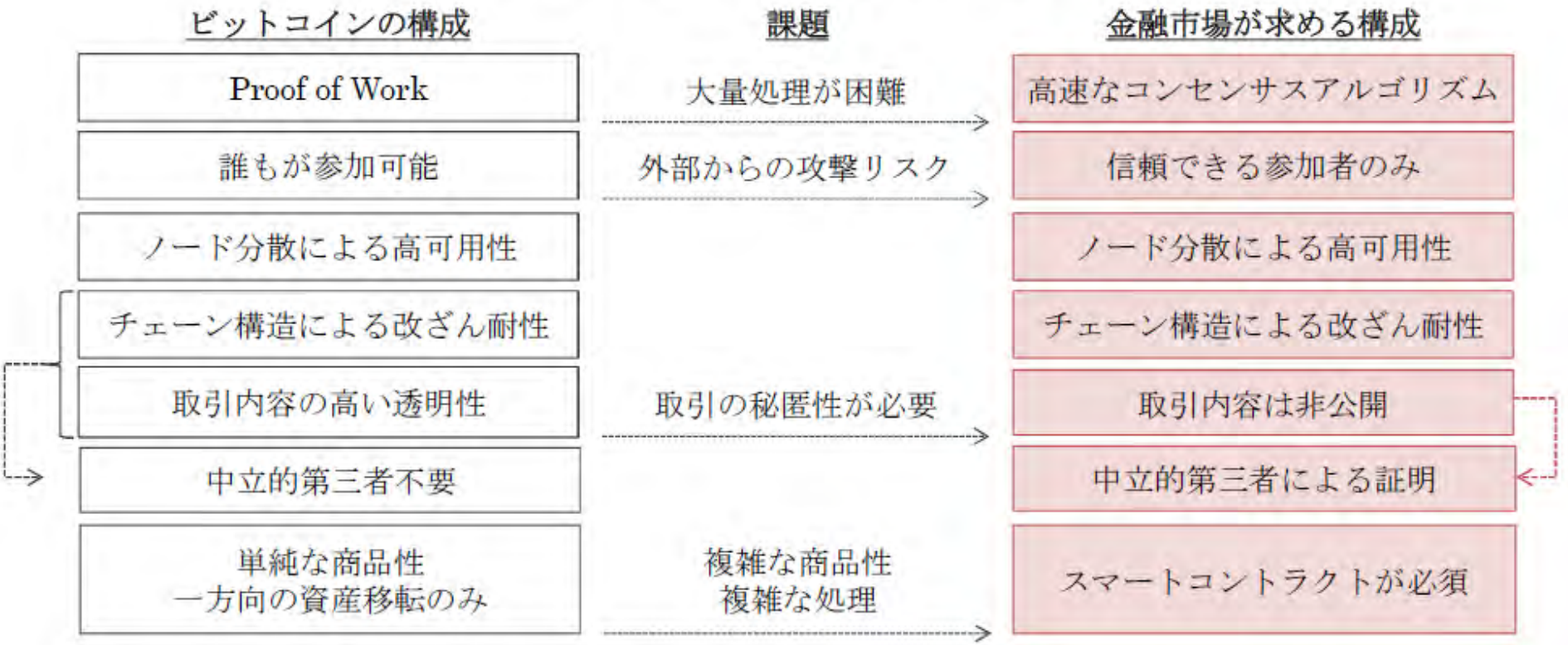
日本取引所の分散型台帳WPから

Blockchainではなく
分散型台帳技術(DLT)
と表記している



パブリック型ではなくコンソーシアム型を選択

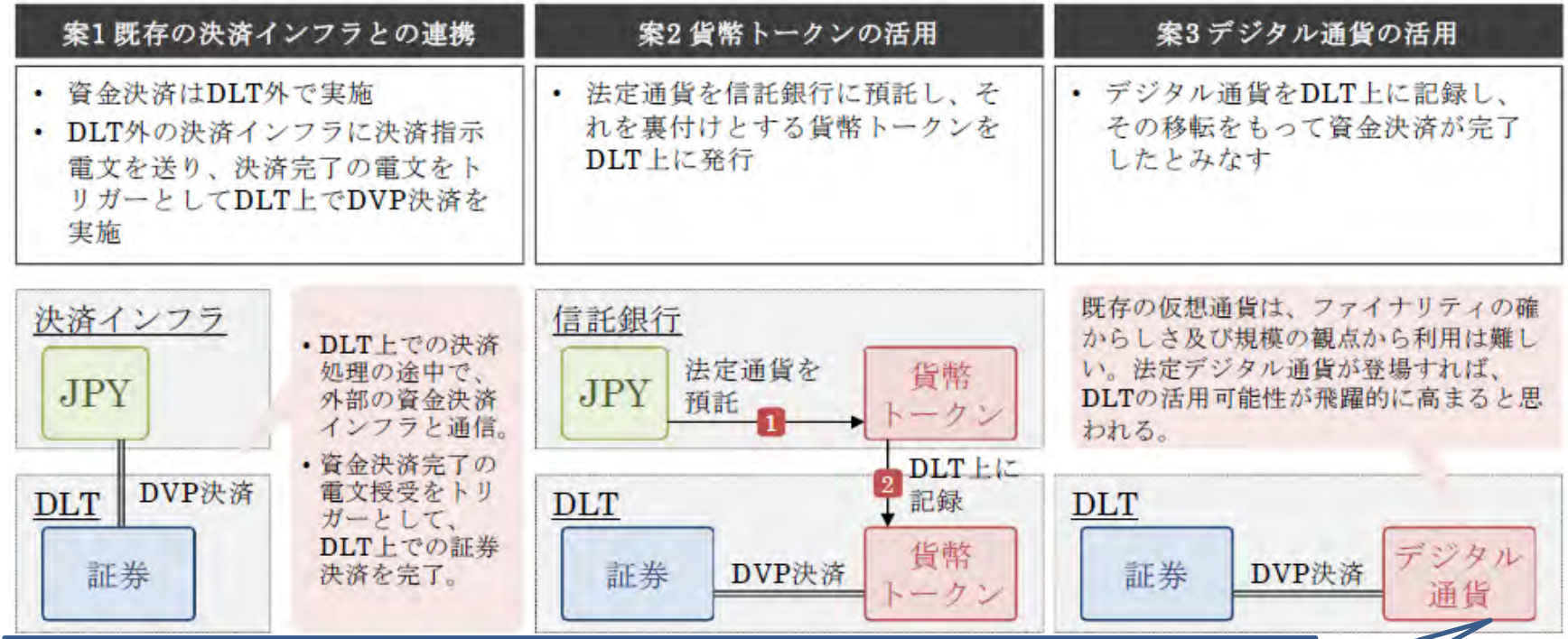
図 3 金融市場が求める DLT の構成



出典：日本取引所、JPXワーキング・ペーパー『金融市場インフラに対する分散型台帳技術の適用可能性について』、2016年8月

証券決済DVP実現の対応案

図 9 DLT 上で資金決済を行う対応案

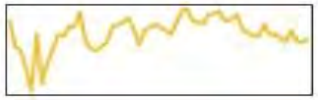


安定したファイナリティと十分な発行量を保証する法定デジタル通貨を中央銀行が発行し、DLT上で取り扱う事を可能とすれば、これらの問題を抜本的に解決する可能性がある。

出典：日本取引所、JPXワーキング・ペーパー『金融市場インフラに対する分散型台帳技術の適用可能性について』、2016年8月

6. Blockchain 2.0とthe DAO事件

Bitcoin以外の仮想通貨も注目される

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$11,233,882,844	$703.71	15,963,864 BTC	$60,647,900	-0.64%	
2	Ethereum	$926,534,335	$10.81	85,741,788 ETH	$5,999,140	-0.57%	
3	Ripple	$289,512,650	$0.008121	35,649,569,539 XRP *	$2,343,430	-0.81%	
4	Litecoin	$186,289,753	$3.85	48,336,854 LTC	$2,120,750	-0.57%	
5	Ethereum Classic	$79,784,944	$0.931574	85,645,310 ETC	$1,007,390	-5.06%	
6	Monero	$76,749,170	$5.77	13,291,373 XMR	$3,762,970	16.44%	
7	Dash	$68,789,557	$10.02	6,868,516 DASH	$1,592,100	7.07%	
8	Augur	$52,789,550	$4.80	11,000,000 REP *	$519,258	-2.90%	

Blockchain 2.0

近年、「ブロックチェーン2.0」と呼ばれる新たなサービスが勃興している。

- bitcoinのような仮想通貨としてのブロックチェーンを1.0とした時に、「契約」の機能を果たすものを2.0と位置付ける呼称。

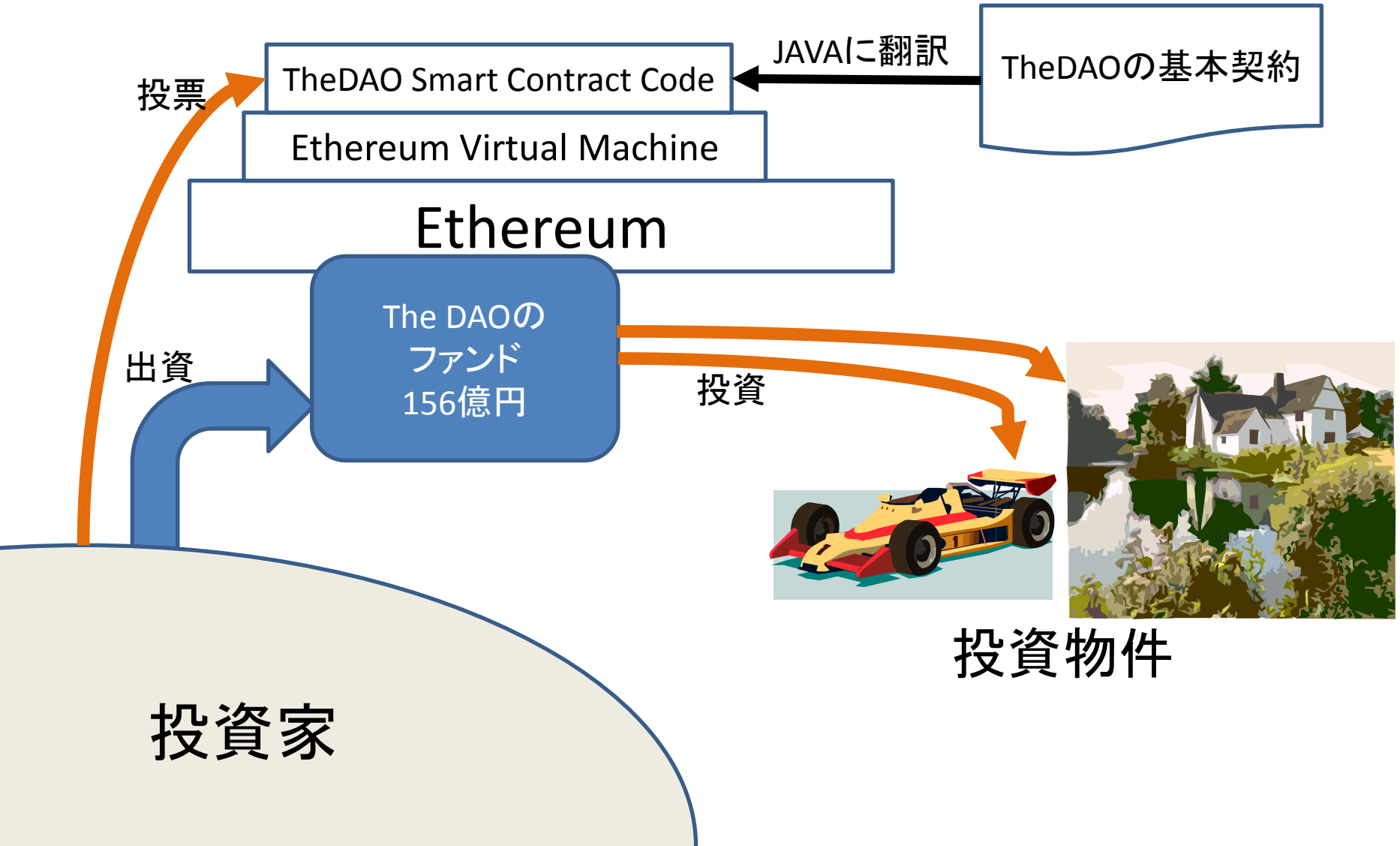
スマートコントラクト	契約書をブロックチェーンに載せ、契約を執行させる機能を持たせたもの。
スマートプロパティ	資産・契約書をブロックチェーンに載せたもので、契約を執行させる機能はない。
DAO (Decentralized Autonomous Organization)	分散型自動化組織。スマートコントラクトをさらにまとめて、自動執行するようにしたもの。
DAC (Decentralized Autonomous Corporation)	DAOの会社版。出資をして株主のために配当を支払うこと等を自動的にブロックチェーン上で行う。

その一類型として、”DAO”がある（一般名詞としてのDAO）。

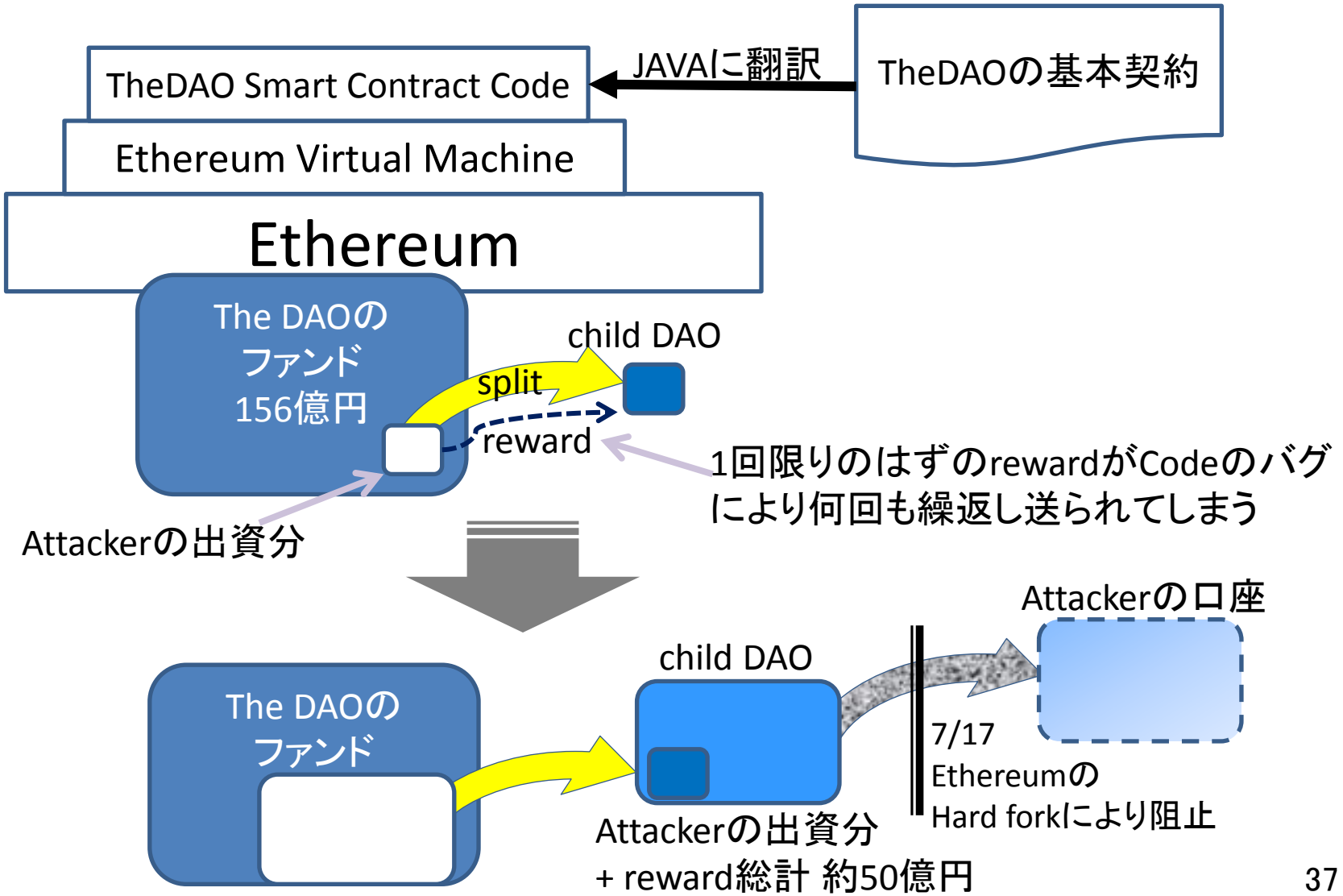
The DAOとは

- The DAO（固有名詞）は、ドイツのIoTベンチャー企業であるSlock.it社が、DAO（一般名詞）のコンセプトを実証するために2016年4月30日にEthereum上に組成した事業ファンド。組織を運営する役員を置かず、Ethereum上で出資したメンバーが投票によってガバナンスする仕組み。
- Slock.it社は、IoTを活用したシェアリング・エコノミーの展開を目指しており、スマートロック（IoT接続された電子的な錠）が装備された車、家などを、Ethereum決済によって利用可能とする事業を展開。その一部は、AirB&Bでも活用されている。
- The DAO は2016年5月に出資を募り、5月28日までに11000人の投資家から約156億円を調達した。

The DAOの基本構造



The DAO事件：攻撃の手口



The DAO事件の教訓

- ブロックチェーンによる「株式会社の再発明」の試みは、ひとまず頓挫。
- 実験の最初から、156億円もの資金を集めたのはリスクがあった。
- 既成の法制度に頼らない、de-centralized な合意形成の仕組みが必要／有用であるとしても、その制度設計・システム設計には、更なる検討が必要。
- 問題発生と対応の過程で、スマートコントラクトやブロックチェーンによる価値の保有そのものの問題が明らかに。
- とはいえ、IoTと連動したFinTechは有望と考えられており、更なるチャレンジが予想されている。

7. Blockchainと中央銀行

各国中央銀行がデジタル通貨に関心

銀行券、銀行預金、デジタル通貨

	基盤となる技術	AML	プライバシー保護	受渡における第三者の関与
銀行券	偽造防止技術	対応困難	対応不要	不要
銀行預金	個人認証＋勘定系	対応可能	対応困難	必要
デジタル通貨	ブロックチェーン技術	対応可能	対応可能	不要

「FinTech センター」の設立に寄せて

近年、情報通信関連など新しいテクノロジーを金融面に応用し新しい金融サービスに繋げていく、いわゆる「FinTech」への注目が、一段と高まっています。

金融がもともと「情報」と密接な関わりを持っていることを踏まえれば、情報技術の進歩とその応用は、金融サービスのフロンティアを大きく拡げ得るものといえます。また、このようなイノベーションは、金融サービスの効率化などにとどまらず、新たな経済活動を促すことなどを通じて、経済全体に幅広いメリットをもたらす潜在力を持つものと考えられます。

新しいものを産み出していく上では、さまざまな知見や創造の「相互作用」が、きわめて重要です。FinTech を発展させ、経済全般に最大限寄与するものとしていく上では、伝統的な金融業にとどまらない幅広い企業や、さらには学界などとの間での、建設的かつインタラクティブなコミュニケーションが求められます。このような問題意識を踏まえ、日本銀行は本日、決済機構局内に「FinTech センター」を設立しました。

日本銀行は、FinTech の動きが金融サービスの向上や持続的成長に資するものとなるよう、一段と取り組みを強化していく考えです。日本銀行としては、FinTech センターが外に開かれた拠点として、金融実務と先端技術、調査研究、経済社会のニーズなどを結び付ける「触媒」としての役割を積極的に果たすよう、努めていきたいと思います。また、金融イノベーションや FinTech に関わる幅広い方々には、是非ともこのセンターの活動にご協力頂くとともに、センターを最大限活用して頂くことを願っています。

2016 年 4 月 1 日

日本銀行総裁

黒田東彦

Message from Governor Kuroda on the occasion of the establishment of the FinTech Center

April 1, 2016

FinTech is gaining considerable attention in recent years as it applies new technologies -- including those of information and communications -- to innovative financial services.

Considering that finance is closely associated with information, developments in information technology and its application can broaden the frontiers of financial services. In addition, such developments have the potential to improve the efficiency of financial services, and further bring a wide range of benefits to the economy as a whole through promoting new economic activities.

In order to bring new products and services to life, the interaction of knowledge and creativity is extremely important. To foster FinTech and maximize its contribution to the economy as a whole, constructive and interactive communication among a wide range of players, including those affiliated with traditional finance industry and academic community, is required. Bearing this in mind, the Bank today established the FinTech Center within its Payment and Settlement Systems Department.

The Bank aims to reinforce its efforts in which the developments of FinTech will contribute to enhancing financial services and achieving sustainable growth of Japan's economy. The Bank will also endeavor to play an active role as a catalyst for promoting interaction among financial practices and innovative technologies, research and study, and the needs of the economic society. The Center will serve as a hub for such interaction. I hope that a wide range of parties involved in financial innovations and FinTech will give support to and take full advantage of the Center's activities.

Haruhiko Kuroda
Governor of the Bank of Japan

日本銀行のFinTech検討体制