A New Peer-to-Peer Double Entry Settlement Network based on Encrypted Asset (1)

Ken ITO, Tomoki YATSUZUKA, Kyôske TOMONARI
Interfaculty Initiative in Information Studies
The University of Tokyo[1]

暗号資産技術に基づく 新しい P2P 複式簿記と決済ネットワーク（1）

伊東　乾、八塚友紀、友成恭介
東京大学大学院情報学館

Abstract

The Blockchain technology based on encrypted assets, such as Bitcoin, have expanded rapidly. In this paper, we systematically redesign the encrypted asset and propose a theoretical framework using double entry bookkeeping methodology. The Blockchain technology can be viewed as an incomplete application of ledger system, that is single entry bookkeeping. The ledger is shared by all Bitcoin users in the peer-to-peer network and it enables the system to settle payments. In order to ensure an appropriate accounting practice in the system, the ledger and other accounting information needs to be recorded and organized by using double entry bookkeeping to facilitate a true audit process.

The Blockchain technology was proposed as a peer-to-peer network system without center of trust. However, Bitcoin users have pursued their own profit and changed Bitcoin's quality, from a currency to a kind of speculative investment. In order to overcome this difficulty, Facebook and its cooperative companies proposed a new reserve currency, "Libra" ; a sort of stable coin or sovereign coin, which is convertible to legal currencies. However, Libra's management entity, the Libra Association, is composed of commercial enterprises and it is impossible to prevent the association from pursuing profit-motivated activities. Therefore, the association cannot deliver a fair and impartial monetary policy to maintain a stable Libra system (IWAI's Monetary Instability Principle).

We propose a peer-to-peer network composed only of central banks, which impartially maintain the stability of the financial system without profit motivations. For such a network, we are developing a new Blockchain system, "NAKASO-IWAI's Post Blockchain systems". In this article, we will mostly show the fundamentals' outline, and for the details we will publish following articles in turn.

[1] 7-3-1 Hongo, Bunkyo-ku 113-0033 Tokyo JAPAN, mail to: itosec@iii.u-tokyo.ac.jp

要旨

ブロックチェーン技術は、ビットコインに代表される暗号資産の基礎を成し、急速に普及している。この論文では、複式簿記の手法を用いた理論的なフレームワークを体系的に再構築する。ブロックチェーン技術は単式簿記による台帳の不完全な形態として解釈することが可能である。その台帳はビットコインの peer-to-peer ネットワークですべての利用者によって共有され、そのシステムの決済を可能としている。システムにおける適切な会計の実施を保証するためには、台帳や他の会計に関連する情報は複式仕訳によって構成されている必要があり、それが正しく会計監査を実施することに繋がる。

ブロックチェーン技術は信用中心が不在の peer-to-peer ネットワークシステムとして提案された。しかし、ビットコインの利用者たちは自分たちの利益のみを追求してビットコインの本性を貨幣から投機商品へと変質させてしまった。この困難を克服するために、Facebook とその協力企業は新たな準備通貨として“Libra“を提案した; それは法定通貨と兌換可な stable coin ないし sovereign coin である。ところで、Libra の管理主体 Libra Association は大企業で構成されており、利潤動機に基づく活動から回避することは不可能である。 したがって、この組織は公正かつ公平な金融政策によって Libra システムを安定させることができない（岩井の通貨不定性の原理）。

私たちは、安定性が公平に維持された利潤動機に基づかない金融システムとして、中央銀行のみから構成された peer-to-peer ネットワークを提案する。そのようなネットワークを、私たちは新たなブロックチェーン・システムとして研究しており、中曾-岩井のポスト・ブロックチェーンシステムと呼んでいる。この論文では、私たちは主に基盤となるアウトラインのみを示し、その詳細については引き続く論文で展開していく。

Key words: ブロックチェーン、暗号資産、Libra、基軸通貨、中央銀行、非利潤動機、複式簿記

1. グローバル・カレンシーと本位通貨、その限界

グローバル金融の安定化と自由貿易の促進を目指し、Davit Ricard らがイギリスに金本位制を導入したのは、ナポレオン戦争終結直後の 1816/17 年であった[1]。安定であると同時に停滞的な本質を持つ金本位制は 19 世紀の国際経済を支えるとともに、1929 年の世界大恐慌を以って実質的に廃止された[2]。

John Maynard KEYNES は金本位制を廃止し、管理通貨制度への移行を主張した。だが、第二次世界大戦後のグローバル経済を再建していくに当たって採用されたのは、米ドルと金の兌換システムを含んだ、IMF 体制であった[3]。1971 年、IMF 体制は最終的にはニクソン・ショックを契機として崩壊し、管理通貨システムへ置き換えられた[4]。これによりグローバル経済は長足の進歩を見せることになった。

2008 年の世界金融危機のダメージは、当時、日本銀行の担当責任者であった中曾宏や6主要中央銀行の代表者らの努力によってドル不足解消のために作られたドル・スワップ・ネットワークを活用することによって軽減された[5]。その直後に、Satoshi NAKAMOTO は、ビットコインに用いられる peer-to-peer ネットワークであるブロックチェーン技術を提唱した。これはグローバル社会にはじめて現れた信用中心を欠く実用的な決済手段であった[6]。

しかし、日本の経済学者岩井克人はビットコインのような暗号通貨は投機商品になってしまったため、貨幣として流通する可能性がなくなってしまった事実を指摘した（岩井の通貨不安定性の原理（仮想））[7]。2019 年の 6 月、Facebook が中心となってブロックチェーン技術のフレームワークに基礎に置く stable coin Libra が発表された[8][9]。Libra は米ドルやユーロなどといった法定通貨などから構成される準備基金を後ろ盾にしており、初めてのグローバルかつ安定な貨幣となる可能性を秘めている。Libra は基軸通貨である米ドルにとって脅威となりうる。そのため、Libra は J. M. Keynes によって厳しく批判された金本位制に類似したシステムとして sovereign currency がもつ停滞性のリスクを宿している。

私たちはこれら二つの限界を克服するための新たなフレームワークを提案したい。暗号資産の歴史的背景を概観し、21 世紀の実用的な暗号資産として中曾-岩井ポスト・ブロックチェーンの基本的な構想を紹介する。

2. 公開鍵暗号、電子通貨、放射状ネットワーク

ワンチップ・コンピュータ、すなわち、LSI（Large Scale Integrated circuit）は 1970 年代初期に登場した[10]。情報理論の進展と相まって、LSI は変動相場制導入後のグローバル経済や為替取引に革新をもたらした[4]。これらの技術的発展のなかでも RSA 暗号をはじめとする公開鍵暗号の発展や実装は、それらの革新において、本質的役割を果たした[11]。コンピュータの性能の急速な向上なしでは公開鍵暗号は決して実用化されることはなかっただろう。公開鍵暗号はクレジットカードやプリペイドカードを広く普及させ、1980 年代以降、電子通貨を先進諸国に定着させることに成功した[12][13]。

これらの電子通貨システムは必ず信用中心をもつ。クレジットカードの場合では、最終的な決済は、利用者の銀行口座とクレジットカード会社との間でおこなわれる。同様に、プリペイドカードの場合も、採取的な決済はプリペイドカード会社のサーバーでおこなわれる。その様子は Fig. 1 の概念図にまとめられている。左側の図において、矢印の向きは決済の方向を示している。

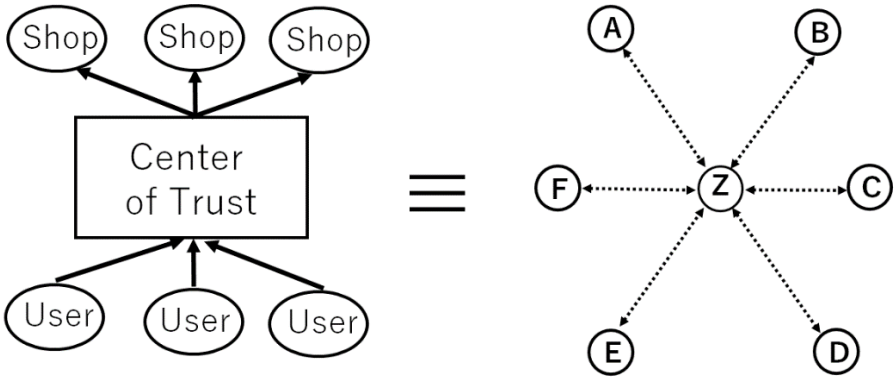

Fig. 1.　公開鍵暗号に基づく電子通貨の放射状ネットワーク構造.

クレジットカード会社にとっては、財やサービスを購入する消費者やそれらを売る小売店はいずれも顧客である。Fig. 1 の右図においては、Z を信用中心として表記している [2]。ここでは、クレジットカードの利用者が3人おり、そのクレジットカード会社と契約している小売店が3店舗あるとしよう(Fig. 1 の左図を参照)。そのとき、私たちは、Z をネットワークの中心として6つの顧客を結んだ放射状のネットワークを得る(Fig. 1 の右図を参照)。ここで、右図に示される点線は顧客間の決済の可能性を表している。Z はこのネットワークのすべての顧客と点線で結ばれており、一方、顧客はお互いに直接的には結ばれていないが、顧客間における決済を唯一おこなえるノードである Z を経由して間接的に結ばれている。したがって、私たちは Z を特権化ノードと見なすことができる。

3. 2008 年の世界金融危機とドル・スワップ・ネットワーク

2008 年 9 月 15 日のリーマンブラザーズの倒産に起因して生じた世界金融危機を鎮めるためには、各国に安定かつ迅速に米ドルを供給することが不可欠であった。日本銀行の中曾宏を含む 6 主要中央銀行の代表者たちは、米ドルの不足を軽減するために FRB とその他の中央銀行を結ぶ米ドルのスワップ・ネットワークを構築した(Fig. 2)[5]。このスワップ・ネットワークを活用することで、それらの中央銀行はこの金融危機のダメージを最小限に留めるべく、金融システムが安定性を取り戻すよう努力した[5][7]。

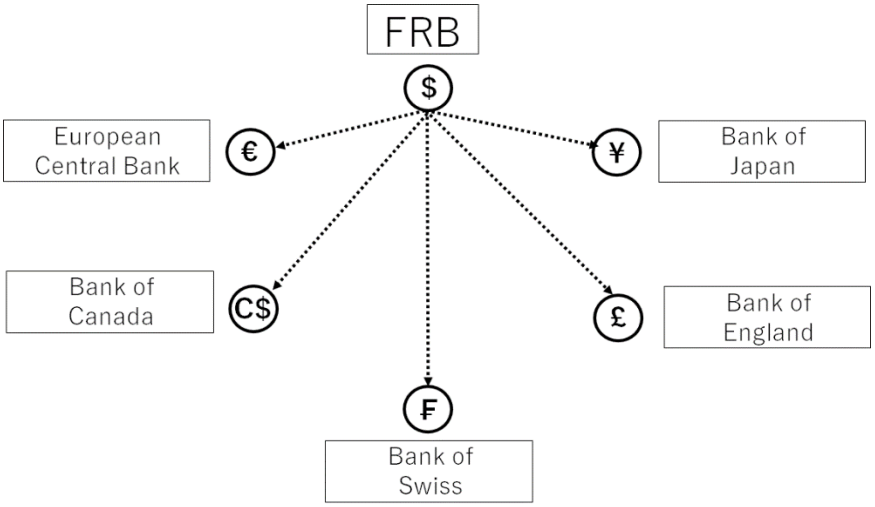

Fig. 2. 世界金融危機への対策として主要 6 中央銀行が構成したドル・スワップ・ネットワーク

どんな中央銀行も、FRB から離れては、米ドルの深刻な不足が起こっても米ドルを発行することはできない。他方、FRB は米ドルを必要なだけ発行できるが、米ドルの不足によって危機に瀕している他国の中央銀行に米ドルを供給することはできない。そのため、米ドルを必要とする他国

[2] ドイツ語の単語の“Zentrum”の頭文字をとっている。

の中央銀行に米ドルを供給することを可能とするためにそれらの中央銀行は米ドルのスワップ・ネットワークを構築したのである。このネットワークを活用することで、各国中央銀行は米ドルを必要としている市場に融資することができた。そのため、首尾よく公共性に基づいてこの危機を克服し、公正な金融秩序を回復することができた[5][7]。

FRB は米ドルの唯一の供給源であることから、Fig. 2 にある概念図は FRB を中心とした放射状ネットワークになっている。Fig. 2 の点線は、これらのルートを通じて米ドルが供給されている事実を表すのではなく、供給が可能であることを示しており、このネットワークにおいてはどのノードも FRB を介してお互いに結ばれている。我々はこのネットワークを“中曾の放射状中央銀行ネットワーク”と呼ぶことにする。

2008 年の世界金融危機が解決されたのち、中曾宏とその他 6 主要中央銀行の担当者たちは、この米ドルのスワップ・ネットワークを自国の貨幣を他国の中央銀行に供給できるように拡張した(Fig. 3)[5][7]。私たちはそれらの放射状ネットワークを Fig. 4 に示すように単一のネットワークとして表示しよう。Fig. 4 は 6 つの中央銀行間においてそれぞれことなる通貨の交換可能性を示している。二重点線は異なる通貨間における決済の可能性を示している。私たちはこのネットワークを“中曾の中央銀行多角スワップ・ネットワーク”とよぶことにする。

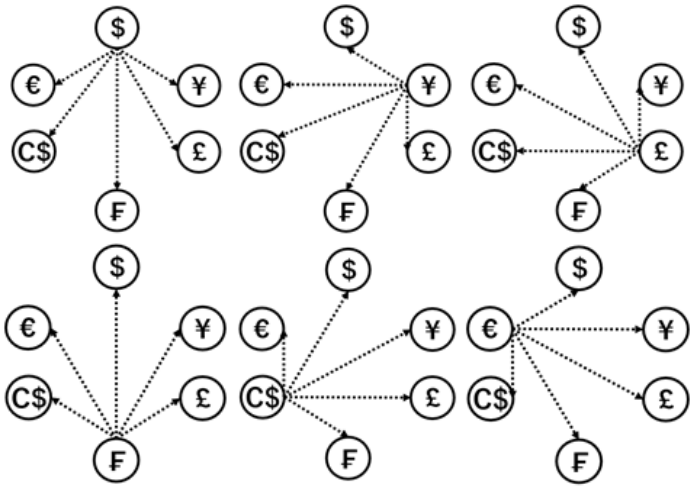

Fig. 3. 中曾の中央銀行放射状ネットワークの相互拡張

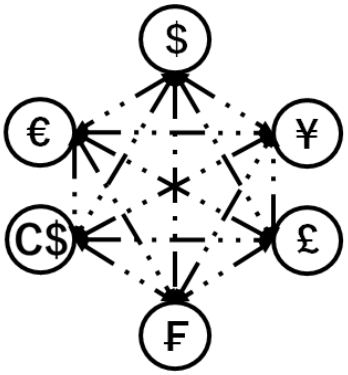

Fig. 4. 中曾の中央銀行マルチラテラル・スワップ・ネットワーク

さて、中曾の中央銀行マルチラテラル・スワップ・ネットワークをより詳細に調べてみよう。第一に、このネットワークのすべてのノードは中央銀行であることに注意しよう。そこにはいかなる利潤動機で活動する利用者も存在しない。あらゆるノードはグローバルな信用秩序の維持、ないし危機的状況においてはその事態の収拾のみを目的として、協調的に介入する。第二に、このネットワークには特権的なノードが存在しないことに注目しよう。この多角的なネットワークはシステム全体に対して信用の中心が存在しないという特異な性質をもっており、すべてのノードが公共性にのみ基づいてお互いに決済をおこなう。このネットワークには信用の中心がなく、すべてのノードが平等につながっているため、peer-to-peer ネットワークとなっている。このネットワークのグラフ構造はすべてのノードがお互いに結ばれており、“完全グラフ“を構成している。

4. ブロックチェーンの P2P ネットワーク構造

2008 年、“Satoshi NAKAMURA”はホワイトペーパー"Bitcoin: A Peer-to-Peer Electronic Cash System" を世界金融危機の直後に発表した[6]。2009 年 1 月、現在の暗号資産の基盤技術となっている“ブロックチェーン”はシステム実装された [14]。第 2 節で述べたように、ビットコイン以前のすべての電子貨幣システムは例外なく銀行のような信用中心をもった放射状ネットワークの構造を持っていた。ところが、ビットコインは信用中心を欠く peer-to-peer ネットワークと見なすことができる。

2008 年の世界金融危機は金融機関における情報の寡占が部分的な原因となって引き起こされた[15]。 “Satoshi NAKAMOTO”名義の開発者は金融システムにおける特権的な情報の非対称性を批判した[16]。すべてのノードが完全に対等に扱われ、利用者がお互いに直接決済が可能な完全グラフ構造をもった電子通貨ネットワークのシステムを NAKAMOTO は提唱し、それが実装可能なシステムであることを示した。Fig. 4 および Fig. 5 からこれらのネットワークは極めて類似していることが見て取れる。すなわち、これらはいずれも完全グラフの構造を持っている。しかしながら、これらの間には、いくつかの決定的な違いがある。

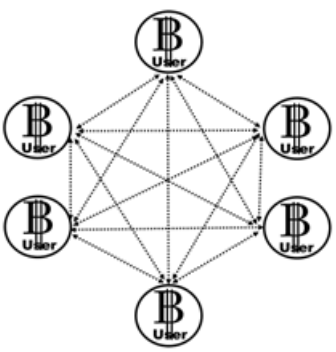

Fig. 5. ビットコインの P2P ネットワーク

まず、Fig. 4 のスワップ・ネットワークでは複数（6 種）の通貨が交換されているのに対し、Fig. 5 のネットワークでは唯一の通貨としてビットコインだけがやり取りされている。その他の違いとしては、“マイニング機構”の存在などが挙げられるが、これらの図には明示されていない [3]。Fig. 4 で見られる peer-to-peer ネットワークは公共性もつ中央銀行からなるが、Fig. 5 のネットワークでは、マイニング競争を通じて利潤を追求する利用者からなる。Fig. 5 におけるネットワークではそのシステムを維持するためにブロックチェーン技術が新たに導入されており、Fig. 4 の中曾の中央銀行マルチラテラル・スワップ・ネットワークではブロックチェーン技術は用いられていない。

ここで、ブロックチェーン・システムについて簡単に確認しておこう [4]。Satoshi NAKAMOTO 名義のブロックチェーンの開発者（たち）は信用中心のない電子通貨を実現するために二つのアイディアを組み込んだ[6][17]。第一に、NAKAMOTO はネットワーク全体で決済情報を共有するようにシステムを設計した。この情報は伝統的なシステムの信用中心によって排他的に独占されていた。この構想では、特定のプライバシー・ポリシーのもとで、台帳情報はすべてのノードによって対等に共有される。これにより、この新しいアプローチはシステム全体における会計の透明性を保証している。第二に、NAKAMOTO はいかなるコインの偽造も回避するよう努力した。デジタル通貨は単なるデジタルな数値情報にすぎないので、適切な不正回避の機構なしには、制限なくコインを複製することができてしまう。元来はこの問題を解決するために、NAKAMOTO は利用者によるコインの二重使用を困難にする電子署名技術を適用した。ここでは正当性が承認された決済が記録された台帳の“ブロック”を10分ごとに確定する仕組みが実装された（Proof-Of-Work）。このシステムをブロックチェーンという。すべてのノードは“正当性を承認する問題”を解く上で完全に対等である。また、その問題の難易度は新しいブロックを適切に有効化するように調整されており、各ブロックは公正な決済によってのみ構成されている。ビットコインはこの問題を最も早く解決したノードに報酬として発行される。そのような競争原理を導入することで投機的な動機を刺激し、ビットコインはまたたくまに成長していった。

ビットコインの総発行数はあらかじめ定められており、それぞれのマイニングに対する発行数は徐々に逓減していく。ビットコインは金本位制のような金地金の準備が必要ない純粋な管理通貨と見なせる。また、ビットコインのシステムは利息の概念を欠く。ビットコインは既存の金融システムを否定するように設計されている。このシステムは純粋な等価交換と解釈することができ、共産主義社会と類似したものと見なせる。利子収入とは、既存の金融システムにおいて、特権的なノードである銀行に預金することによって発生する。

2019 年 6 月、Facebook が中心となって設計した“Libra”プロジェクトが公表された。アメリカが最も極端な反応を示した[18]。US は Libra の開発をやめるようにと要求した。アメリカはこのデジタル通貨を米ドルへの脅威になりうるとみなしたためだ[19]。

---

[3] マイニングは我々の議論には関係してこないことから、その詳細については論じない（[17]を参照せよ）。

[4] ここでは、本論文では、私たちの議論は Proof-Of-Work に関連しないので、その説明の詳細は割愛することにする（[17]を参照せよ）

以下では、Libra の基本的な構造を調べるに先立って、岩井克人の議論、すなわち、金融秩序を維持しながら貨幣が流通し続けるための要請について理論的に概観する。

5. 岩井克人による貨幣に関する議論と中央銀行の中立性

岩井克人は、投機の対象となってしまったことで、ビットコインは通貨として流通する可能性がなくなった、と指摘する[7]。一般に、投機商品の市場価格は激しく変動する。もし、暗号通貨が安定した貨幣価値を維持するなら、貨幣として流通する可能性がある。Facebook の Libra は“Stable Coin”として活用することで貨幣価値の安定という条件を満たしている。岩井は、同様に、自由なグローバル経済市場の成長を支えるためには、過剰な利潤動機に基づいた新自由主義は適切に制御されるべきであると主張する[7]。高い揮発性のため、ビットコインはもはや貨幣として流通しない。2008 年の世界金融危機が不適切な投資や融資によって引き起こされたことを想起しよう。1933 年の世界恐慌直後に制定されたグラス＝スティーガル法は 1999 年に撤廃された[15]。金融危機や恐慌は投機による金融市場の毀損によって生じる。 岩井は利潤動機のない中央銀行のような独立機関の市場への介入がグローバル金融システムの安定と、金融危機や恐慌を回避に必須不可欠であると指摘する。 これを “岩井の中央銀行中立性”の要請と呼ぶことにしよう。岩井は利潤動機をもたずに市場を規制する組織を“ビッグ・ブラザー”と呼ぶ [5]。中央銀行は“岩井のビッグ・ブラザー”の典型である。

暗号資産を活用してグローバル経済の決済システムを安定させるためには、私たちは、岩井のビッグ・ブラザーを必要とする。私たちは、この基本的な要請を岩井の通貨不安定性の原理とよぶことにしたい。また岩井は、行き過ぎた自由主義はグローバル金融の安定性や自由貿易システムに対して危害を及ぼす可能性が高い、と指摘する。

次節から、私たちは、Facebook の Libra を岩井の主張を参照しつつ概観する。

6. Facebook の Libra 案

2019 年 6 月、27 億人の利用者を擁する Facebook は、クレジットカード大手である Visa や Mastercard などを含む大手企業 27 社と共同で、電子通貨 Libra の構想を発表した[8]。これに対し France の Chantilly で行われた G7 先進国首脳会議では、各国財務大臣や中央銀行関係者が、Libra を厳しく監視する必要があると結論付けた[20]。Facebook は Libra を多くの点でその他の暗号資産と異なる性質を孕むブロックチェーン技術を用いた電子通貨であると説明している[8][9]。

第一に、Libra は、法定通貨を含んだ実体資産で構成される準備基金によって、価値の変動（ボラティリティ）を抑制する。これはビットコインが達成できずに終わった性質でもある[8]。J. M. Keynes によって提唱され、20 世紀後半に普及した管理通貨制度よりも、Libra はむしろ 19 世紀

[5] George Orwell の小説“１９８４”に登場する“Big-Brother”から取っているという[7]。

に支配的であった基軸通貨の性質を有している。この古典的なシステムは不安定で、信用不安が生じた場合、取付騒ぎを招きかねない。

Libra システムは三種類のステークホルダーから構成される； 第一は、投資家で、準備基金に多様な資産を提供する。第二は、Libra Association で、このシステムを管理する。第三は、Libra の利用者であり、商品やサービスの決済にこの“貨幣”を使う。これらは Fig. 6 に概念図としてまとめた。一見すると、Fig. 6 は Fig. 4 や Fig. 5 似た構造をもつように見える。しかし、よくみると Libra のシステムには特権的な信用中心のノードが存在している。これこそが Libra とビットコインのネットワークの本質的かつ最大の相違点である。Fig. 6 の中では、この特権化ノードは“f”と表記されている。この“f”は金本位制における兌換銀行のような役割を演じる。投資家にとってこのノード“f”は、投資が利益を産み出すノードになっていることに注意によう。したがって、この“f”は、ヘッジ・ファンドと同じように、Libra を発行する投資銀行の機能を果たす。Libra システムは銀行と投資ファンドを分離する意味において潜在的に深刻なリスクを孕んでいる。利用者は、共通の通貨“Libra”で決済をするが、“Libra“は“f”を兌換銀行として米ドルやユーロなどの法定通貨とも交換可能であることから、私たちは、Fig. 6 で利用者を結ぶ矢印と、利用者と“f”を結ぶ矢印を区別している。

第二の本質的な特徴は、この電子通貨の交換は、それだけでは如何なる利息も産み出さないことである。これにより、“Libra 利用者”のネットワーク＝社会の資産経済の成長の制約条件となる。利用者の Libra 資本は如何なる利息によっても増大することがない。ある国家において同様の状況を想定してみよう； この国の金融資本は利息によって成長することができない。海外投資家たちは、実体経済が成長した場合、Libra 準備基金から配当を受ける。しかし、国民＝Libra 利用者の金融資産の成長は明らかに制限される。Libra 準備基金は利潤を追求する投資銀行としての役割を演じ、中央銀行の公共性とは完全に異なる性質である。

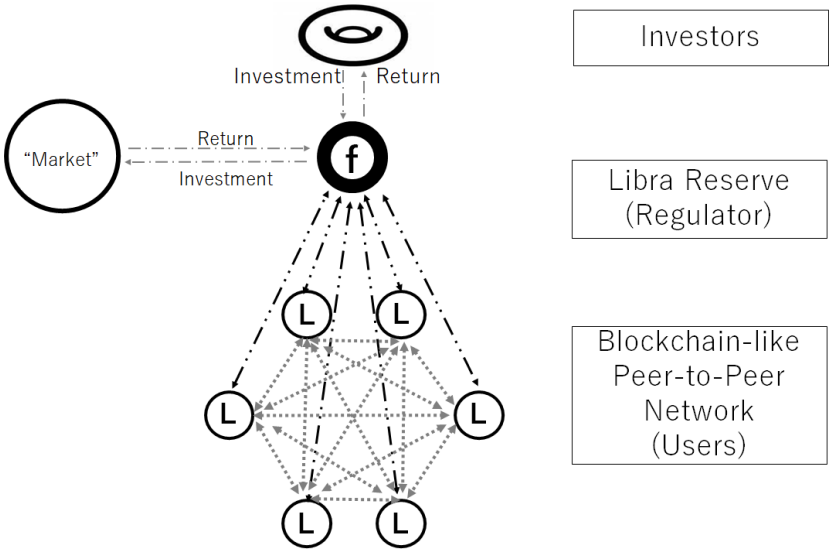

Fig. 6. Libra ネットワークの概念図

第三に、Libra Association は公平かつ独立した第三者機関として運営されると Facebook は主張する。その本拠地はスイスにおくとされるが、この第三者機関は投資家たちにとっての平等を保障している。貨幣の発行者として中央銀行が持つべき公平性の要求は満たされていない[8]。Libra Association は民間企業として明確な利潤動機に基づいて経営判断をするだろう。Libra Association は金融システムの安定を維持するための中立な金融政策を講じることができない。したがって Libra は、長期的に安定したグローバル通貨として機能することが困難である。現状の構想では、利用者たちが織り成すネットワーク社会は“投資家”たちの“電子植民地”と見なせる。

7. グローバル暗号資産の条件

では、どのような暗号資産ないしグローバル電子貨幣が考案されるべきなのか？Facebook のような民間企業に公共性あるグローバル通貨管理の中核を担うことは困難である。岩井克人が指摘するように、金融システムは、公平かつ公正な仲裁者なしで秩序を保つことが難しい。利潤動機のない仲裁者が不在の状態では、金融緩和のような適切な金融政策を施行することでシステム全体の安定を取り戻すことはできない。

この問題を視野に入れて、J. M. KEYNES は“神の見えざる手”が 1929 年の世界大恐慌を回避できなかったことを指摘する。中央銀行による通貨管理や政府による公共投資のように、公共的かつ中立的な立場に基づいた金融政策や財政政策の必要性を主張したのである[21]。

私たちは中曾のマルチラテラル・スワップ・ネットワークのような中央銀行のみから構成されるシステムを考えることができる（Fig. 7 参照）。このネットワークには自己利益を追求する民間企業は存在しない。私たちは、ビットコインに類似した peer-to-peer ネットワークシステムにより、オリジナルなグローバル決済システムを考えることができる。このネットワークは 1944 年に KEYNES が Breton Woods 会議で提案したシステムに類似している[3]。

KEYNES は前世代的な金本位制を管理通貨制度に置き換えることを提唱した。彼は“BANKOR”と名付けたシステムを提案する。それは peer-to-peer ネットワークの構造をもつものであった。だが、このアイディアは彼自身よるものではなく、ドイツで生まれナチ時代にイギリスに移住した Ernst Fritz SCHUMACHER（1911－77）の原案を変形したものであった[22]。KEYNES は新たな基軸通貨として”BANKOR“を提案したが、それが採択されることはなかった。Breton Woods 会議は米ドルを唯一の金と兌換可能な通貨として定め、米ドルを基軸通貨とする IMF 案を採択する。部分的に金本位制は残された[3]。1971 年、Richard NIXON が米ドルの金兌換を廃止し、管理通貨制度に移行して以降も、なお米ドルは事実上の基軸通貨として健在である[4]。このような米ドル中心のグローバル経済システムに対して、Libra は潜在的な脅威となりうる。

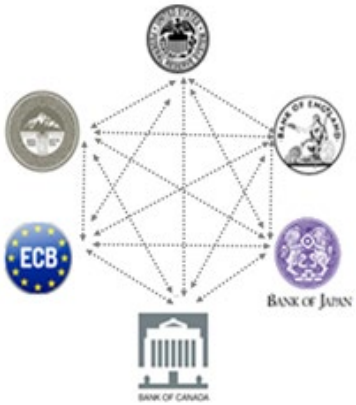

Fig. 7. 中央銀行のみのよる P2P ネットワーク

KEYNES と SCHUMACHER は国際的な決済同盟“Clearing Union”の P2P システムを考えた。この観点を参照するとき、Satoshi NAKAMOTO の P2P システムには本質的に不足している点がある。ブロックチェーンは極端に単純化された一種の単式簿記であることに注意しよう。

一般には、NAKAMOTO のブロックチェーンは電子「通貨」とみなされるが、その実体は不完全かつ独特な単式簿記“台帳（Ledger）”である。そこでは最低限のセキュリティが電子著名などの技術を応用することで確保されている。しかしながら、公正な経済システムを維持するために欠かせない会計監査には、借方や貸方の情報が必須である。以下では、私たちは暗号セキュリティの議論はおこなわない。会計監査の議論には不要であり、実装の段階でシステムに必要な暗号技術を導入すれば十分だからである。加えて、中央銀行の peer-to-peer ネットワークは利潤動機に基づくマイニング競争がない。したがって、私たちはマイニングに関係する詳細を省略する。Fig. 7 にあるような6つの中央銀行から成る peer-to-peer ネットワークがあるとき、私たちはこれらの間における決済を6×6の正方行列によって表現することができる（Fig. 8）。私たちはこの行列 X を元取引行列と呼ぶことにする。

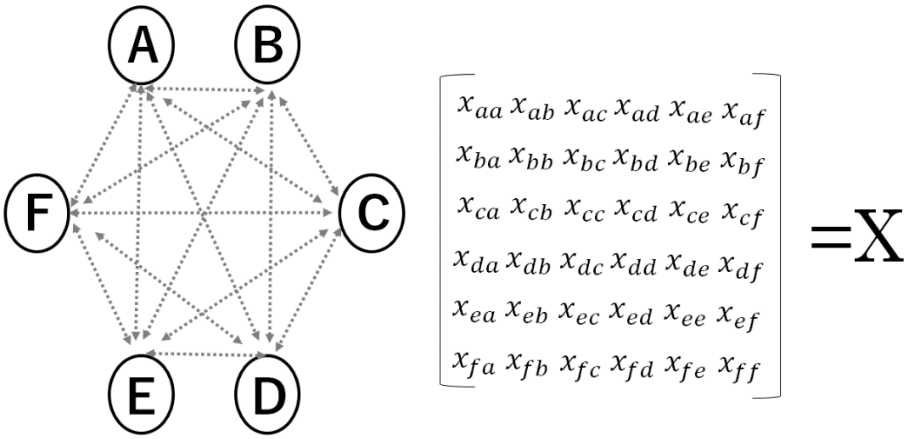

Fig.8 元取引行列

元取引行列の対角成分と非対角成分は、それぞれ異なった意味をもつ。非対角成分は中央銀行間の取引を示す。一方、対角成分はそれぞれの中央銀行が保有する資産の総量を示す。そこで、私たちはこの元取引行列を二つの部分に分けることにしよう(Fig. 9)。

さらに、私たちは適切な取引情報を紐づけることで、元取引行列を含むデータベースにまとめ上げることができる。私たちは元取引行列の対角成分のみからなる行列を元ストック行列とよび、非対角成分のみからなる行列を元フロー行列と呼ぶことにしよう。ブロックチェーンのシステムでは、私たちはそれぞれの取引を貸方や借方で確認することができない。また、すべてのノードが中央銀行で構成されたネットワークの場合は、システムのセキュリティを保証するための暗号化が必要ない。

現実には、元取引行列は上で示したような簡単な形にはならないだろう。しかし、資金のストックとフローを行列の形式で表すことで、わたしたちは適切にすべての取引を正しく会計監査を実行可能な形で整理することができる。さらに、私たちはそれらの元取引行列を行列型のデータベースに拡張することで、容易にすべての取引情報を把握できるはずである。私たちはこのようなシステムを“ポスト・ブロックチェーン”を呼ぶことにする。各会計年度の財務諸表を行列を含むデータベースと見なすことができる。さらに、私たちは、前年度のストック行列に次年度のフロー行列に作用させることで次の会計年度のストック行列を得ることもできるだろう。

$$X = \begin{bmatrix} x_{aa} & 0 & 0 & 0 & 0 & 0 \\ 0 & x_{bb} & 0 & 0 & 0 & 0 \\ 0 & 0 & x_{cc} & 0 & 0 & 0 \\ 0 & 0 & 0 & x_{dd} & 0 & 0 \\ 0 & 0 & 0 & 0 & x_{ee} & 0 \\ 0 & 0 & 0 & 0 & 0 & x_{ff} \end{bmatrix} + \begin{bmatrix} 0 & x_{ab} & x_{ac} & x_{ad} & x_{ae} & x_{af} \\ x_{ba} & 0 & x_{bc} & x_{bd} & x_{be} & x_{bf} \\ x_{ca} & x_{cb} & 0 & x_{cd} & x_{ce} & x_{cf} \\ x_{da} & x_{db} & x_{dc} & 0 & x_{de} & x_{df} \\ x_{ea} & x_{eb} & x_{ec} & x_{ed} & 0 & x_{ef} \\ x_{fa} & x_{fb} & x_{fc} & x_{fd} & x_{fe} & 0 \end{bmatrix}$$

$$= \quad S \quad + \quad F$$

Fig. 9. 元ストック行列と元フロー行列

ストック行列とフロー行列はそれらが互いに関係しあった連鎖の系列として考えることができる。これ以降の段階で、適切に暗号化をシステムに適用すればセキュリティの確保が可能であろう。私たちはこのシステムが二つの種類の行列が相互に作用しあうこと、またその様子がリープ・フロッグ・アルゴリズムに類似していることから、この暗号資産システムを“フロッグ-チェーン”と呼ぶことにする[23]。

さて、すべてのノードが中央銀行からなるネットワークにおいて、各ノードが利益中立的に行動するとしても、おのおのの国益という背景は免れることができないだろう。そこで、ちょうど国際決済銀行に相当するような、個別の国家から独立した“中央銀行の中央銀行”を考えてみよう（Fig. 10）。Fig. 10 のネットワークは peer-to-peer システムの構造 (Fig. 5 and Fig. 7)と異なっていることに注意する。この構造は Fig. 6 で示した Libra の構造に一部類似している。Fig. 10 で、“Z”は”中央銀行の中央銀行“を表している。

Fig. 6 と Fig. 10 にはいくつかの相違点がある。第一に、Fig. 10 のネットワークのすべての矢印は同じ種類の双方向矢印となっている。このシステムの暗号資産は金地金や法定通貨などからなる準備基金を必要としない。このネットワークは SCHUMACHER や KEYNES によって提唱された ”Clearing Union”と同様、完全な管理通貨制度の下で運用される[24]。さらに、Fig. 10 では、いかなる利潤動機をもった投資家も存在しない。このネットワークは岩井の中央銀行中立性に立脚して中曾の中央銀行マルチラテラル・スワップ・ネットワークを発展させることで得られる。そこで、私たちはこのネットワークを“中曾-岩井のポスト-ブロックチェーン・ネットワーク”と呼ぶことにしよう。

中曾-岩井のポスト-ブロックチェーン・ネットワークの実例は続稿で展開する予定である。

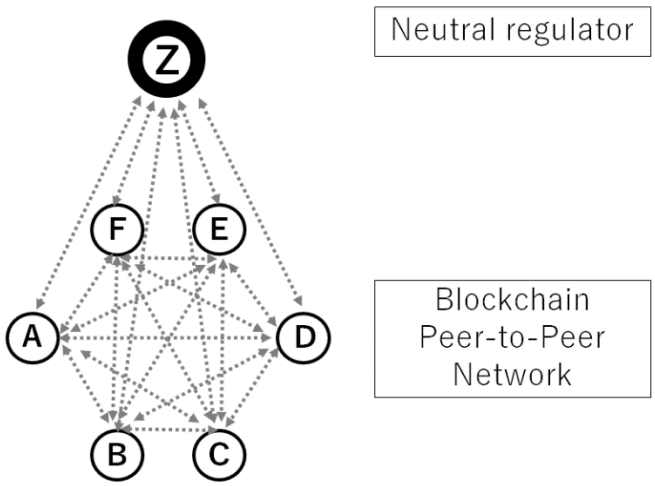

Fig. 10. 中曾-岩井のポスト・ブロックチェーン・ネットワーク

8. 結論および留意点

本稿を閉じるにあたり、2030 年国連アジェンダを参照しつつ論旨の全体を振り返ってみよう[25]。

2030 年国連アジェンダは SDGs；Sustainable Development Goals としても知られ、持続可能なグローバル社会経済の発展を達成するための 17 分野にわたる詳細な目標から構成される。それらの中で、貧困撲滅ないし格差是正は、G20 や G7 などの指導者会議でも繰り返し強調されている[20]。

2019 年現在、人類の大多数が貧困に苦しむ一方で、ごく少数の富裕層が世界の富の大半を独占している。

岩井克人は Anthony ATKINSON や Thomas PUKETTY らの経済・社会格差に関する研究を援用しつつ、営利企業が基幹技術革新（Core Innovation）を担うと、開発の方向性が資本家の利益追求へと偏向する傾向に警鐘を鳴す[7]。また、PIKETTY による、資本の利益率が経済成長率を上回ることに起因する格差拡大の説明は広く知られることとなった[26]。 PIKETTY の議論を考慮しつつ、岩井は“株主資本主義”を批判する[7]。もっぱら、株主の利益を追求し、公共性ある仲裁者が不在の金融システムは、長期的な安定と成長を実現できない。本論の結語に換えて、Facebook の Libra を SDGs アジェンダの観点から検討してみよう。

第一に、持続性について、公共性ある仲裁者を欠くシステムは公平な金融政策を講じることができず、Libra は持続的でない可能性が高い。

第二に、発展性について、Libra はその使用地域で Libra 使用者の資産経済成長の足かせになる可能性が高い。Libra は利用者間では等価交換されるのみであり、そこでは、利息による資産経済の成長が見込めない。Libra は既存の金融システムに参加できない 17 億の人々に参加の機会を提供する、と Facebook は主張する[8]。17 億の人々に新たな情報的な繋がりが提供されることは、当該地域の実体経済を成長させる潜在的な可能性を秘めている。しかし、Libra 構想の概念図（Fig. 6）は、Libra のシステム全体から得られる成長の恩恵が発展途上国の人々ではなく、主として投資家にもたらされる懸念を示している。

第三に、格差是正や貧困撲滅について、現在の Libra 計画は、巨大企業が自らの利潤を追求するため協力、発展させていく構図となっており、ATKINSON や IWAI が厳しく批判する典型的な株主資本主義に他ならない。現状の Libra 計画は持続可能なものではなく、格差や貧困を悪化させる懸念がある。

以上のように、現行の Libra 案は地域経済の発展を妨げる可能性があり、格差や貧困の問題を悪化させ、持続可能性や安定性を欠くものであると言わざるを得ない。これらの問題点を克服するため、私たちは“中曾-岩井のポスト-ブロックチェーン・システム”を、来るべきグローバル暗号資産に課されるべき条件として考えたい。ここで、私たちは Facebook の Libra 案のもつ可能性を全面的に否定しているわけではないことを注記しておく。現行案は非常に多くの深刻な欠点を孕んでおり、その実装はグローバル経済に危機をもたらしうる。しかし、適切な形でこの種の電子通貨が普及した場合、SDGs アジェンダで掲げられる深刻な問題のいくつかを解決ないし軽減する可能性も指摘することができる[6]。

有用な多くの議論を共有された Lang WILLET、Kerryn POOK および Michelle YATSUZUKA に深く感謝する。

[6] 我々は続稿で具体的なモデルについて論じる予定である。

References

[1] Hayek, Friedrich, “The Restriction Period, 1797-1821, and the Bullion Debate”, 1991, The Trend of Economic Thinking., ISBN 978-0865977462.

[2] John K. Galbraith, “The Great Crash 1929”, 2009, MARINER BOOKS.

[3] Steil, Benn, “The Battle of Bretton Woods: John Maynard KEYNES, Harry Dexter White, and the Making of a New World Order”, 2013, Princeton University Press. ISBN 978-0-691-14909-7.

[4] Lewis, Paul, “Nixon’s Economic Policies Return to Haunt the G. O. P.”, August 15, 1979, The New York Times.

[5] H. NAKASO, "Evolving Monetary Policy: The Bank of Japan's Experience - Speech at the Central Banking Seminar Hosted by the Federal Reserve Bank of New York -", 2017, Bank of Japan, https://www.boj.or.jp/en/announcements/press/koen_2017/ko171019a.htm/

[6] Satoshi NAKAMOTO,“Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, www.bitcoin.org.

[7] K. ITO ed. “Encrypted Asset and the Capitalism”, 2019, to be published by The Tokyo University Press.

[8] The Libra Association Members, “An Introduction to Libra”, 2019, https://libra.org/enUS/white-paper/

[9] Zachary Amsden, Ramnik Arora, Shehar Bano, et. al., “The Libra Blockchain”, 2019, https://developers.libra.org/docs/the-libra-blockchain-paper

[10] Mead, Carver A. and Conway, Lynn, “Introduction to VLSI systems.”, 1980, Boston: Addison-Wesley. ISBN 0-201-04358-0.

[11] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, 1978, dl.acm.org.

[12] Davit S. Evans, Richard Schmakensee, “Paying with Plastic: The Digital Revolution in Buying and Borrowing”, 2004, The MIT Press.

[13] Finn Brunton, “Digital Cash; The Unknown History of the Anarchists, Utopians, and Technologies Who Created Cryptocurrency”, 2019, Princeton University Press.

[14] "Block 0 – Bitcoin Block Explorer". Archived from the original on 15 October 2013.

[15] Jacob Soll,“ THE RECKONING: FINANCIAL ACCOUNTABILITY and the RISE and FALL of NATIONS ”, 2014, Basic Books.

[16] "Satoshi's posts to Cryptography mailing list". Mail-archive.com. Retrieved 26 March 2013.

[17] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, 2016, Princeton University Press.

[18] See https://www.theverge.com/2019/6/18/18684268/facebook-libra-cryptocurrency-stop-congress-house-democrat-maxine-waters-regulation

[19] See https://medium.com/hackernoon/the-shocking-reason-why-the-united-states-wants-to-stop-libra-5ee97d68647e

[20] See https://www.japantimes.co.jp/news/2019/06/29/national/full-text-g20-osaka-leaders-declaration/#.XX07bSj7SUl

[21] J. M. KEYNES, “ The General Theory of Employment, Interest and Money ”, 1936, Palgrave Macmillan.

[22] Barbara Wood,“ E. F. Schumacher, his life and thought ”, 1984, Harper & Row1st U. S. ed.

[23] Radford M. Neal, “MCMC using Hamiltonian dynamics”, 2012, arXiv:1206.1901v1[stat.CO] 9 Jun 2012.

[24] E. F. SCHUMACHER, “ Multilateral Clearing ”, 1943, Economica-New-Series-Vol.-10-No.-38-May-1943-pp.-150165.

[25] See https://www.un.org/sustainabledevelopment/

[26] T. PIKETTY, "Capital in the Twenty-First Century", 2014, The Belknap Press of Harvard University Press.