ビットコインから考える共存共栄の社会

ブロックチェーンに学ぶ分散型処理

小森三郎

目 次

目　次

まえがき

第1章 従来のコンピュータシステム
コンピュータの利用史　／設置場所が一か所　／中央集権型システムの処理形態

第2章 ビットコインのシステム
ビットコインシステムとは　／ビットコインシステムの設計思想
／システム全体で二重支払い防止

第3章 ビットコインシステムの革新性
国家に頼らない通貨の創発　／管理者のいないネットワーク　／参加と離脱が自由なノード
／汎用データが取り扱える設計　／オープンソフトウェア

第4章 ビットコインシステムの仕組み
ノードの自立と連携　／仮想通貨を実現した仕組み　／分散台帳のイメージ

第5章 ビットコインに触発されたシステム
イーサリアムとは　／ピアコインとは　／リップルとは　／リブラとは

第6章 ブロックチェーンから考えるシステム
ブロックチェーンの革新性　／巨大ＩＴ企業のコンピュータ利用
／共存共栄のコンピュータ利用

あとがき

参考文献

まえがき

ビットコインは、報道で相場価格の大幅な上下変動及び取引所からの資金流出で、時々話題になりました。それでも、今やビットコインに関心をよせるのは、投資家やＩＴ技術者だけでなく、経済学者はもちろんのこと、起業家や政治家など多くの人に及んでいます。ビットコインは、謎の人物ナカモト・サトシが考案した仮想通貨（外国では暗号通貨と称す）です。ビットコインは、信用すべき金融機関なる第三者がなくとも、信頼できる送金システムとして正確に作動します。ビットコインシステムは、仮想通貨を暗号化して正確に相手へ送り、記録した台帳は事実上改ざんできません。多くの人が関心をよせるのは、通貨としての投機的なビットコインの魅力よりも、正確な分散型処理の社会性に魅了されるからです。分散型処理では、管理主体がなくともシステム全体が統一的に作動します。

ビットコインは、従来の中央集権型処理と真逆の分散型処理です。分散型処理は、自立したコンピュータ同士がコンピュータ間連携を取りながら、統一のとれた動きをします。革新的なビットコインの仕組みが、信用すべき第三者が介在しないシステムで発生する送金問題を巧妙に解決しました。仮想通貨は電子的なものであり、取引を電子的に記録する必要があります。電子的なお金を送る行為は、お金を送るとき、そのコピーを手元に残して置いたら、何度も同じお金（＝ニセ金）を使えます。ナカモト・サトシは、二重支払い問題を複数の仕組みで解決しており、送金取引処理順にバラして説明します。その仕組みは、ひとつの生態系のようであり、コンピュータとコンピュータシステムを支える人間集団が、合目的な動きをします。この合目的な作動原理に、多くの人が関心をよせるわけです。

作動原理を支える技術が、ブロックチェーンです。従来の中央集権型処理にブロックチェーンを適用できますが、長所が生きません。ブロックチェーンは、分散型処理に適用してこそ長所が生きます。分散型処理とブロックチェーンを結び付ける考えは、共存共栄にあります。中央集権型処理に活用していたＩＴ技術が、ビットコインによって、分散型処理にも使えることが例証されました。我々は、地球全体を覆う持続性の暗雲から文明の転換期を感じます。ビットコインの作動原理は、社会づくりを考えたうえの民による分散型処理システムであり、ブロックチェーン技術を共存共栄の作動システムに応用できます。ブロックチェーン技術を生かした共存共栄システムは、混迷及び混乱のグローバル資本主義を突破します。

第1章 従来のコンピュータシステム

コンピュータの利用史

１９６０年頃に事務処理用のコンピュータが登場しました。コンピュータの利用は、バッチ処理
でした。バッチ処理とは、データをまとめて一括に処理する意味です。企業では月１回の給与計算
、在庫管理などにコンピュータを利用しました。

１９６４年（昭和３９年）の東京オリンピックの後に、ＩＢＭ社が当時の三井銀行の普通預金の
事務処理にコンピュータを適用しました。この時のコンピュータ利用は、オンラインリアルタイム
処理です。利用者が、支店の窓口に普通預金通帳と支払い伝票を出すと、窓口の行員が端末を操作
し、データは回線を通じて中央のコンピュータに届くと、たちどころに事務処理を終え、返答を支
店の端末に返しました。端末の操作完了から返答が来るまでの間は、即時処理され数秒です。この
成功の影響は、全国の金融機関に波及し、その後１９８０年代に金融機関は、第三次オンラインシ
ステムを次々と稼働させました。

１９９５年にパソコンの登場により、コンピュータの利用形態に革命が起きました。しかも、パ
ソコンには今のウェブブラウザが組み込まれていました。パソコンと中央のコンピュータをインタ
ーネットで結び、パソコンと中央のコンピュータで文字情報以外の画像など複雑な処理を機能分担
することができました。この処理形態は、サービスを利用する側とサービスを提供する側の合作と
なり、クライアントサーバ処理といいます。その後、スマートフォンの登場により、サービスの提
供が多種多岐にわたり、クライアント側の利便性は一段と増しました。

設置場所が一か所

クライアントサーバーの処理形態に至っても、サービスを提供する側は、オンラインリアルタイ
ム処理と同様一か所で処理をします。しかも、サーバーを管理するのはサービス提供者です。サ

ー
ビス提供者は企業であり、サービス提供者が利益を得るために、サーバーを管理します。

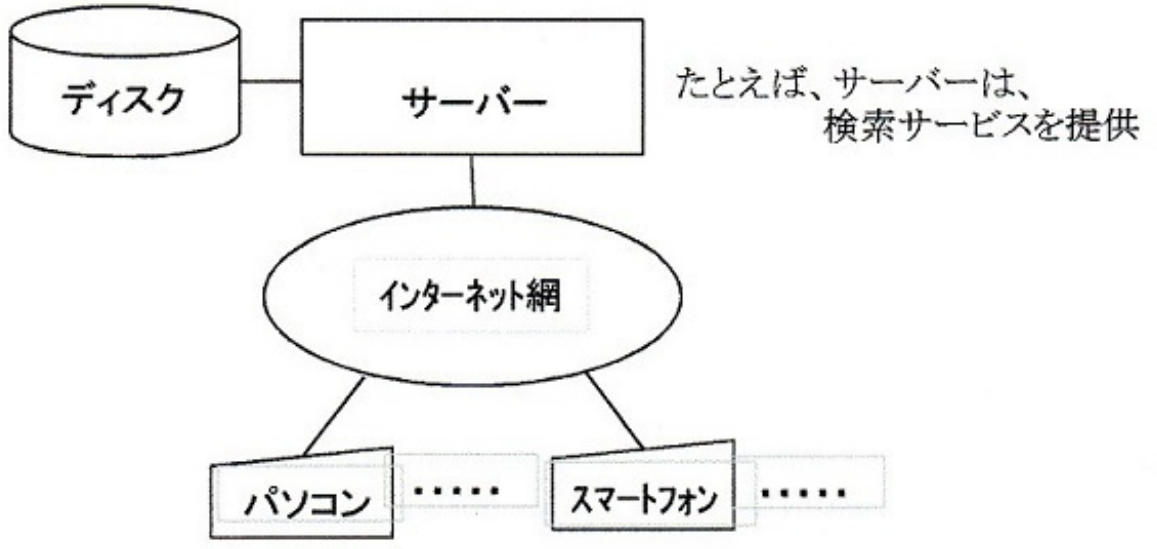


図１：クライアントサーバの処理形態

　サービス提供者は、組織の都合上どうしても一か所のサーバーにデータを集め処理します。（図
１参照）サービス提供者がサービスで利益を得るために、データを集める作業及びサーバー管理を
一か所ですると、システム維持費用が大きく下がります。クライアントサーバーの処理形態は、別
名中央集権型システムといいます。従来のコンピュータシステムは、全て中央集権型システムです。

　中央集権型システムの処理形態
　中央集権型のシステムは、処理場所が一か所ゆえ、一か所でディスクを保管します。データは、
あらかじめサーバーのディスクに保管されます。銀行の勘定系システムを例に取れば、口座開設時
に新規に個人データがディスクに保管されます。銀行ＡＴＭから現金の引出し依頼があれば、コン
ピュータはディスクの口座残高を書き換え、つまり更新します。中央集権型システムは、コンピュ
ータ及びサーバーの管理・保管と同時に、高度な処理も全て一か所で行います。この処理形態は、
バッチ処理から連綿と続く処理形態です。営利企業なら中央集権型システムが、当然です。

第2章 ビットコインのシステム

ビットコインシステムとは

ビットコインは、ナカモト・サトシという人物の名称で、２００８年１１月にインターネット上に掲載された論文（論文名　ビットコイン：Ｐ２Ｐ　電子通貨システム）で、初めて世に知られるようになりました。ナカモト・サトシは日本人名のようですが、今も正体不明で、名前も本名ではないと思われます。そのビットコインのシステムは、２００９年１月に稼働しました。実験的に運用が始まったビットコインは、当初ほとんど利用されず、ビットコインとして初めての商取引は、２０１０年の５月にあるプログラマが、１万ＢＴＣ（ＢＴＣは、ビットコインの通貨単位）とピザ２枚を交換したことだと言われています。そして、これを契機に次第に注目を浴び、現実の通貨と交換できる取引所及び交換所が整っていきます。今では、ビットコインに関心を寄せるのは、投資家やＩＴ技術者だけでなく、経済学者はもちろんのこと、起業家や政治家など幅広い人たちです。

ビットコインシステムは、ノード（図２の白丸）がインターネットを介して最大８ノードと繋がり、世界中におおよそ１１，０００か所に点在します。ノードには、利用者とビットコインシステムの間を取り持つ取引所ノードと、取引データが入っているブロックの承認作業専門のマイナーノードの２種類があります。図２の●は、ノードが保有しているディスクです。しかも、各ノードは同じデータを管理及び保存します。ビットコインシステムは、各ノードが保有しているファイルを頼りにトランザクション処理を進めます。しかも、各ノードは孤立しているのではなく、自分以外のノードと連携しながらトランザクション処理を進めます。ビットコインシステムは、システム全体を管理する運用管理者が不在の非中央集権型システム（＝分散型システム）です。

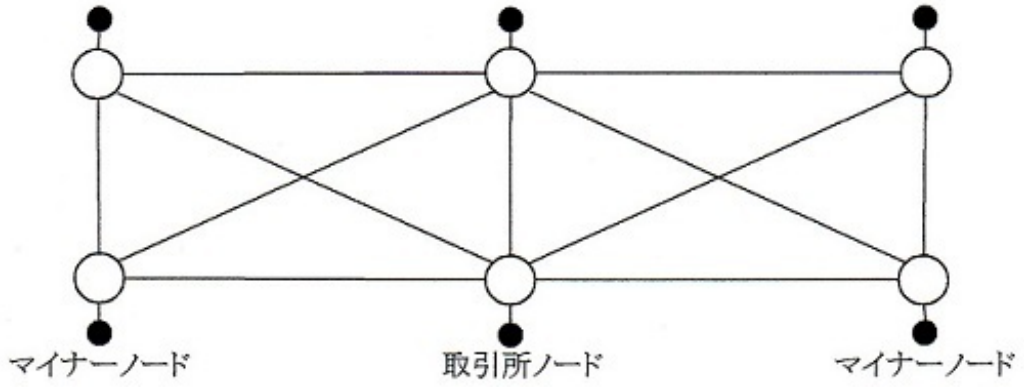


図２：ビットコインシステムのノード間の繋がり

ビットコインが目指すのは、現金のように人から人へと容易に移転できるシステムです。ビットコインシステムは、Ａさんから Ｂさんに、現金に代わり電子通貨（日本では仮想通貨、海外は暗号通貨）を匿名で送金します。この送金データは、世界中のノードに伝達され、世界中のノードがディスクに追加しています。ビットコインシステムは、ハッカーに狙われていますが、今のところ破られていないと言われています。ですから、ビットコインはセキュリティの強いシステムです。ちなみに、２０１４年にマウントゴックスから４６５億円が流出、２０１８年にコインチェックから５８０億円が流出したと報道されました。いずれも、取引所側のシステムに欠陥があり生じた事故です。ビットコインシステムからの資金流出の事故ではありません。

ビットコインシステムの設計思想

ナカモト・サトシは、第三者の金融機関を介在させることなく仮想通貨の送金を実現しました。従来の中央集権型システムの仕組みでも仮想通貨を問題なく執り行えるが、信頼に基づくモデルであるが故の脆弱性が問題になると指摘しています。つまり、金融機関には争議仲裁という避けられない責任があるため、完全に不可逆的な取引の提供ができません。具体的には、電子通貨受取人が電子通貨の所有者が過去に二重支払いしたか否かの検証ができない問題を挙げています。要は、電子的なお金を送るとき、そのコピーを手元に残して置いたら、何度も同じお金（＝ニセ金）を使

え
ます。この問題が、先ほどの二重支払い問題です。ナカモト・サトシはこれを解決する方法として
、取引履歴を時間順に積み重ね、そしてそれを書き換えできない形で記録し、受取人がそれを見て
過去に使われていないことを簡単に検証できるようにすれば、二重支払いは起こらないと言ってい
ます。
　つまり、すべての取引を公開された状態にし、その一元的な取引履歴をみんなで共有するシステ
ムを作り、検証により公正な取引であるかをお互いに常にチェックし、公正な取引のみを、書き換
えできない形で綴っていくようにすればよい、と言っています。そのための工夫が随所になされ、
システム全体で二重支払い問題を解決しています。これが、従来の中央集権型システムに代わる分
散型システムのビットコインです。
ナカモト・サトシは、ビットコインシステムを信用すべき第三者がなくとも、信頼できるシステム
として実現しました。これはノーベル賞級のとてもすごいことです。

　システム全体で二重支払い防止
　ビットコインシステムには、銀行やカード会社のように取引を媒介する第三者がいません。つま
り、第三者がお金の利用量を管理しないから、お金をコピーする二重支払い問題が常に付きまとい
ます。その解決に、システムがすべての取引を公開された状態にし、その一元的な取引履歴をみん
なで共有するシステムを作り、検証により公正な取引であるかをお互いに常にチェックし、公正な
取引のみを、書き換えできない形で綴っていきます。これを可能にしたシステムの仕組みを、分か
りやすさから送金取引処理順にバラして概要を説明します。詳細な仕組みは、第４章で説明します。
①　新しいトランザクション（＝取引）が発生すれば、全ノードに伝達されます。
②　各ノードが、新しいトランザクションを最新のブロックに取り込みます。
③　各ノードが、そのブロックに ｎ 個のトランザクションが集まると特殊処理（注）を始めます

。
④　各ノードは一斉に特殊処理をするが、一番最初に特殊処理に成功したノードが、そのブロック
の承認依頼を全ノードに伝達します。
各ノードは、そのブロック内の全トランザクションが有効かつ未使用の場合のみ、承認します
。
⑥　各ノードは、承認と同時にブロックチェーンを完成させます。各ノードは、検証により公正な
取引であるかを常にチェックし、公正な取引のみを、書き換えできない形で綴っていきます。
そして、すべての取引を公開されたファイル状態にします。
ビットコインのファイル処理は、従来の中央集権型システムと異なり、ファイルを更新せず、常
にファイルに取引データを追加します。ファイルの追加が全てのノードで行われますから、分散
かつ追加型です。しかも、ノードが保管しているデータは、すべての関係者が検索できます。
（注）　特殊処理とは、プルーフオブワーク（Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ：略称ＰｏW）
です。ＰｏWは、後程説明します。

第3章 ビットコインシステムの革新性

国家に頼らない通貨の創発

通貨の本質は交換の媒介であり、発行主体が何であるかは、あまり本質的ではありません。それ
でも長い間に、通貨の発行主体は国家であるとの固定観念が出来上がっています。一部の経済学者
は、通貨の発行主体が国家でなくてもよいと論じてきましたが、実現に至りません。通貨の物理的
性質としては、腐らないこと、朽ちないこと、複製できないことが重要です。それさえ満たせれば
電子情報でも構いません。言うは易し、実現は非常に困難です。ナカモト・サトシは、通貨の本質
を熟知したうえでコロンブスの卵的発想から、仮想通貨を構想しました。それは、完全なｐｅｅｒ
ｔｏ　ｐｅｅｒ（注）電子通貨の実現により、金融機関の介在無しに、利用者同志の直接的なオ
ンライン決済が可能なシステムを生みました。ここに、国家に頼らない通貨（＝ビットコイン）が
創発されました。ビットコインは、送金を介して通貨の交換を果たしています。
（注）人から人への直接的な移転をピア・トゥ・ピア（ｐｅｅｒ　ｔｏ　ｐｅｅｒ）といいます。

管理者のいないネットワーク

従来の中央集権型システムは、いずれも管理者が必須でした。ビットコインシステムは、世界中
にノードがおおよそ１１，０００か所に点在します。それぞれのノードは、世界中に分散し対等で
す。確固たる管理者不在でも、ノードはバラバラではありません。ナカモト・サトシの理念を継承
したシステムの開発集団（＝コア開発者）が、ビットコインシステムを先導しています。

コア開発集団は、ノード保有者からのビットコインの仕様改善などの意見調整を図り、ビットコ
インの仕様を変更します。コア開発者は、従来の中央集権型システムの管理者ごときですが、無償
奉仕です。このゆるい組織が、システムの維持及びソフトウェアの更新をします。企業は利益獲得

集団であり、上下関係がピラミッドのようになっています。しかし、コア開発集団を中心とするノ
ード仲間と利用者は、共存共栄の関係にあります。

参加と離脱が自由なノード

ビットコインシステムは、世界中にノードがおおよそ１１，０００か所に点在します。それぞれ
のノードは、参加が自由なら離脱も自由です。ノードの参加及び離脱は、ノード設置者の自由意思
で決めることができます。ノードの参加及び離脱が自由ゆえに、悪意のある人がネットワークに参
入してくることを想定しなければなりません。ビットコインシステムは、信用できない人がネット
ワークに参入してきても、信用できるシステムとして機能するように工夫しています。各ノードが
、ブロックチェーンのデータを検証し、悪意のあるノードからのデータを見つけ出し拒否します。
この仕組みは簡単ではないが、その仕組みにより、ノード全体がまるでひとつの生態系のような動
きをします。

汎用データが取り扱える設計

ビットコインシステムのトランザクションで使われるスクリプトには、様々なオペレーションコードと呼ばれる命令コマンドがあります。特筆すべき命令コマンドが、ＯＰ＿ＲＥＴＵＲＮです
。ＯＰ＿ＲＥＴＵＲＮは、トランザクション処理のアウトプットに送金以外の任意のデータを格納
しても、通常の送金トランザクションと同様に、ブロックチェーンなる台帳に書き込みができます
。つまり、事実上改ざんできない仕組みの台帳が、金融以外の用途に利用できます。この機能によ
って、あらるゆる分野に応用できます。つまり、ビットコインのような共存共栄のシステムが、あ
らゆる分野で実現できます。

オープンソフトウェア

ビットコインのプログラムは、誰でも無料で複製でき、改変も自由にできるオープンソフトウ

ェ
アです。ビットコインのノード保有者を多く募る必要性から、偉大な発明を無償公開したと思われ
ます。ただし、ソースコードを理解するには、とても高い技術力が必要です。

ノードの自立と連携

ビットコインシステムのノードは、自立分散で動いていますが、ノード全体としてはまるでひとつの生態系のように動きます。生態系に登場するのは、利用者・ノード保有者・ノードで動くプログラムの開発者です。その中で、ノードは自立しながらノード間を連携しますが、その仕組みは複雑です。ナカモト・サトシは、自立と連携の機能を、すべての取引を公開された状態にし、その一元的な取引履歴をみんなで共有するシステムを作り、検証により公正な取引であるかをお互いに常にチェックし、公正な取引のみを、書き換えできない形で綴っていくようにすればよい、と言っています。仮想通貨を実現した仕組みを、送金処理順にバラして説明します。

仮想通貨を実現した仕組み

（1） 公開鍵暗号方式による匿名性の確保

ビットコインは、すべての取引を公開された状態にします。すると、だれだれさんはいくらのビットコインを保有していると分かります。これは、銀行に預けているお金の額をみんなが見れることと同じです。これだと、すぐに泥棒に狙われます。ですから、匿名でビットコインを保有しなければなりません。ビットコインでは、匿名をビットコインアドレスで表します。そのビットコインアドレスが、個人に紐づいています。ビットコインの取引時には、スマーフォフォンの仮想通貨アプリを操作することで、秘密鍵を生成し、秘密鍵から公開鍵を生成し、公開鍵からビットコインアドレスが生成されます。この内、秘密鍵と公開鍵は公開鍵暗号方式により生成されます。公開鍵暗号方式のよいところは、暗号化の鍵と復号化の鍵が異なることです。また、各人が鍵を自由に生成しても、天文学的組み合わせ数からダブルことはありません。

お金を受け取る側は、あらかじめ公開鍵をお金を送る側にメールで伝えます。メールで鍵を公

開
しても、それを知った人が受取人の秘密鍵を逆算することはできす心配無用です。お金を送る側は
、受取った公開鍵でビットコインアドレスを含めデータを暗号化します。受け取る側は、送られて
きたデータを秘密鍵で復号化して、初めてデータの検証ができるとともに、ビットコインアドレス
を頼りに送金を認識できます。ですから、ビットコインのファイルには個人名がなく、ビットコイ
ンアドレスが個人を結び付ける唯一の鍵です。

（２）　ハッシュ関数の活用によるデータ改ざんの防止

　ハッシュ関数は関数と言う名のとおり、可変長のデータを入力すると、ハッシュ関数で計算した
結果、固定長のデータが出力されます。しかし、出力データから入力データを復元できません。ま
た、入力データが一文字でも変わると出力データが代わります。このハッシュ関数の特性を活用し、
データ改ざん検知の仕組みを作ります。ビットコインシステムはハッシュ関数を多用し、データ改
ざんを防止しています。次にハッシュ関数の使用例を説明します。

　仮に、ひとつのブロックに４つのトランザクション（＝取引）が送られてきました。なお、取引
データのどの部分をハッシュ関数の入力にするかは省略します。すると、ハッシュ関数が取引ごと
にハッシュ値１からハッシュ値４を出力します。（図３参照）

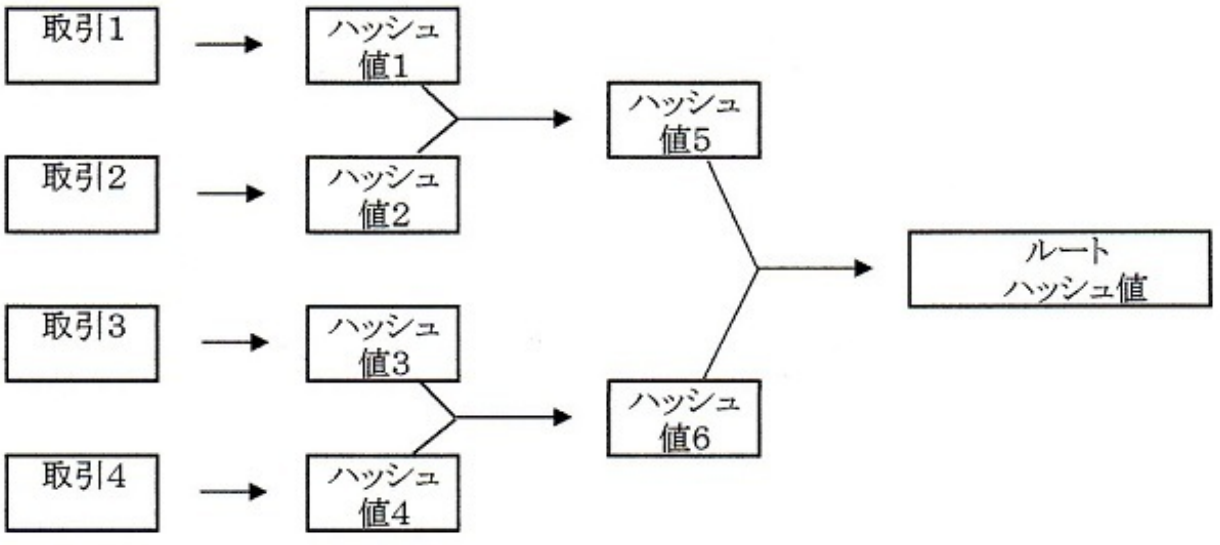


図３：ハッシュ関数の使用例

　更に、これを勝ち抜き戦のように結合して、どんどん上位のハッシュ値を作っていきます。具体
的には、２５６ビットのハッシュ値１と２５６ビットのハッシュ値２を結合し、５１２ビットの入
力データを作り、ハッシュ関数で変換するとハッシュ値５が得られます。その後、２５６ビットの
ハッシュ値３と２５６ビットのハッシュ値４を結合し、５１２ビットの入力データを作り、ハッシ
ュ関数で変換するとハッシュ値６が得られます。最後に、２５６ビットのハッシュ値５と２５６ビ
ットのハッシュ値６を結合し、５１２ビットの入力データを作り、ハッシュ関数で変換するとルー
トハッシュ値が得られます。
　このルートハッシュ値が、改ざん検知用データの片方です。改ざん検知用のもう片方データは、
あるノードがブロックを送信する前に、図３と同様の処理をしてからブロックヘッダのある場所に
埋め込みます。ブロックを受信した各ノードは、自分でルートハッシュ値を求め、受信したブロッ
クヘッダに埋め込まれているハッシュ値と比較します。一致すれば、改ざんのないデータとします
。この仕組みは、ブロックを受信したノードが改ざんしたくてもできない仕組みです。また、この
仕組みは、ノードの自立と連携によりデータの改ざんを防止しています。

（３）　ブロックの承認依頼と報酬
　図４は、ビットコインのブロックチェーンなる台帳です。ブロックチェーンなる意味は、各ブロ
ックの中に前のブロックのハッシュ値が、あたかもブロック毎の取引履歴を紐で綴ったように見え
ることから名付けています。
　ノードが、（２）の処理を終えると、次に図４のブロック３の処理に取り掛かります。この作成
処理がプルーフオブワーク（Ｐｒｏｏｆ　ｏｆ　Ｗｏｒｋ：略称ＰｏW）です。ＰｏWは、ナカモ

ト・サトシによって提唱された、仮想通貨取引のための合意形成アルゴリズムです。ＰｏＷは、ビ
ットコインで取引の 正当性 を保証する役割を担っています。マイナー（採鉱）ノードと呼ばれる一群の参加者が、ＰｏＷに勤しみます。ＰｏＷでは、次に説明する地道な計算に成功すれば報酬が
得られることから、あたかも金鉱山の採掘に似せマイニング（採掘）と呼ばれます。

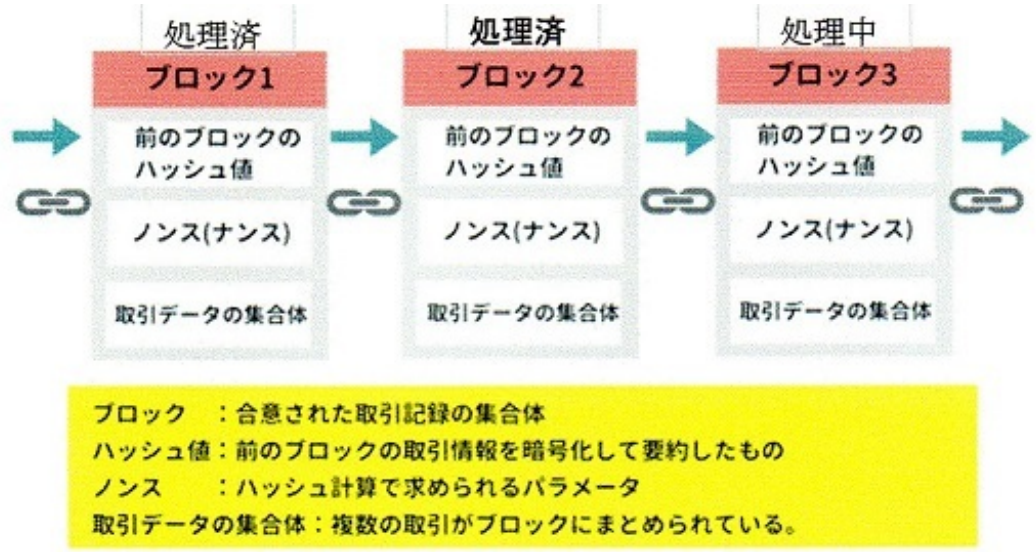


図４：電子情報で綴るブロックチェーン台帳
出典元：「ブロックチェーンの仕組みを図解」より（少し追記）

　マイナーノードの計算に先立ち、「ブロックの承認ができる難度」 がブロックで指定されています。例えば、ブロック３のある場所に２の２５５乗より小さくせよ（＝２の２２６乗より上の桁はゼロ）と指定されています。仮のノンスとその時の時刻をハッシュ関数に入力し、出力を得ます。
得た出力と 「ブロックの承認ができる難度」 を比べ、最初のｎビットが全てゼロで一致したか判定します。一度では一致せず、必要なゼロビットの桁数が見つかるまでノンスの値を変化させ、何度もＰｏＷを実行します。ＰｏＷが設計どおり約１０分で完了すると、ノードはブロックの承認依頼を他のノードに発信します。「ブロックの承認ができる難度」 を探したマイナーは、ブロックを閉じる権利を得たことになります。マイナーは、誰のアドレスのビットコインを減額することもなく、新しいビットコインをインターネット空間から湧き出すことができ、マイナー自身のアドレス

宛
てに送ることができます。ビットコインシステムは、そういう規則にしています。

（４）　台帳へのブロック追加

　ビットコインシステムは、ノードが台帳を管理します。そのノードは、世界中におおよそ１１
,
０００か所に点在します。大切なのは、各ノードの台帳を同じにすることです。あるノードが、
（３）の作業が完了すると他のノードにブロックの承認依頼をします。各ノードがブロックの承
認
をするとき、正統な共通の台帳にしなければなりません。ブロックの承認とは、当該ブロック（
図
４のブロック３）を直前のブロック（図４のブロック２）に接続することです。ビットコインシ
ス
テムは、バラバラなノードが承認の合意形成アルゴリズムに従い、共通の台帳に収れんします。
そ
の承認の合意形成アルゴリズムは、ブロックチェーンの長い方を正統と見做します。ですから、
ブ
ロックを接続する場合、ブロックチェーンの長い方のブロック５Ｂ側に接続します。（図５参照
）
　２本に分岐したブロックチェーンのうち、伸びた方が正統な台帳として扱われます。そして、
２
本に分岐した両方が共に伸び続けることはないそうです。実際は、１ブロックの分岐で勝負が決
す
ることが多いそうです。図５では、ブロック５Ｂが勝ち分岐が伸びました。大切なのはひとつの
分
岐だけが伸びることで、そうなれば、自ずと台帳が安定します。ブロックの承認の合意形成アル
ゴ
リズムにより、ブロックの分岐が生じても、少し待てば、全ノードは同じ台帳を持ちます。

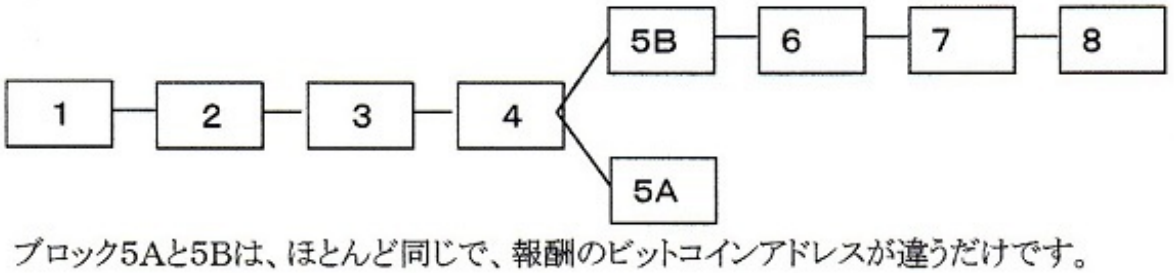


図５：ブロックの分岐

（５）　分散台帳のイメージ

取引データには、送る人と受け取り側の区別があるので、図６のように台帳に綴れます。つまり
、全ノードの分散台帳が、ブロック毎に取引データを綴ります。図６の台帳から、ＡさんはＢさん
に７．０ＢＴＣを送り、０．１ＢＴＣの手数料を支払い、自分から自分へ残り２．９ＢＴＣを送金
しました。ブロックチェーンでは、分散台帳の残高を更新することなく、常にブロック毎に取引デ
ータを綴ります。そのため、送る人のビットコインは、常に使用済みになります。その結果、分散
台帳の受け取り側の未使用分が残高になります。この追記型台帳方式は、電子情報のコピー防止の
一貫です。

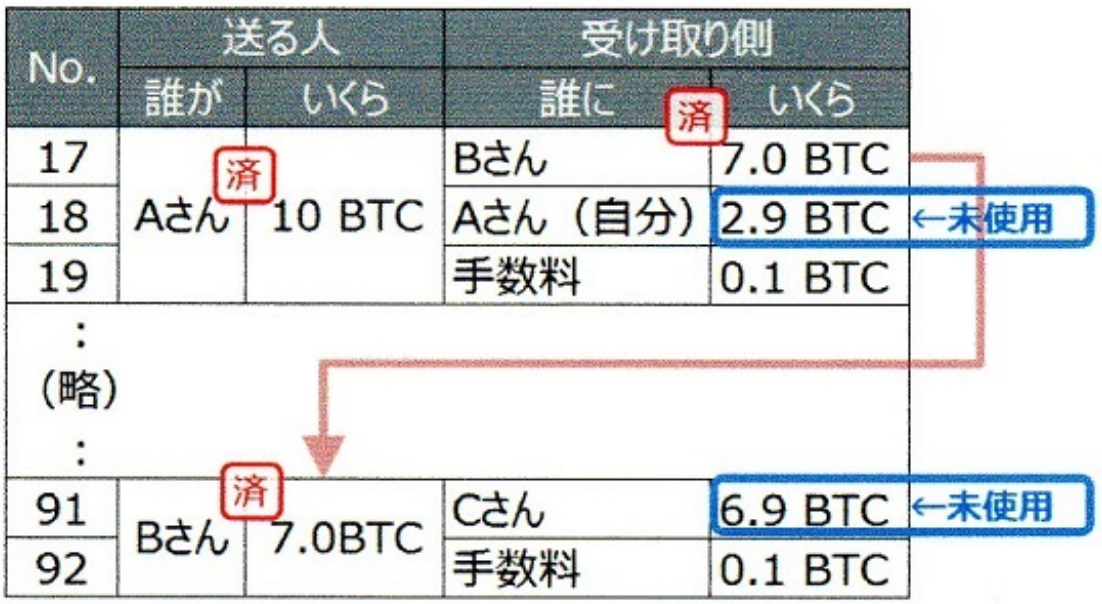


図６：分散台帳のイメージ

出典元：[完全版]　図解！わかりやすいブロックチェーン技術の仕組みより

イーサリアムとは

イーサリアム（Ｅｔｈｅｒｅｕｍ）は、２０１５年に開始されたブロックチェーン台帳が使える
非中央アプリケーションのためのオープンソースのプラットフォームです。ビットコインは、ブロ
ックチェーン台帳を使った最初の仮想通貨送金システムですが、イーサリアムはスマートコントラ
クトという仕組みを提供します。スマートコントラクトの説明に自動販売機が、よく例に挙げられ
ます。自動販売機に利用者がお金を投入し、商品を選択すると商品が出て来ます。スマートコント
ラクトは、オンライン上でさまざまなサービスを実現する仕組みです。具体的には、サービス提供
者が自動販売機に代わるサービス商品をソリディティ（Ｓｏｌｉｄｉｔｙ）というプログラミング
言語を使い開発し、イーサリアムのプラットフォームと連動させ、サービス商品を提供します。サ
ービス商品の売買では、仮想通貨（イーサー：Ｅｔｈｅｒ）を基軸通貨にします。また、プラット
フォーム使用料が、ガスなる単位で細かに決められており、サービス提供者がイーサーで支払いま
す。

ビットコインは、ノードがＰｏＷで報酬を得ていましたが、イーサリアムではノードがプラット
フォーム使用料をもらい受けます。イーサリアムのマイナーは、多くの手数料を支払ってくれるト
ランザクションから、優先的にマイニングするそうです。イーサリアムは、マイナーの合意形成ア
ルゴリズムが、ＰｏＷでないため膨大な電力を消費することはありません。

ピアコインとは

ピアコイン（Ｐｅｅｒｃｏｉｎ）は、サニーキング（ｓｕｎｎｙＫｉｎｇ）と呼ばれる開発集団
によって開発され、ＭＩＴのライセンスのもとで公開されたアルトコインです。ピアコインは、プ

ルーフオブワーク（ＰｏW）とプルーフオブステーク（ＰｏＳ）の併用でブロックチェーンの分散
型ネットワークを支えています。ビアコインは、ビットコインのルートハッシュ値を求める処理（
４章の仮想通貨を実現した仕組みを参照）のみＰｏWで行い、ブロック承認はＰｏＳで行います。
ビットコインとピアコインの違いは、ブロック承認の合意形成アルゴリズムと通貨発行量の上限有
無です。なお、ここでは通貨発行量の上限有無については割愛します。
　ピアコインのＰｏＳは、ノードがわずかな電力でブロックを接続します。これは、ピアコインな
る仮想通貨の所有者が、通貨をもつ割合に応じて、ブロックの接続を承認する方法です。ピアコイ
ンのＰｏＳは、コイン保有量が多く、また長く保有しているほど、マイニングがしやすくなるよう
に設計されています。年間で保有量の約１％が、ＰｏＳのブロック報酬として受け取れますが、最
低３０日以上コインを保有していなければ、ＰｏＳブロックのマイニングはできません。
　しかし、　ピアコインのＰｏＳにはブロック承認に固有の問題が潜んでいます。ビットコインと
同様、ほぼ同時にブロック５Ａと５Ｂが届きました。ノードは、ブロック５Ａと５Ｂのどちらかの
承認をせまられました。多くのノードに承認された方が、正統なブロックとして認められるのはビ
ットコインと同様です。しかし、マイニングするノードは格安コストで図７のように６Ａと６Ｂの
両ブロックを承認できます。なぜなら、一方が負けそうに思えても、念のためもう片方も承認して
おいた方が得だからです。そうすると、どちらの枝が伸びても報酬が得られます。ピアコインは、
枝分かれしたブロックチェーンになっても、あるいはノード間で台帳が不統一になっても、正常に
稼働するため外から問題になりません。この問題は、ビットコインのマイニングでは起こりません
。

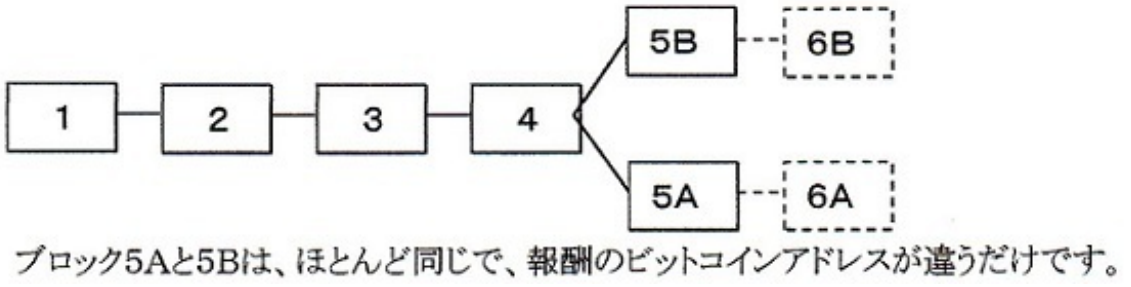


図７：ナッシング・アット・ステーク問題

リップルとは

リップル（ＸＲＰ）は、国際送金システム（スイフト：ＳＷＩＦＴ）にとって代わることを目指して、２０１２年運用開始のリップル社が開発した国際送金システム（注）です。ビットコインは、ブロックチェーンなる台帳を考案しましたが、リップルはリップル社独自のＸＲＰレンジャー（ＸＲＰＬｅｄｇｅｒ）と呼ぶ非ブロックチェーンの分散型台帳にしました。ＸＲＰレンジャーでは、リップル社が指定したバリデータ（Ｖａｌｉｄａｔｏｒ）と呼ばれるか所が、ビットコインのノードに相当し、バリデータがＰ２Ｐネットワークで結ばれています。リップルでは、バリデータがブロックチェーン台帳に代わるアドレスの状態や残高を示す、ＸＲＰレンジャーなる電子台帳を更新します。バリデータは、自分と隣接するバリデータの８割以上が自分と同じ判断をしているなら、取引データを承認します。つまり、周囲のほとんどが自分と同意見なら、自分の判断を確定させます。この仕組みをプルーフオブコンセンサス（ＰｏＣ）といいます。

ＰｏＣは多数決の原理であり、取引データの承認作業量が既存のブロックチェーンよりも少なくて済みます。しかし、リップル社の指定したバリデータが、取引の承認作業を行っており、リップル社による中央集権型システムです。

（注）　リップルシステムは、リップルなる仮想通貨を用意していますが、あくまでも従です。集権型システムです。海外送金を主目的にしており、日本円・米ドル・ビットコインやゴールド等の通貨やその他資産の取引をボーダレスに行います。

リブラとは

リブラ（Ｌｉｂｒａ）は、米国のフェースブック（Ｆａｃｅｂｏｏｋ）によって開発されたブロックチェーンベースの仮想通貨です。２０２０年に稼働する予定が、米国の金融当局の許可が得られる見通しが立たず、暗礁に乗り上げました。リブラは、米ドルを含む主要通貨４つをリブラの裏付けにすることで、仮想通貨の価格が安定化する仕組みにしています。ですから、システムが稼働すると、リブラは仮想通貨世界に留まらず法定通貨世界までの基軸通貨になりそうです。

リブラ協会の企画書では、リブラを発行する目的が世界の金融インフラを整えるためだそうです。リブラが目指すのは、スマートフォンの仮想通貨財布を使った決済や送金です。何しろ、交流サイトを運営してるフェースブック主導ですから、仮想通貨の財布はお手の物です。リブラは、スマートフォンを個人の銀行、あるいは仮想ＡＴＭに見立て、交流サイトのノウハウを生かし、キャッシュレス社会の世界銀行を目論んでいます。リブラは、ビットコインと似て非なる壮大な中央集権型システムです。しかし、世界の中央銀行が巨大ＩＴ企業に基軸通貨になりそうなリブラの発行を許可するとは思えません。

ブロックチェーンの革新性

銀行の勘定系システムの台帳を残高更新型から、ブロックチェーンの追記型に換えても、従来の中央集権型システムは稼働できます。さすれば、ナカモト・サトシが問題にしている二重支払い問題は解消しますが、数秒で処理が終わりません。銀行とかカード会社の決済処理は、処理時間を極限まで短縮し、大量のトランザクションを処理しています。ですから、処理時間の長いＰｏＷの合意形成アルゴリズムを除いても、ブロックチェーン台帳は大量のトランザクション処理に不向きです。

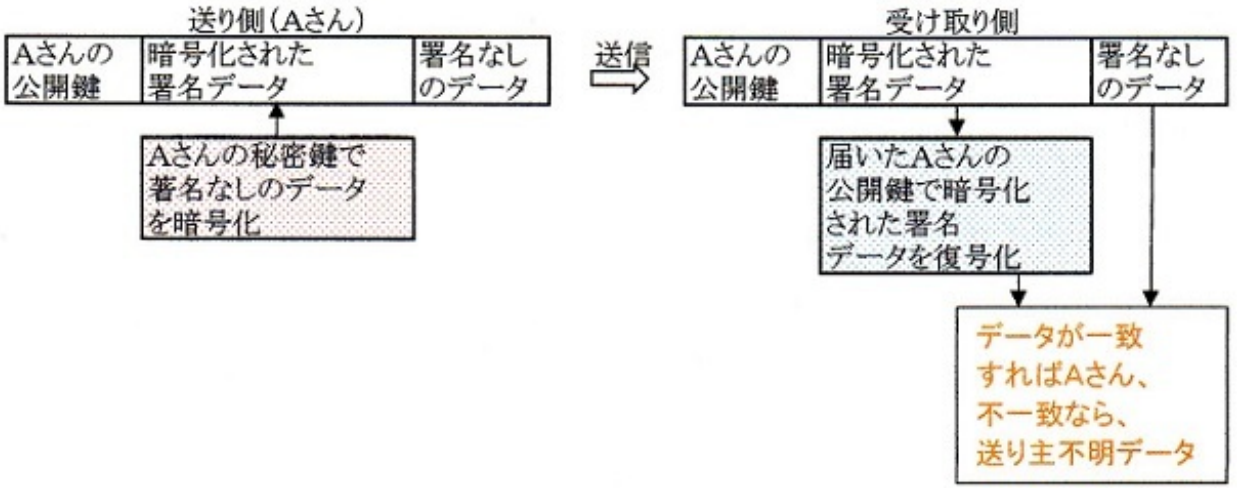
ブロックチェーン台帳の長所は、取引履歴を時間順に積み重ね、そしてそれを書き換えできない形で記録します。分散型処理において、ノードが取引を電子署名（注）で公正か確認した後、過去の取引履歴と突き合わせ、合意形成された取引のみ綴り、その取引履歴はすべて公開された状態にします。従ってブロックチェーン台帳は、分散型処理においてこそ長所を発揮します。しかも、分散型処理はノード連携が欠かせず、合意形成アルゴリズムが中央集権型システムにない機能です。

ブロックチェーン台帳を採用する分散型処理は、合意形成アルゴリズムに見られるようにひとつの社会づくりです。人間集団においては悪意を有する人が混じりますが、ノードには悪意を有する人が参入するところは一緒です。分散型処理では、ノードが担う機能と分散型処理を支える人間集団の役割を切り分けた事前の制度設計が欠かせません。ブロックチェーンの革新性は、分散型処理に適した台帳技術に加え、社会づくりをもとめていることにあります。

(注)　電子署名の仕組み

公開鍵暗号方式では、秘密鍵で暗号化したデータは、公開鍵でしか復号できない仕組みです。受

け取り側で、Ａさんの公開鍵で復号化したデータと署名なしのデータが一致すれば、Ａさんからの
データであることの証明になることから電子署名と呼ばれています。



巨大ＩＴ企業のコンピュータ利用

１９９５年以降、パソコンの普及がさまざまな仕事を変革しました。パソコンが、経理のような
マニュアル化しやすい「ミドルスキル」の仕事がパソコンにとって代わられました。これにより、
中流社会を構成していた職業はマニュアル化できない「ハイスキル」の仕事（研究者や高度な技術を有する技師など）と低賃金の単純作業である「ロースキル」のふたつの仕事に分極化しました。更に、政府は外国人労働者の雇い入れ、ホワイトカラーエグゼプションなる残業無制限など大
企業の人件費削減のための法案を無理やり国会を通しました。その結果、日本はもとより世界中で
中流社会は崩壊し経済格差が拡大しました。世界中で進行するＩＴ革命は、人間を競争の厳しい仕
事環境に追いやります。「ハイスキル」のポストが増えない中、「ハイスキル」のポスト獲得競争に敗れた多くの人は、「ロースキル」の仕事に甘んじざるをえません。仕事の分極化及び非正規雇用が、経済格差を進展しました。

ＧＡＦＡ（注：ガーファ）と呼ばれる巨大企業は、ＩＴ技術を活用し、世界規模の商機を見いだし、巨額の利益を上げています。ＩＴ技術を活用したグローバル市場では、巨大企業へ情報と人と金が一手に集まる経済現象に恵まれます。ＩＴ技術を使えば、人を増やさずに、新規にグローバル市場が開拓でき、巨額の利益が得られます。米国のフェースブックが、仮想通貨リブラを開発したのは、キャッシュレス社会の世界銀行を狙っています。リブラなる仮想通貨の秘めたる狙いに、Ｇ２０はおそれおののき、実施を中止させました。

お金は、１円・２円と数えます。コンピュータはアナログ処理よりデジタル処理が得意です。分
散型処理に別名デジタル通貨なるビットコインが、最初に登場したのもお金とコンピュータの相性
の良さの例証です。そもそも会社組織は、中央集権型のピラミッド構造になっており、コンピュー
タの処理形態も中央集権型システムで発展してきました。巨大ＩＴ企業が目指す利益独り占めに、
中央集権型組織と中央集権型処理が似合います。ビットコインのような分散処理は、きわめて異例
です。ビットコインの構想には、中央集権の権力から独立した通貨への願望が底流にあります。

（注）ＧＡＦＡ（ガーファ）とは、 グーグル(Google）、アップル(Apple)、フェースブック(Facebook)、アマゾン(Amazon)の４社のこと。 頭文字を取ってＧＡＦＡと称される。いずれも米国を代表する巨大IT企業であり、4社は世界時価総額ランキングの上位を占めている。

共存共栄のコンピュータ利用

近江商人の心得は、三方よしの 「売り手よし、買い手よし、世間よし」 です。その近江商人は、
江戸時代から明治時代にわたって日本各地で活躍しました。翻って、グローバル資本主義における
巨大ＩＴ企業の心得は、三方よしに代わる自分だけの 「株主よし」 です。グローバル資本主義では、会社での主たる仕事が株主様のお金儲けの手伝いです。江戸時代は、大名による分権統治でしたが、現在は国民国家です。その国民国家の市場は、自由貿易なる美名でグローバルに統合されました。グローバリズムは、国民国家の市場をグローバルに統合したが、国民国家の社会をバラバラにしました。

ビットコインで分かるようにお金とコンピュータの相性は抜群で、世界中の大手金融機関が抱えている巨額の丁半博打の金融派生商品（＝デリバティブ商品）は、コンピュータがなければ組成できません。自由貿易を旗印にするグローバリズムは、金融派生商品を生んだ巨大な国際金融資本以外に、利益独り占めの巨大ＩＴ企業を生みました。巨大ＩＴ企業は、グローバリズムの申し子で

あ
り、経済的影響力は国をも凌駕します。経営者の方向感は、グローバル市場での独占です。そのた
め、巨大ＩＴ企業は、ＩＴ技術を商売のタネにし、かつ、効率的ピラミッド組織にも邁進します。
グローバリズムの経済の力学が、上から下へ放射状に働き社会をバラバラにしますが、水平に働く
のは共存共栄のシステムです。
　中央集権型システムに活用していたＩＴ技術が、ビットコインによって、分散型システムにも使
えることが例証されました。分散型システムには、共存共栄の考えが底流にあります。近江商人は
、民による「三方よし」の共存共栄を実現しました。ですから、共存共栄の理念は荒唐無稽ではありません。我々は、地球全体を覆う持続性の暗雲から文明の転換期を感じます。グローバリズム
型中央主権の考えに立脚していては、国際社会のあり方、社会・経済の価値観がいずれ立ち行かな
くなります。ビットコインの作動原理は、社会づくりを考えたうえの民による分散型処理システム
であり、ブロックチェーン技術を共存共栄の作動システムに応用できます。ビットコインシステム
では、幸いにもお金以外の情報がブロックチェーン台帳で取り扱えます。幅広い共存共栄の市場に
することが、グローバリズムの悪影響に打ち勝つ方策です。
　たとえば、フマートフォンから選挙の投票をし、ブロックチェーン台帳に投票結果を保存すれば
どうでしょうか。この方法には、多くの長所があると思われます。

あとがき

　ビットコインを評価する多くの人は、ブロックチェーン技術を挙げます。そのブロックチェーン
技術は、従来の中央集権型システムと相性が悪いです。しかし、ブロックチェーン技術が分散型処
理に適していることを当たり前と考えており、ブロックチェーン技術と分散型処理の統合的視点が
ありません。まして、ブロックチェーン技術がマイニングや合意形成アルゴリズムなどの論理から
、社会づくりをもとめていることを指摘する人はおりません。
　グローバリズムに染まったグローバル資本主義は、経済の力学が上から下へ放射状に働き、社会
をバラバラにしました。ビットコインの作動原理は、社会づくりを考えたうえの民による分散型処
理システムです。ビットコインには、共存共栄の考えが底流にあります。グローバリズムの経済の
力学と似て非なる力学が、ビットコインの水平力学です。今後は、ブロックチェーン技術と分散型
処理を組み合わせた、革新的サービスの起業が望まれます。非常に困難な課題ですが、共存共栄の
システムこそ西欧発祥の資本主義に代わる新たな社会組織になります。

参考文献

第１章 従来のコンピュータシステム

なし

第２章 ビットコインのシステム

- サトシ・ナカモト著　ビットコイン：　Ｐ２Ｐ　電子通貨システム（翻訳版）　ｂｉｔｃｏｉｎ．ｏｒｇ
- 坂井豊貴著　　暗号通貨ＶＳ．国家　　ＳＢクリエイティブ株式会社
- 石黒尚久　河除光瑠著　　ブロックチェーンがよ～くわかる本　　秀和システム

第３章 ビットコインシステムの革新性

- 坂井豊貴著　　暗号通貨ＶＳ．国家　　ＳＢクリエイティブ株式会社
- 石黒尚久　河除光瑠著　　ブロックチェーンがよ～くわかる本　　秀和システム

第４章 ビットコインシステムの仕組み

- サトシ・ナカモト著　ビットコイン：　Ｐ２Ｐ　電子通貨システム（翻訳版）　ｂｉｔｃｏｉｎ．ｏｒｇ
- 坂井豊貴著　　暗号通貨ＶＳ．国家　　ＳＢクリエイティブ株式会社
- 石黒尚久　河除光瑠著　　ブロックチェーンがよ～くわかる本　　秀和システム

第５章 ビットコインに触発されたシステム

- 坂井豊貴著　　暗号通貨ＶＳ．国家　　ＳＢクリエイティブ株式会社
- 石黒尚久　河除光瑠著　　ブロックチェーンがよ～くわかる本　　秀和システム

第６章 ブロックチェーンから考えるシステム

- 坂井豊貴著　　暗号通貨ＶＳ．国家　　ＳＢクリエイティブ株式会社
- 石黒尚久　河除光瑠著　　ブロックチェーンがよ～くわかる本　　秀和システム