【ＤＲニュース・029】：ブロックチェーン技術の特徴～ビットコインと分散型台帳管理

2017 年 02 月 13 日発信

金融業界で今話題のブロックチェーン技術とは？ ・・・ 金融業界に革命を起こすといわれています。

ブロックチェーンとは、“暗号技術”と“P2P（ピア・ツー・ピア）ネットワーク技術”を応用した分散型の記録管理技術であり、仮想通貨「ビットコイン」の基幹技術としても知られています。

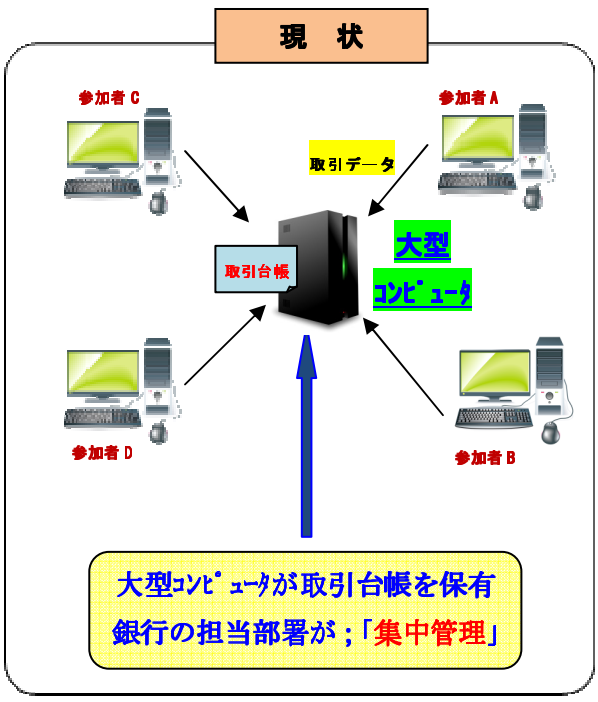
今回のテーマは、金融と情報技術を融合させた新サービス「フィンテック（FinTech）」。
・・・そのキーテクノロジーとされている「ブロックチェーン」について、調べて見ました。

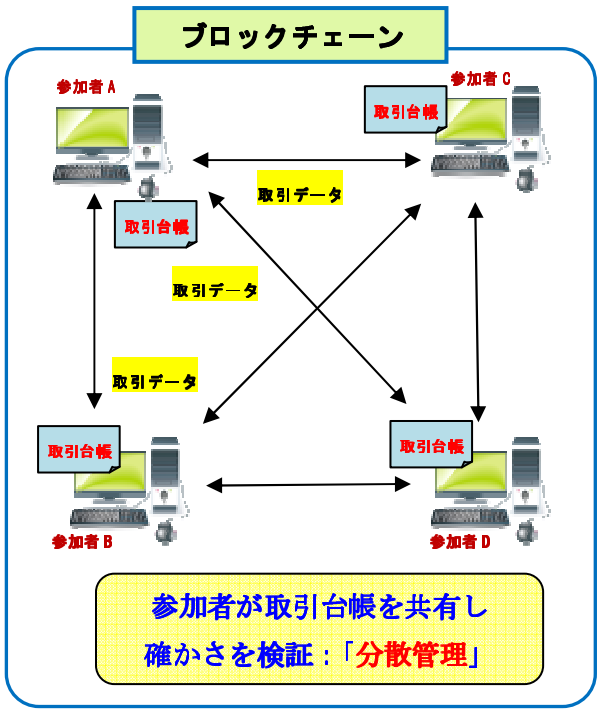
⇒ ブロックチェーンの管理技術は、「次の新しいインターネットの基盤」になるのだろうか？

1．ブロックチェーン

現行の金融機関は、銀行を通るすべての金融取引のデータを行内の大型コンピュータで取引台帳（勘定元帳：口座＆取引情報）を管理しているため、システムの投資に多額の費用が掛かっています。

今後は、複数の小型コンピュータのネットワーク上に、改ざんされにくい「取引記録の台帳」を安く構築できる「ブロックチェーン」と呼ばれる新技術を活用して、大型コンピュータを介する必要がなくなるため、システムの投資を大幅に抑えられるという。





（1） ブロックチェーン技術の特徴

ブロックチェーンには、「改ざんができない」「データが消えない」「停止しない（ゼロダウンタイム）」といった特徴があり、信用を重んじる金融機関からの人気を集めています。

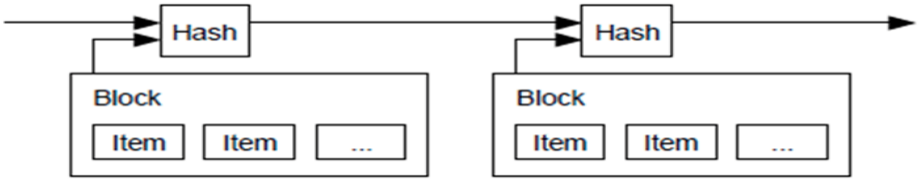
また、システムコストを抑えるという２次的なメリットもあり、銀行の勘定系システムや送金システム、証券取引システム、不動産の登記・閲覧システム、契約管理システムなど、今ではフィンテックだけでなく幅広い分野で応用が期待されています。

① データ構造自体に優れた改ざん耐性を装備

- ブロックチェーンでは、ネットワーク内で発生した取引の記録を「**ブロック；Block**」と呼ばれる「**記録の塊**」に格納します。
- 個々のブロックには、「**取引の記録**」に加えて、１つ前に生成されたブロックの内容を示す「**ハッシュ値；Hash**」と呼ばれる情報などを格納します。
- 生成されたブロックが、時系列に沿ってつながっていくデータ構造が、まさにブロックチェーンと呼ばれる理由です。
- もし仮に、過去に生成したブロック内の情報を改ざんしようと試みた場合、変更したブロックから算出されるハッシュ値は以前と異なることから、後続するすべてのブロックのハッシュ値も変更しなければならず、そうした変更は事実上困難なことです。

※１；ハッシュ値（Hash）を用いたブロックのチェーン

前のブロック（Block）のハッシュ値と、新しい Block の中の**取引（Item）**を用いて、**新しいハッシュ値を計算**します。



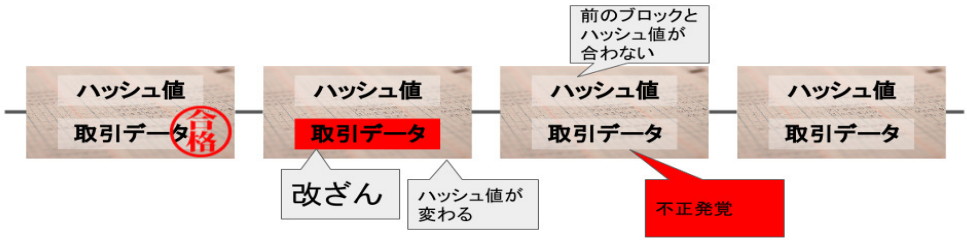
ハッシュ値とは、元になるデータから一定の計算手順により求められた、規則性のない固定長の値。その性質から暗号や認証、データ構造などに応用され、ハッシュ値を求めるための計算手順のことをハッシュ関数、要約関数、メッセージダイジェスト関数などという。

※　ハッシュ関数変換ツールがフリーソフトで提供されているので、算出してみると！

変換前文字数	SHA-256 ハッシュ　（少しでも変換前文字が異なるとハッシュ値も異なる）
DRTECH	0000000000000000000005e404b075c4ba74f3f66488c6824be0
DRTECH1	00000000000000000000000374b5ecc667945f959dd4f346bea6

（ハッシュ値が大きいほど良いとされ、以前は MD5 が使われていたが、SHA1→**SHA2** への移行が推奨）

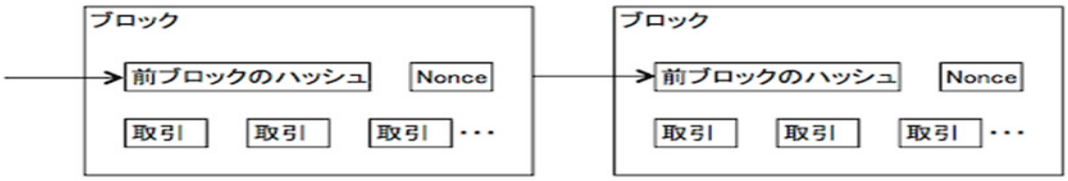
ハッシュ値は元のデータの長さによらず一定の長さとなっており、同じデータからは必ず同じハッシュ値が得られる一方、少しでも異なるデータからはまったく異なるハッシュ値が得られる。不可逆で情報量の欠損を含む計算過程を経るため、ハッシュ値から元のデータを復元することはできない。



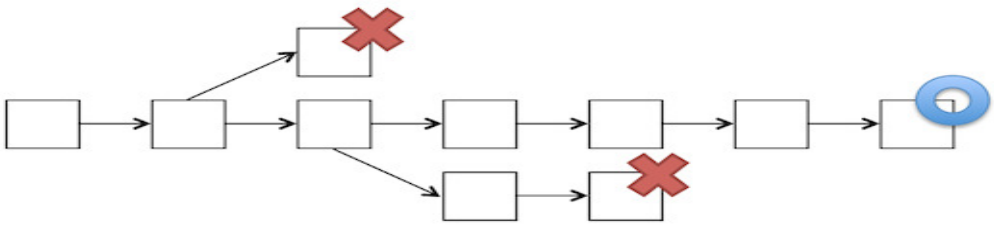
ハッシュ値とはアルゴリズム（**ハッシュ計算**）により算出された一定量の情報をコンパクトにまとめるデータのことで、情報が少しでも変更（改ざん）されると、計算されるハッシュ値は全く異なるものになります。ハッシュ値が合わないと不正があったものと扱う。

・・・ **ブロックチェーンの最大の特徴は「データの改ざんが極めて困難なこと」です。**

※２；プルーフ・オブ・ワーフ（Proof of Work）と呼ぶ仕様を採用



ブロックチェーンは、いくつかのトランザクションをまとめて「ブロック」として、ブロック単位で整合性を検証し、検証済みのブロックを直列に連鎖（チェーン）させたもので、新しいブロックを完成させるためには、未検証のトランザクションを集めて、それらの整合性を検証したうえで、ブロックのハッシュ値を計算します。新しいブロックには、直前のブロックのハッシュ値を持たせます。これによりブロックチェーンが形成されます。
（ブロック生成者は、ハッシュ値が規定の条件を満たすまで、Nonce の値を変えてトライします）



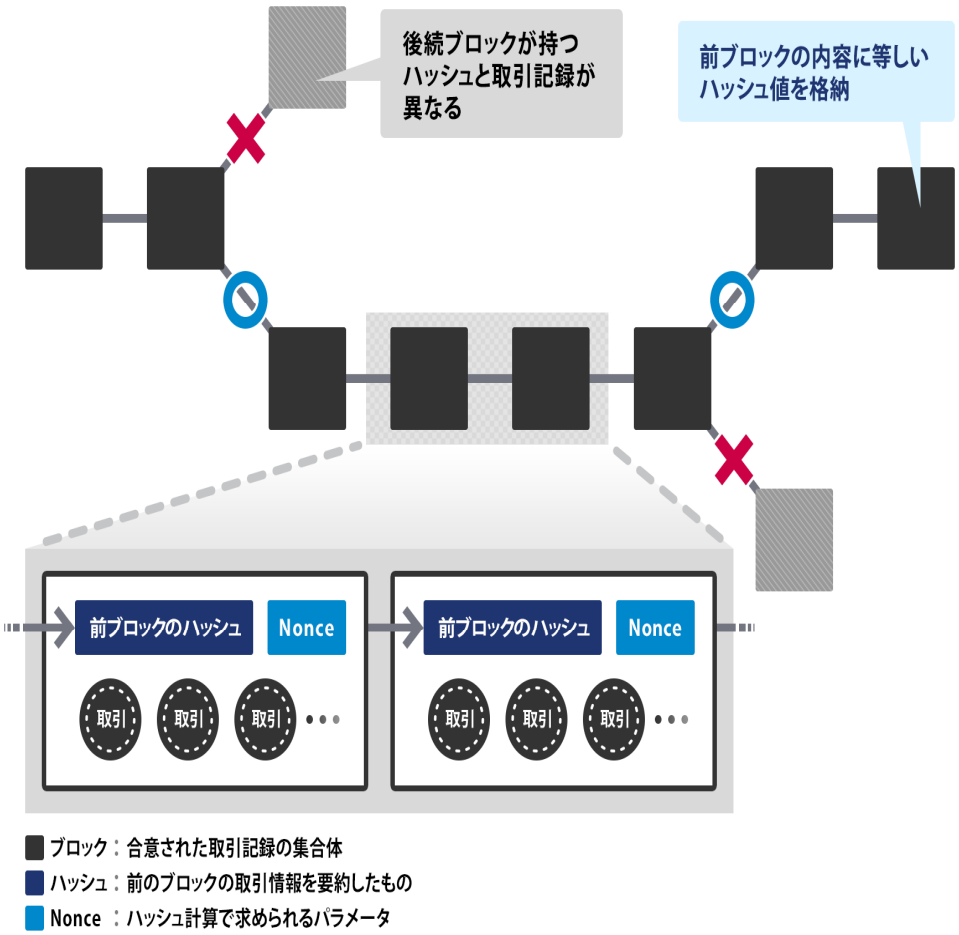
ブロック生成の試みは多数のノードによって行われる為、複数の異なるブロックチェーンが出来てしまいます。その場合、長いチェーンが正として受け入れられ短いチェーンは破棄される。この仕様は「コンフリクト（異なる観点から複数の視点や見識を取り込む。合意と確約につながる）の解決手段」であるとともに不正防止にもなっています。

・・・**ビットコイン**で使われる**プルーフ・オブ・ワーフ（Ｐｏ Ｗ）**とは、仕事量によってビットコインのセキュリティーの保護を担うシステムのことです。仕事量は計算量と置き換えても構いません。

ビットコインの取引単位をブロックと言います。通常、このブロックには送金額や送信者自身の取引情報などが含まれていますが、そのほかにも「**nonce（ノンス）**」と言う使い捨ての**ランダム変数**が含まれています。**この使い捨ての**ランダム変数、nonce **こそ、プルーフ・オブ・ワークの説明には欠かせないものです**。

たとえば送金リクエストがあると、それを受け取る役目の別の参加者（ノードと言う）に送金データが送られるようになっています。そこでは、この送金リクエストが間違っていないかを**検証**できるようになっています。次はこのリクエストが正しいデータとして正式に支払い済みと採用されるため、ビットコインのネットワーク上のすべて参加者（ノード）に競争させるわけです。この競争が**マイニング**（**採掘**）なのはご存知の方も多いと思います。この時の計算に使われるのが、先ほども出てきた nonce という使い捨ての**ランダム変数**です。

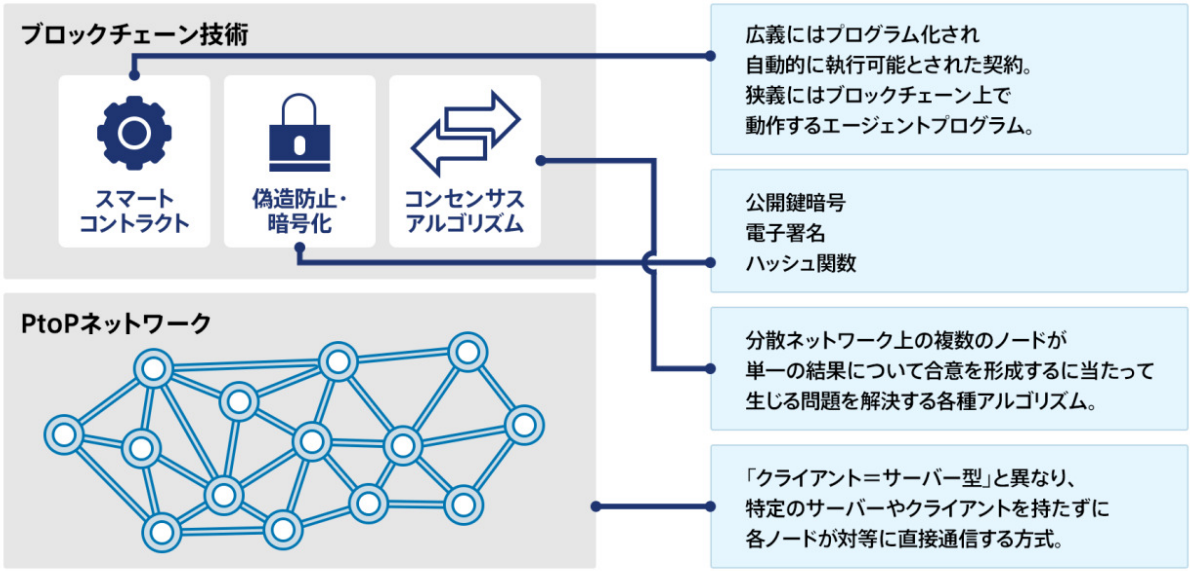
・・・　**プルーフ・オブ・ワークは、ブロックチェーンの改ざんを極めて困難にします。**



② ブロックチェーンを支えるさまざまな技術

■ ブロックチェーンはデータ構造に加えて、データの管理方法にも改ざんを防ぐ仕組みを備えています。「**分散型の台帳**」と言われますが、ブロックチェーンはネットワーク内で発生した全ての取引を記録する「**台帳**」としての役割を持ち、ネットワークに参加している全てのユーザーが同一の「**台帳**」を共有することで、情報の信ぴょう性を確保しています。

■ そのほか、ブロックチェーンは「**P2P ネットワーク**」や「**コンセンサスアルゴリズム**」「**スマートコントラクト**」「**偽造防止・暗号化技術**」といった複数の技術の組み合わせで実現されています。



※１：分散型の台帳管理を支える「P2P ネットワーク」

● ブロックチェーンのデータ管理の役割を担うのが、P2P ネットワークです。クライアント＝サーバー型とは異なり、特定のサーバーやクライアントを持たずにノードと呼ばれる各端末が対等に直接通信することで、ユーザー同士の情報共有や決済のやりとりを可能にします。

● 既存の決済システムのようにサーバー側で情報を集約して管理する場合には、そこが障害時の弱点（単一障害点）となりますが、ブロックチェーンの場合にはユーザー全員が同じ情報を持っているため、複数のノードに障害が発生してもシステムを維持できます。

● P2P とは、ネットワーク上で対等な関係にある端末間を相互に直接接続し、データを送受信する通信方式。また、そのような方式を用いて通信するソフトウェアやシステムの総称。データの送り手と受け手が分かれているクライアントサーバ方式などと対比される用語で、利用者間を直接つないで音声やファイルを交換するシステムなどが実用化されています。

- P2P 方式のシステムには、扱うデータの種類や利用者の参加の仕方により様々な種類がある。特定の利用者間をつないで 1 対 1 で音声通話やメッセージの送受信を行うインスタントメッセンジャーやインターネット電話、利用者がバケツリレー式に別の利用者にデータのコピーを送信するインターネット放送システム、不特定多数の利用者を匿名でつないでお互いにファイルを交換し合うファイル共有ソフトなどが有名な応用例である。
  ・・・単に P2P と言った場合は最後のファイル共有ソフトのことを指す場合が多いです。

※２；契約の自動化を実現する「スマートコントラクト」

- 契約行動をプログラム化し、自動的に実行しようとする仕組みが「スマートコントラクト」です。ブロックチェーン上で動くエージェント・プログラムで、特定の条件を満たした場合に契約を行うなど、さまざまな業務処理を記述することが可能です。
  ・・・実現性の程度はブロックチェーンの基盤によります。

※３；全体の合意形成で正当性を確認する「コンセンサスアルゴリズム」

- 中央集権的な管理者を持たないブロックチェーンでは、台帳情報をネットワーク上の全員で共有するため、全体の合意形成を行います。

- そうした合意を行う方法が「コンセンサスアルゴリズム」です。コンセンサスアルゴリズムには、ビットコイン等に用いられる Proof of Work（PoW）や Hyperledger Fabric 等に用いられる Byzantine Fault Tolerance（PBFT）など複数の方法があります。

※４；「偽造防止・暗号化技術」

- ブロックチェーンでは、「**公開鍵暗号技術**」により電子署名を用いて相手との安全な取引を実現したり、台帳情報の共有による取引の透明性とプライバシー保護を両立したりしています。

ブロックチェーンは、P2P 上の電子マネー決済システムである「ビットコイン」の基幹技術として発明された概念です。また、ブロックチェーンは、ネットワーク内で発生した全トランザクションを記録する「台帳」としての役割を持ち、それは参加している全てのノードで同一のものが保有されます。

◆ **「データの巨大化が懸念？」**；すべての取引をすべての参加者のコンピュータで管理します。
ブロックチェーンの巨大化とネットワークやコンピュータの高速化・大容量化の競争・激化します。

◆ **「データの照合・更新？」**；取引のたびに送信・照合・更新されるデータが大きくなるシステムは、あまり行儀の良いシステムと言えません。何れは、どこかに無理が生じてきます。

◆ **「参加者のデータ整合性・同期は？」**；一部のコンピュータが破壊されただけでは、複製しながら復旧することができます。途中から参加者の「台帳」の整合性をどうするのか？同期は時間かかりすぎ？

⇒ **ブロックチェーンの技術は、万能ではないため、特性を理解し、適用領域を考えていく必要がある。**

2．ビットコイン（Bitcoin）とは？

ビットコインを実現するために誕生したのが、ブロックチェーンの技術となります。

（1） ビットコインとは仮想の通貨

- **ビットコインとは何か**、ひとことで言えば「**仮想」の「通貨**」です。まず、「通貨」ということからも、「コイン」ということからも分かる通り、ビットコインはお金です。円やドルというように、「お金」であることには変わりありません。「お金」なので、**通貨の単位が存在します**。

- ビットコインの単位は、**BTC（ビーティーシー）** と表記されます。1 円や 1 ドルのように、**1BTC（1 ビットコイン）**と、数えることができます。しかし、「仮想」ということから分かる通り、円やドルとは違って、手にとって目に見える姿形が存在しません。

- 仮想通貨としてイメージしやすいのは、オンラインゲーム内の通貨です。円やドルを支払って、ゲーム内で使われている通貨を手に入れれば、そのゲーム内で使われている通貨が「使える」ゲーム内のお店で、アイテムを買うことができます。ゲーム内でのみ使える、仮想の通貨です。

- ビットコインも似ています。ビットコインを手に入れることができれば、ビットコインが「使える」所で物やサービスを買うことができます。

（2） ビットコインは何が違うのか

- 先の例で紹介したような**仮想通貨とビットコインは、何が違うのでしょうか**。
  ・・・・・・ **実は、存在している理由が全く違うのです**。

- 特定のゲームや Web サイト内でのみ使える仮想通貨は、企業単位で作られており、利用者を囲い込むことによって仮想通貨の運営主体（＝ゲームや Web サイトの運営会社）が利益を上げることを目標としています。

- 一方のビットコインは、国家単位で運営されている円やドルと同じく、経済活動を円滑に進めるために作られた仮想通貨なのです。ビットコインは、世界中で日常生活に「使える」ようにすることを目指して作られています。仮想の通貨なので紙幣や硬貨は存在しませんが、代わりにパソコンやスマートフォンをお財布代わりにして、物の売買が実現できるようにつくられています。

- まだまだ発展途上ではありますが、円やドル以上に利便性が高く、安定し、**世界中で利用できる次世代の通貨をめざして作られた仮想通貨なのです**。

（３） ビットコインと電子マネー

- **仮想通貨と似たような概念として、電子マネーというものが存在します**。ビットコインを説明する上でよく登場する言葉です。**これらを混同していると理解の妨げになりますので、整理しておきます。**

- **電子マネーとは**、紙幣や硬貨を使わないで、電子的に（＝データのやりとりで）決済を実現する手段の事です。オンラインで決済を実行するタイプもあれば、最近主力になりつつある非接触型の決済方法もあります。電車に乗るときや、コンビニでの支払いに利用するものです。すでに日常生活に浸透しつつあるしくみですので、多くの方が実際に利用したことのあるものだと思います。小銭を財布から出す手間もかからず、非常に便利です。（Suica,PASMO～等々）

- **ビットコインも、電子マネーとして使える特徴を持っています**。そもそもビットコインは紙幣や硬貨が存在しない仮想通貨なので、電子マネーとして使えるのは当然のことです。

（４） ではビットコインは電子マネーなのか

- 現在一般的に利用されている**電子マネーは**、基本的にはその地域で使われている通貨を使って電子的に決済を行うために存在しています。

- 日本国内の例であれば、円での支払いをより便利にするために、円の紙幣や硬貨の代わりとして電子マネーが活躍します。そのため、利用者は所有する円を電子マネーの端末に入金したり、あるいは電子マネーでの支払いの際に利用される銀行口座にお金を入れておくことになります。

- 紙幣や硬貨を利用せず、電子的に決済を実現していますが、実態としては円という通貨をやりとりしていることには変わりありません。ビットコインは、何らかの端末に円をチャージするというものではありません。

- ビットコインを利用して商品を購入する際には、まず手持ちの円という通貨をビットコインという通貨に両替しなくてはなりません。円をビットコインに両替してはじめて、ビットコインでの支払いが実行できるのです。両替をしたその後の支払いの流れは、一般的な電子マネーと同様です。

- ビットコインでの支払いを受け付けているお店で、電子的にビットコインでの決済を実行すると、自分の所有しているビットコインが減り、お店が所有しているビットコインが増えます。

- ビットコインは、円やドルと違って仮想ではありますが、通貨です。電子マネーとは、貨幣を使わないで決済できるようにするしくみのことです。**仮想通貨＝電子マネー、ではありません**。

（５） ビットコインを使うメリット

■ 国家や企業が関与していないので、例えば個人間の送金においては、次のようなメリットが存在します。

A) 個人間で文字通り「直接」送金できる

一般的な通貨で送金を行う際には、銀行などを仲介する必要があります。しかし、ビットコインの場合には、個人間が直接支払うことができます。メリットとして、直接会って財布からお金を出して支払うのと同じように、ビットコインを使えば直接相手にお金を支払うことができるのです。

B) 手数料が無料か格安

仲介する組織が存在しないので、基本的には手数料を払う必要がありません。これは個人間の少額な支払いにおいては、非常に重要な特徴です。銀行送金でも、クレジットカード支払いでも、一定の手数料が存在します。そのため、少額の商品の売買が難しくなったり、ビジネスの利益率が下がったりします。

ビットコインは、その最大のメリットとも言える直接送金のしくみのおかげで、従来の手数料の概念を覆した決済を実現するのです。

C) 監視や制限が存在しない

ビットコインでの決済は銀行を経由した決済では無いので、煩わしい手続きや制限が存在しません。お金の流通が、より自由に行えるようになります。

また国によって通貨の単位が異なるといった特徴もありませんので、ビットコインを使えば、世界中で同じ通貨が利用できるというメリットがあります。

そのためにはもっとビットコインが広まって、ビットコインでの支払いを受け付けるお店が増える必要がありますが、いまでもすでにビットコインでの決済が可能なお店は世界中に存在します。

（６） ビットコインは、どこに保存されているのか

■ ビットコインには、**ウォレット（財布）**という概念があります。これは、円やドルの例で言えば、銀行口座にあたるものです。ビットコインを利用するすべての人はウォレットを持ち、そこにビットコインを保存し、決済に利用します。つまり、ビットコインを使いたい人は全員、ウォレットを作成する必要があります。

■ 個人に割り振られるメールアドレスのようなものです。実際には、長い文字列でウォレット ID が表現されます。そのままでは覚えにくいため、個人間送金が難しくなります。

そこで、一般的には ID を短縮したコードを用いたり、スマートフォンで読み取れる QR コードに変換したりして、交換します。

・・・ **「ウオレット ID やパスワード」などの本人確認コードなどを管理しているデータ情報は、そもそも、どこで管理（集中管理なのか？/分散管理なのか？）されているのだろうか？**

（7） ビットコインの課題

- もちろん、円やドルでの決済がそうであるように、ビットコインでの決済でも、双方がビットコインによる支払いを受け付けている事が必須となります。**ビットコインという通貨が「通じる」間柄でなければ、決済はできないのです**。

- 円やドルと違ってまだまだ普及の初期段階にあるビットコインにおいて、**これは非常に大きな課題です。**

（8） ビットコインで何ができるのか

- ビットコインでできる事は、通常の通貨と同じです。ビットコインを用いれば、個人間、企業間を問わず、物やサービスの対価として支払いを実行できます。つまり、ビットコインは仮想であるというだけで、通常の通貨と同じように使えるお金の一種だと言えます。

- 円やドルのような通貨と違う事としては、ビットコインでの支払いは、電子的に行う必要があるという事です。現物の紙幣や硬貨がない仮想通貨なので、当然の事です。

- ビットコインでは電子的に決済を行うため、インターネット経由で送金することが容易にできます。遠く離れた相手、あるいは目の前にいる人に短時間でビットコインを送金できるのです。

（9） ビットコインは誰が管理しているの？

- ビットコインは、他の通貨と比較して何が決定的に違うのでしょうか。最大の違いは、通貨を管理する「中央銀行」が存在しない、ということです。ビットコインには、発行を司る組織や流通を管理する組織が存在しないのです。

- ビットコインは、国家や企業が運営している仮想通貨ではありません。円やドルと同じような通貨なのに、どこの国も、企業も、ビットコインの発行・流通には関与していないのです。この非常識の概念が、ビットコインの最大の特徴です。

- ビットコインは、中央での管理を行わない代わりに、コンピューターのネットワークを利用して通貨を管理する仕組みとなっています。

- ビットコインにおける新しい通貨の発行や、取引の詳細情報は、そのすべてがコンピューターネットワーク上に分散されて、保存される仕組みです。ビットコインで行われたすべての取引記録を記載した、1 つの大きな取引台帳が存在しているとイメージしてください。この可視化された記録のおかげで、通貨の偽造や二重払いなどを防止することができます。

■ すべての記録は残りますが、その記録に個人情報は含まれません。記録はあくまでも、ビットコインの流通の整合性を保証するために存在するのです。

■ ビットコインは、特定の組織の元にではなく、分散されたコンピューターのネットワーク上にその１つの大きな取引台帳を置くことで、中央管理を不要とする仕組みなのです。

■ 取引の整合性を保証するための１つの大きな取引台帳なのに、そのデータが分散されて保存されていたら、取引記録に不整合が発生してしまいそうです。しかし、ビットコインはこの解決策を生み出したために、今日に至る広がりをみせています。

（１０） ビットコインの採掘（さいくつ）（マイニング）とは

■ ビットコインは、一定期間ごとに、すべての取引記録を取引台帳に追記します。その追記の処理には、ネットワーク上に分散されて保存されている取引台帳のデータと、追記の対象期間に発生したすべての取引のデータの整合性を取りながら正確に記録することが求められます。

■ その整合性を取る作業はコンピュータによる計算で実現できるのですが、膨大な計算量が必要となります。分散されて保存されている１つの大きな取引台帳のデータも、追記対象の取引のデータも、すべてを正確に検証してから追記しなければならないのです。

■ そこで、ビットコインでは、この追記作業に有志のコンピューターリソースを借りています。余っているコンピューターの計算能力を借りることによって、膨大な計算を行い、みんなで共有する１つの大きな取引台帳に追記を行っているのです。

■ この追記作業の手伝いをしてくれた人、追記作業のために膨大な計算処理をし、結果として追記処理を成功させた人には、その見返りとしてビットコインが支払われます。つまり、追記作業を手伝ってビットコイン全体が健全に運用されるようにがんばってくれたことへの報酬として、ビットコインが支払われるのです。

■ この報酬は、新たに発行されたビットコインによって支払われます。

■ この新規発行に至る行為は「**採掘（マイニング）**」と呼ばれています。コンピューターの計算能力をお金に変えるビジネスと割りきって、日夜採掘（マイニング）に励んでいる人たちが世界中に存在します。そのおかげで、今日もビットコインの安全性が保たれているのです。

■ 通貨としてのビットコインの新規発行は、この採掘（マイニング）を通じてしか行われません。そのため、ビットコインの発展を信じる人達が、次々と採掘活動（＝1 つの大きな取引台帳の更新作業）に力を注いでいるのです。

（１１）　採掘（マイニング）で無限に生み出されるのか

■ ビットコインの発行総量は、事前に決められています。
また、採掘（マイニング）によって発行される量も調整されています。そのため、一瞬にして発行量が増えてインフレが起こったり、混乱が生じることを避けた設計がなされています。

■ **ビットコインの発行総量は**、2140 年までに 2,100 万 Bitcoin とされていて、それ以降は新規に発行されることがありません。(1 ブロック毎に 50 コインからはじめて、210,000 ブロックごとに半減し、6,929,999 番目のブロックが最後。これを計算すると、生成されるビットコインの総量は、約 2100 万枚です。これがビットコインの発行上限です）

（１２）　誰がビットコインを考えて、つくったのか

■ ビットコインは、2008 年 10 月に、**中本哲史（Satoshi Nakamoto）**と名乗る人物がインターネット上に投稿した**論文**によって、提唱されました。

■ それからわずか 3 カ月後、2009 年 1 月には、ビットコインの理論を実現するためのソフトウェア（Bitcoin-Qt）がオープンソースで開発され、公開されました。そしてすぐに、ビットコインの最初の取引が行われています。
（開発者や、この時からビットコインを所有している人たちは、膨大な価値を持ったビットコインを所有していると言われています）

■ それからおよそ 1 年後の 2010 年 2 月に、ビットコイン両替ができる最初の取引所が誕生しました。そして、同年 5 月、はじめて現実社会でビットコインを使った決済が行われています。

（１３）　どうやってビットコインを手に入れる？

① **購入；ビットコイン取引所で、お金を払いビットコインを購入する方法。**
② **収入；サービスや商品の対価として、ビットコインを受け取る方法。**
③ **採掘；発掘されていないビットコインブロックを採掘して、報酬として稼ぐ方法。**

・・・取引所を決めたら、メールアドレス/電話番号で認証を行う。日本円で入金してビットコインを購入する。通常、BTC という単位で購入されるが、2016 年 12 月上旬現在のレートは 1BTC；8 万 5,000 円程度である。日々購入レートは価格変動している。

※ 2015 年 9 月 10 日に公開された次の YouTube(映像時間 50 分間)を一読してください。
NHK《密着 ビットコイン最前線》 ： （ビットコインの中国での採掘や規制を含む）
https://www.youtube.com/watch?v=poYOAJCb_OI

（１４）　ビットコインと課税については？

■ ビットコインは、どの管轄においても法的通貨の地位をもつ不換紙幣ではありませんが、**どんな媒体を使おうとも納税義務が生じます**。**多くの管轄で、多種多様な法律規制があり、ビットコインでも、所得、販売、給与、資本利得やその他の納税義務が生じます**。

※ 反面、ビットコインには、国境や地域の概念がなく世界共通通貨であること、それにより海外への送金も非常に高速かつ安全で低コストに行える利点があります。

（１５）　ビットコインは、匿名ですか？

■ ビットコインは、他の形状の通貨と同様に、ユーザーが、許容レベルのプライバシーで支払いを送ったり受け取ったりできるように作られています。しかし、**ビットコインは匿名ではありませんので**、現金のようなプライバシーを提供することはできません。

■ ビットコインを使用すると大規模な公的記録を残しますが、ユーザーのプライバシーを保護する様々なメカニズムがすでに存在し、**現在開発中のものも数多くあります**。
しかし、ほとんどのビットコインユーザーに、こうした機能が正確に使われるには、まだまだやるべきことがたくさんあると言えるでしょう。

■ ビットコインを使った個人の取引が、違法な目的で使われるという懸念もあります。
しかし、ビットコインが、既存の金融システムに行使されている**規制の対象となることは、疑う余地がありません**。

■ ビットコインは現金より匿名性が低く、**犯罪捜査が行われることを防ぐことは出来ません**が、**ビットコインは様々な金融犯罪を防ぐようにデザインされています**。

（１６）　なぜビットコインは、価値を持つのでしょうか？

■ **ビットコインは、通貨のように役立つものなので**、**価値があります**。

■ ビットコインは、物質的なもの（金や銀のようなもの）や中央権力への信頼（不換通貨のようなもの）が達成するようなものではなく、**数学的な特性に基づいた通貨の特徴（耐久性、ポータビリティー、代替可能性、希少性、分割可能性、および認知度）を達成**するものです。

■ こうした特性を持ち、価値を持つ通貨になるために必要なものは、**信頼と採用です**。
通貨としてのビットコインの価値は、それを支払いとして承諾する人々の存在によってのみ生まれるのです。

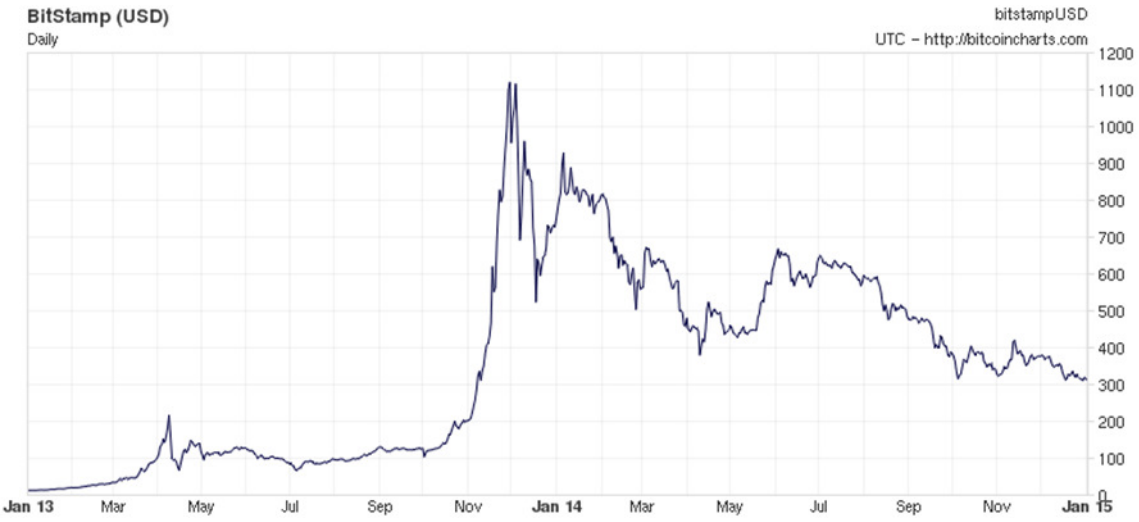
（１７）　ビットコインの価格は、どのように決まるのですか？

- **ビットコインの価格は、需要と供給で決められます**。
  ビットコインの需要が高まれば､価格が上昇します｡そして需要が減れば､価格も下降します。

- 市場に出回るビットコインの数には限りがあり、新しいビットコインの数は予想可能で、速度を落としながら作られています。つまり、**価格を安定させるには、需要がこのインフレーションレベルに追従しなければならないのです**。

- なぜなら、ビットコインは、その可能性に比べてまだ比較的小さな市場で、市場価格を左右するために多額の通貨を必要とせず、従って**ビットコインの価格はとても不安定だからです**。

（１８）　ビットコインの値段、2013 年から 2015 年まで　・・・　価格変動（リスク）が大きい。



（１９）　ビットコインは安全ですか？

- ビットコイン・テクノロジー；プロトコルと暗号学には強力な安全性の実績があり、ビットコインネットワークは、おそらく世界最大の分散コンピューティング・プロジェクトといえる。

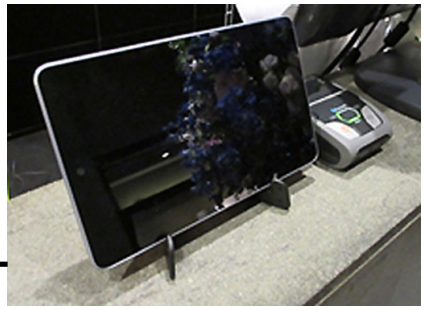
- ビットコインの最も一般的な**脆弱性は、ユーザーのエラーにあります**。

- 必要な秘密鍵を保管するビットコイン・ウォレット・ファイルをうっかり消したり、紛失したり、盗まれたりすることです。これは現金を電子的に保管するのと似ていますが、幸い、ユーザーは、通貨を守るためにセキュリティー対策をしっかり行ったり、レベルの高いセキュリティーと窃盗や紛失に対する保険を提供するプロバイダーを使って対応することができます。
  （**最近では、ランサムウェアに感染して、ファイルがロック・映像記録が出来ない状態が発生**）

（２０）　ビットコインの店舗利用方法：例

ここではお店で飲食代金の支払い時にビットコインを利用する方法を紹介します。
（ビットコインを電子マネーのように使っているケース？　営利はお店の利便性なのかなぁ？
たとえば、ビットコインを使うと割引クーポンを発行するとか？　いろいろな付加価値が付く）

① レジに設置されているタブレットとレシート印刷機



② 支払い時は、円で会計金額を入力すると、自動的に
ビットコイン換算額が、QR コードとともに表示される。

③ 顧客はスマートフォンの**ビットコインウォレット**
で **QR コード**を読み取ると、店舗の支払先ビット
コインアドレスと、支払金額が表示されるので、
ビットコイン送金を実行する。

④
⑤

④ 即時にタブレット上で入金確認が表示され、レシートが印刷されることで支払い完了となる。

ビットコインは、スマートフォンさえあれば世界的に垣根なく共通価値基準として利用可能である。

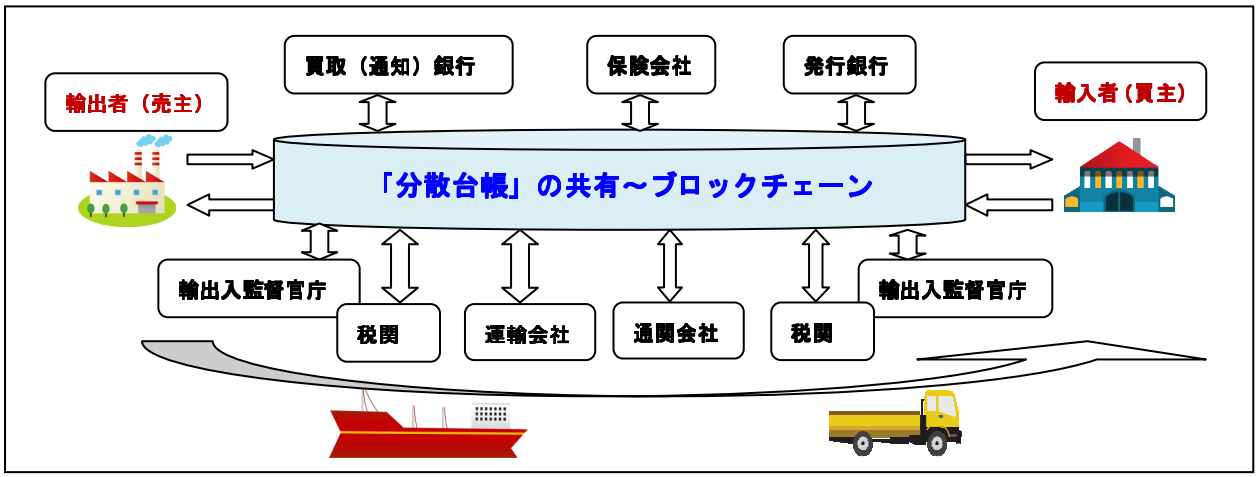
ブロックチェーンは、どうしてもビットコインから有名になった技術なので、仮想通貨や海外送金のイメージから無意識のうちに金融の取引などに影響を与えるかもわかりませんが、
・・・・　「ビットコインはブロックチェーンの技術を利用した一つの実装例」でしかありません。
ブロックチェーンとは“分散型台帳”を支える技術です。
・・・　ブロックチェーンの応用分野は、金融分野に留まらず、広く「分散型台帳」として各分野で応用が期待されています・・次はネットワークを介して共有される台帳データの適用を追ってみょう。

３．「分散型台帳」の応用が与える社会への適用＆変化

発生した全てのイベント情報が台帳に記録されるブロックチェーンは、システムの仕組みを大きく変える可能性のある技術として、現在多くの組織・団体により、研究や実証実験が盛んに行われている。

（１） 貿易関連への適用

各システムが個別にデータを保有する世界から、分散型台帳によるデータ共有を前提として、システムが連携する世界へ⇒利権移転の管理、製品ライフサイクル管理、ワークフロー管理等



これまで、**トレーサビリティ（物品の流通経路を生産段階から最終消費段階あるいは廃棄段階まで追跡が可能な状態をいう。日本語では追跡可能性とも言われる）を実現させることが困難な領域、あるいはコストがかかっていた領域に対し、シンプルに分散型台帳という形で実現する可能性がブロックチェーン技術にある。**

（２） 土地の登記サービスへの活用

ジョージア（グルジア）共和国政府は、2017 年 2 月 7 日、ブロックチェーンを活用した台帳管理のシステムを、様々な分野に拡大していくと発表した。

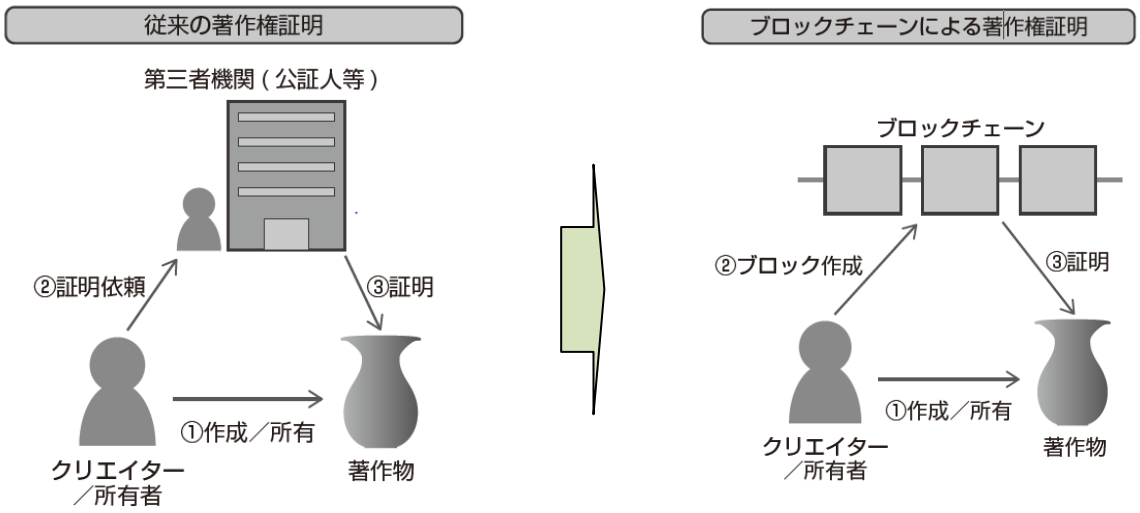
ブロックチェーンに土地の登記を行い、取引を外部から監査可能な形にする動きが進められてきた。政府がビットコインや**ブロックチェーンの仕組みを公的取引の監査に導入する**のは世界で初めての試みとなる。
ジョージア政府当局は、これまで 20 数件の**土地登記を行っており、今後は土地の購入や売却時の登録、抵当権の設定や公証制度の運用といった場面にこのネットワークを活用して行く。**

ブロックチェーンを用いた土地の登記サービスは様々な企業によって進められており、同様なソフトウェアは**スウェーデン**や**ホンジュラス等**でも導入事例がある。

（3） 著作権管理への適用

■ 著作物の情報をブロックチェーンに記録し、著作権の証明書を発行するサービス

■ 従来は第三者機関の証明が必要 ⇒ 改ざん耐性を備えた著作権情報のオープン化
（**第三者機関が不要で証明が可能となる**）



（4） エストニア共和国に見る国家的戦略の“e 国家”

国家の仕組みのデジタル化において先進国として知られるのが東欧のエストニア共和国。同国のデジタル化の状況と成功要因を見ることによって、先端 IT の推進に必要な要件を抽出する。

最近も「ブロックチェーンを ID カードに導入」「医療データの記録にブロックチェーン利用へ」「ブロックチェーンで公共サービスを提供」といった同国に関する記事が多数報道されている。

年　度	導入したシステム
2000 年	e-Tax ボード、m-Parking
2001 年	Popudation ﾚｼﾞｽﾄﾘ、 x －Road
2002 年	e-Scool、デジタル署名
2003 年	ID バスチケット、e-Land ﾚｼﾞｽﾄﾘ
2005 年	オンライン選挙
2007 年	モバイル ID、e-Polith システム

年　度	導入したシステム
2008 年	e-Health システム
2010 年	e-Prescription（クスリの処方箋）
2011 年	スマートグリッド（電力）
2012 年	EV(電気自動車)の急速充電ﾈｯﾄﾜｰｸ
2013 年	x-Road. Eurpe
2014 年	電子居住、データ大使館　等々

デジタル化によって人々の生活やビジネスをシンプルにすることを推し進めてきた。**「国にとって必要なのは領土ではなく人」という考えをベースに、人や国に関するデータおよび、国の仕組みをサイバー空間上に実現している。**

4．最後に次のインターネット～？　・・・　技術革新や適応領域の応用範囲が拡大して進化している

（1） イーサリアムというサービス　・・・今後、どんな技術の基盤が発達するのだろう。

イーサリアム（Ethereum）は、「ブロックチェーン」と呼ばれる技術をベースに、なんら特別な管理者のいない P2P システム上で様々なサービスを実現するための基盤を提供するものです。

お金を A さんから B さんへ送るだけなら、A さんが署名すればいいだけだから、普通のビットコインのシステムは一方通行なんです。
・・・・・　でも契約書は A さんと B さんの相互署名が必要だから、一方通行ではできません。

イーサリアムはビットコインの仕組みを使っているけれど、一方通行ではなく、土地の権利書や自動車の所有証明書などの契約書をインターネット上で作成できるようにした。
・・・・・・・　そしてイーサリアムは中央集権機関がない任意団体なんです。

（2） ブロックチェーンとの相性の良い領域とは　・・・今後、どんな分野に発展してゆくのだろう。

ブロックチェーンの利点

① データの高い透明性・トレーサビリティ
② 仲介者を介さない直接的なやり取り
③ 高改ざん耐性
④ 単一障害点がない（高可用性）

ブロックチェーンの課題

① P2P ネットワーク上で動作するための遅延
② 高可用性だけが重視されており、データの一貫性や分断耐性が不十分（CAP 定理）
③ 方法によってはデータのファイナライズが不確定

ブロックチェーンとの相性の良い領域

① 台帳を共有することで価値を見出せる領域
- **トレーサビリティ：追跡可能性（物品の流通経路を生産から最終消費あるいは廃棄段階まで追跡可能な状態）**
- **サプライチェーン：共通連鎖（原材料・部品等の調達から、生産、流通を経て消費者に至るまでの一連のビジネス）**

② リアルタイム性を求められない領域

◆ビットコインは、お金のやりとりに関する仕組みなので、一般に流通するためには、まだまだ、規制や課税、安全性や価値の問題などクリアしなければならない課題が多々あります。しかし、スタートアップ通貨というものは、かつて世界にはありません・・・これが、今後どのように展開するのか？
◆方や、ブロックチェーンとは何か、なぜインターネットに匹敵する発明だと言えるのだろうか？
⇒ブロックチェーンの優れている点は、やりとりを管理する中央集権的な組織や仕組みの存在が不要なところです。やりとりは、インターネットなどのネットワークを通じて共有される点が、既存のやりとりを仲介するシステムと大きく違うところです・・・・今後、どんな分野に発展してゆくのか？
大型ｺﾝﾋﾟｭｰﾀが取引台帳を集中管理した時代から、参加者が共有する分散管理の時代へと考えを改革しょう