令和元年度「専修学校による地域産業中核的人材養成事業」
スマートコントラクトを使用したシステム開発人材の育成

ブロックチェーン概論
指導マニュアル

学校法人 麻生塾　麻生情報ビジネス専門学校

令和元年度「専修学校による地域産業中核的人材養成事業」
スマートコントラクトを使用したシステム開発人材の育成

ブロックチェーン概論
指導マニュアル

学校法人 麻生塾 麻生情報ビジネス専門学校

ブロックチェーン概論指導マニュアル

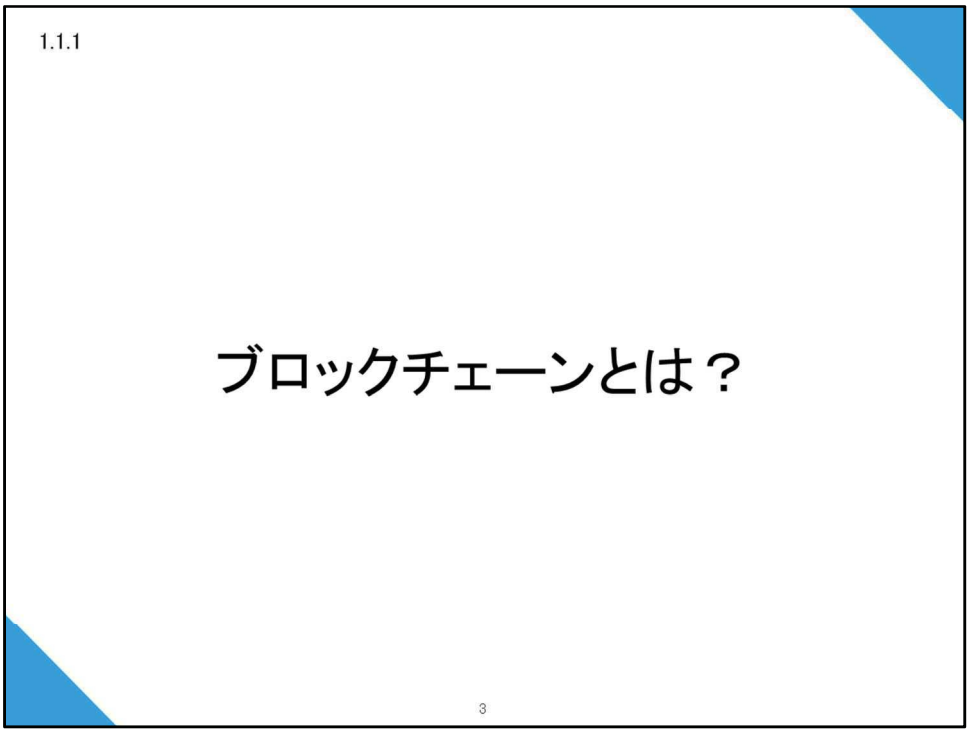
このスライドは
「ブロックチェーン概論」の教科書とリンクしており、
講師が授業に利用できる構成となっています。
教科書とのリンクはスライド左上部の章番号を参照してください。

各スライド内で説明する内容、注意事項は
「ブロックチェーン概論指導マニュアル」冊子をご覧ください。

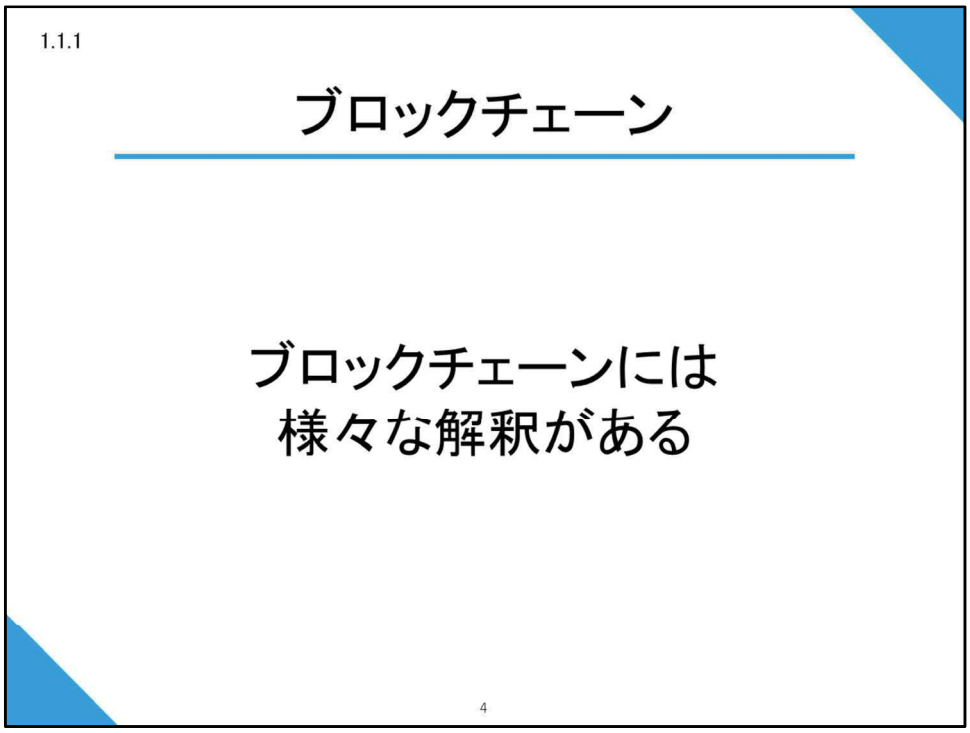
1

1. ブロックチェーンの概要

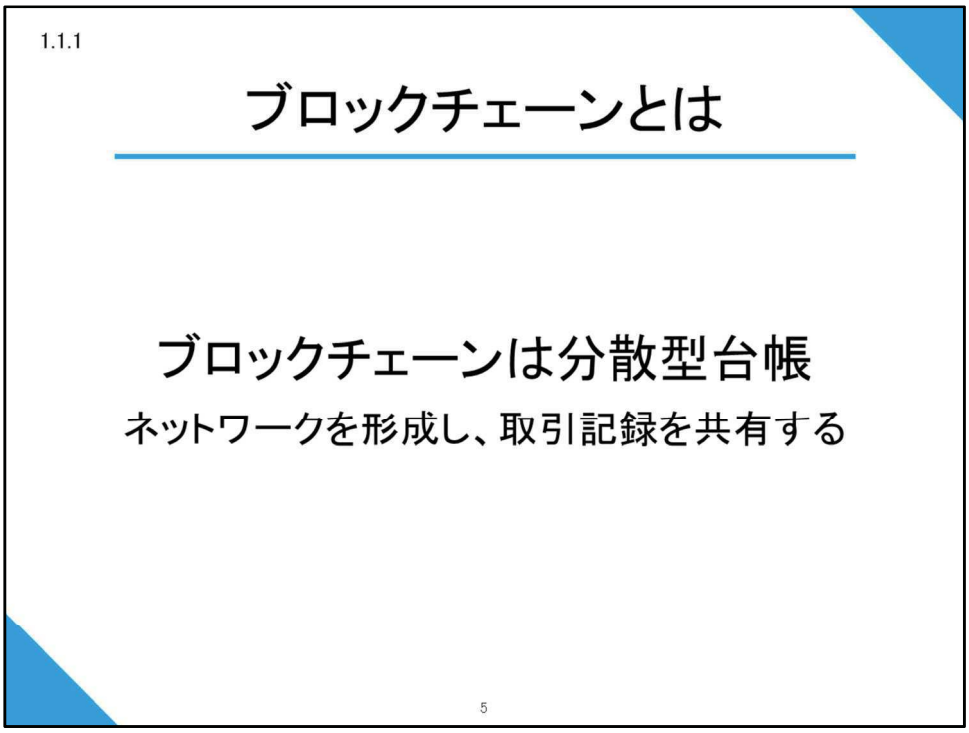
2



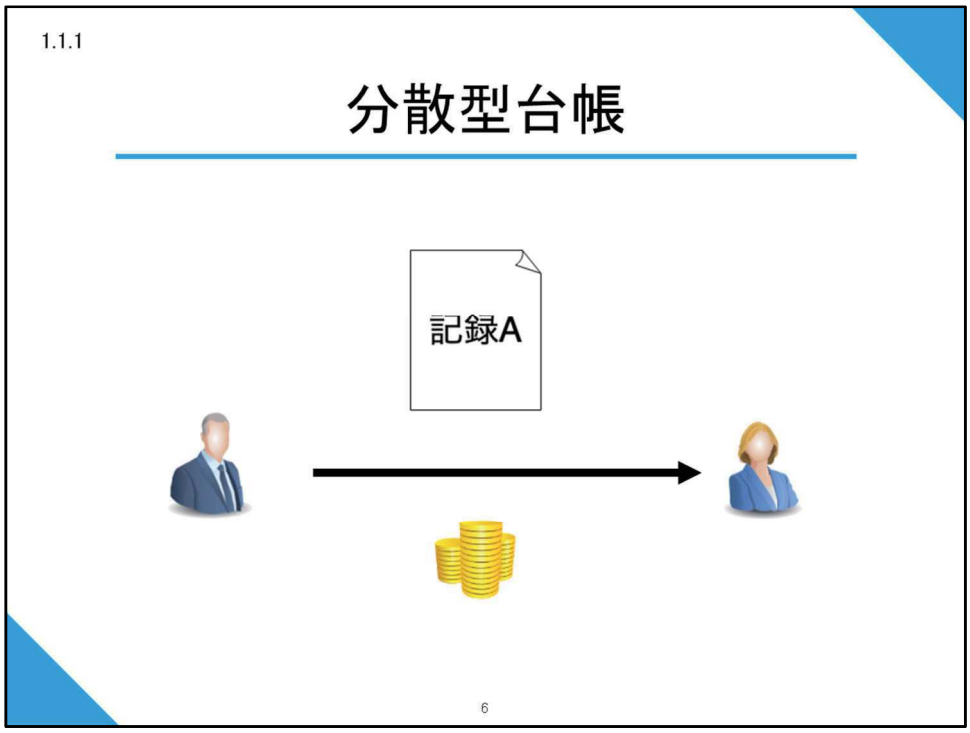
生徒に対して問いかけを行い、ブロックチェーンについて知っていること、イメージなどについて発言してもらう。



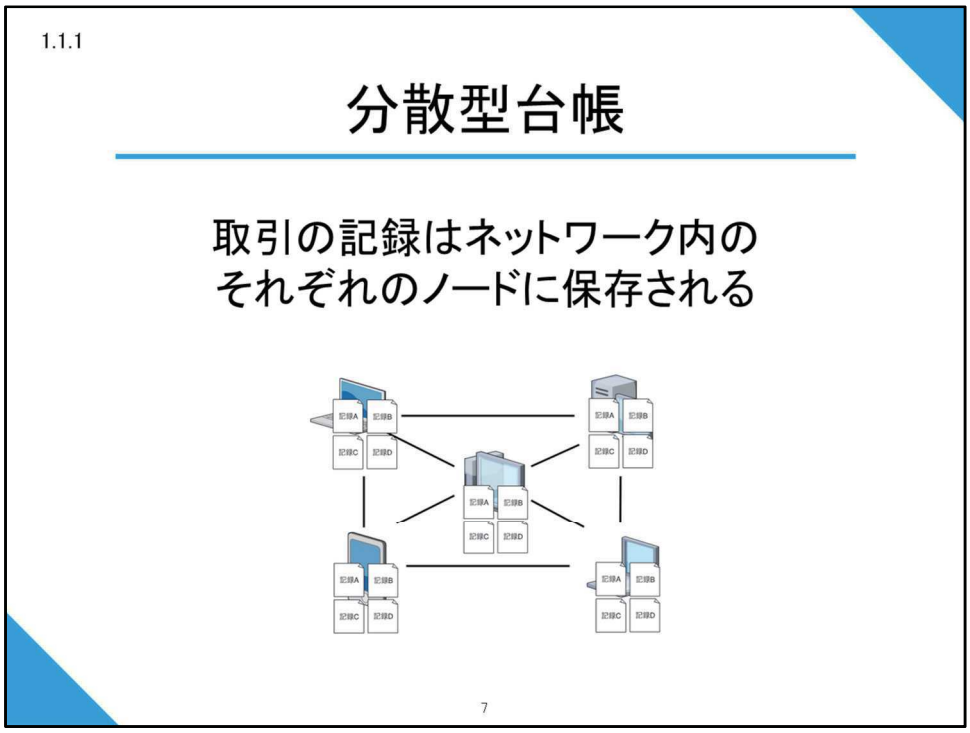
- ブロックチェーンには様々な解釈が存在する。
- ブロックチェーンに厳密な定義は存在しない。
- 「ここまでがブロックチェーンで、ここからはブロックチェーンではない」という線引きは難しい。



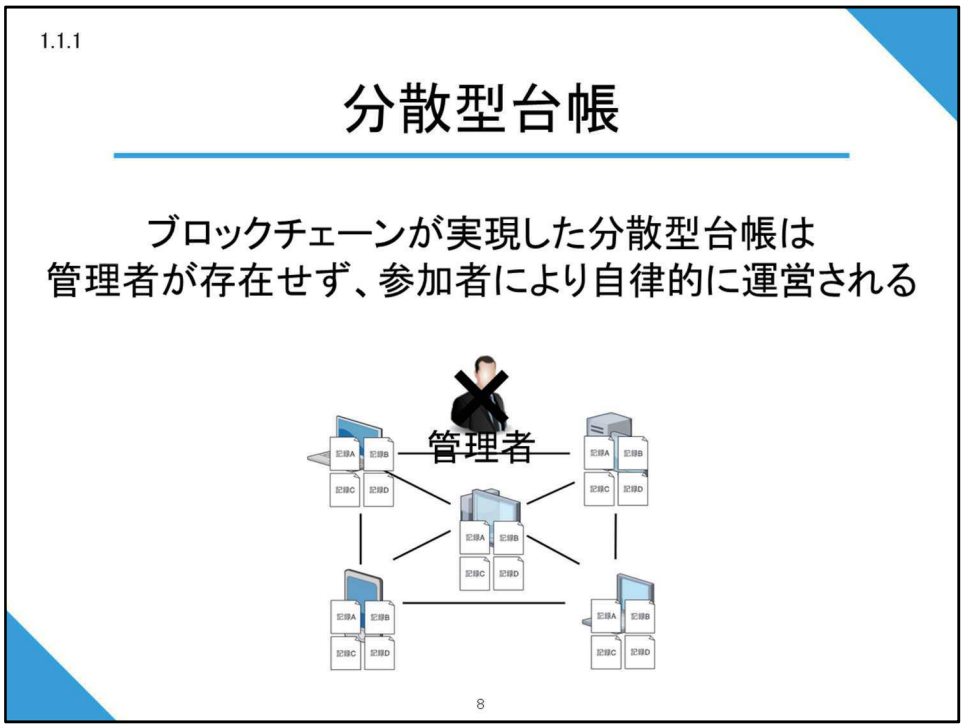
- ここではブロックチェーンは「分散型台帳」であると定義する。
- ブロックチェーンでは、参加者によりネットワークが形成され、その中で取引の記録が共有される。
- 単純に取引の記録を保存するだけの台帳ではなく、取引自体の処理もネットワーク内で行われる。



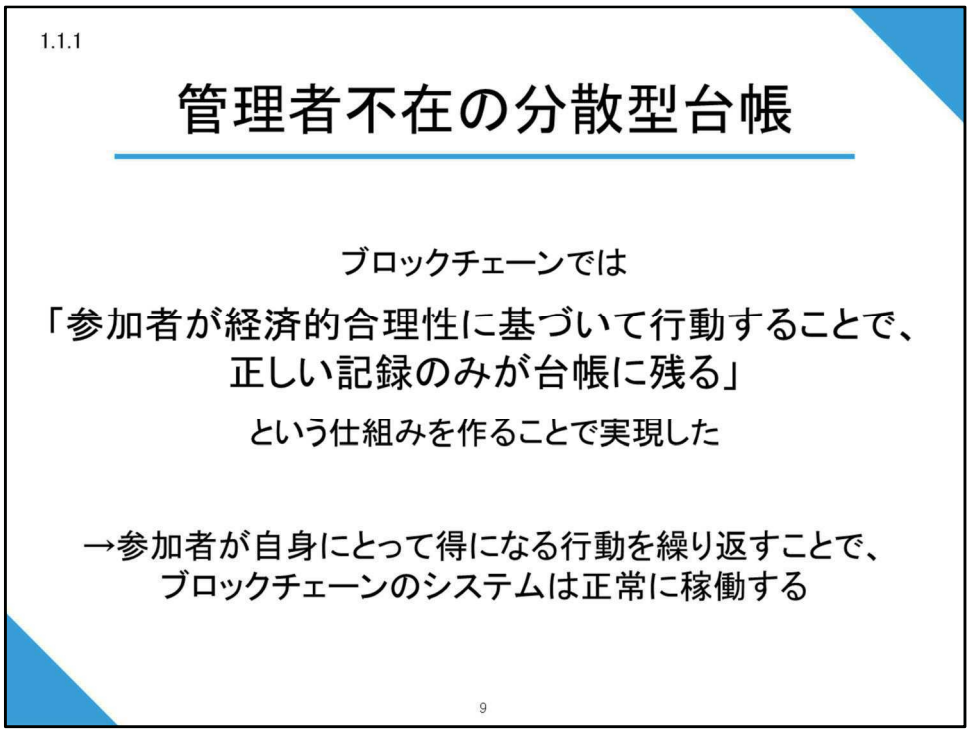
- ある取引がブロックチェーンネットワーク内で行われたとして、その取引記録を「記録A」とする。



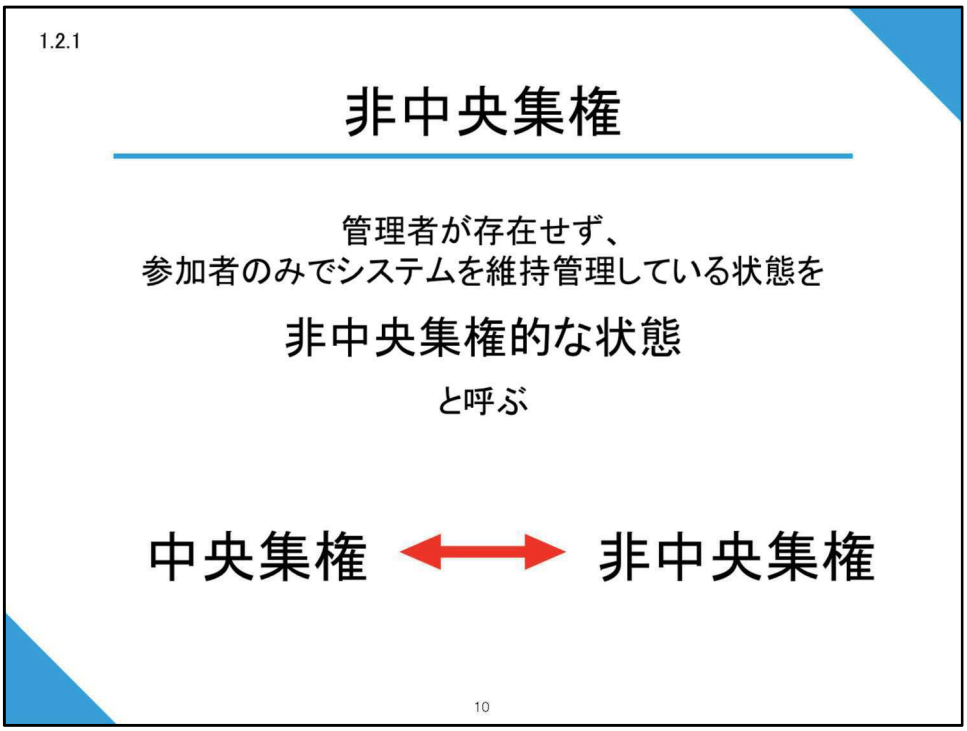
- 記録Aは特定の場所ではなく、ブロックチェーンネットワーク内のそれぞれのノードに保存される。
- 記録A以外にもネットワーク内で行われた様々な取引がノードに保存される。
- このような仕組みからブロックチェーンは分散型台帳であると言われる。



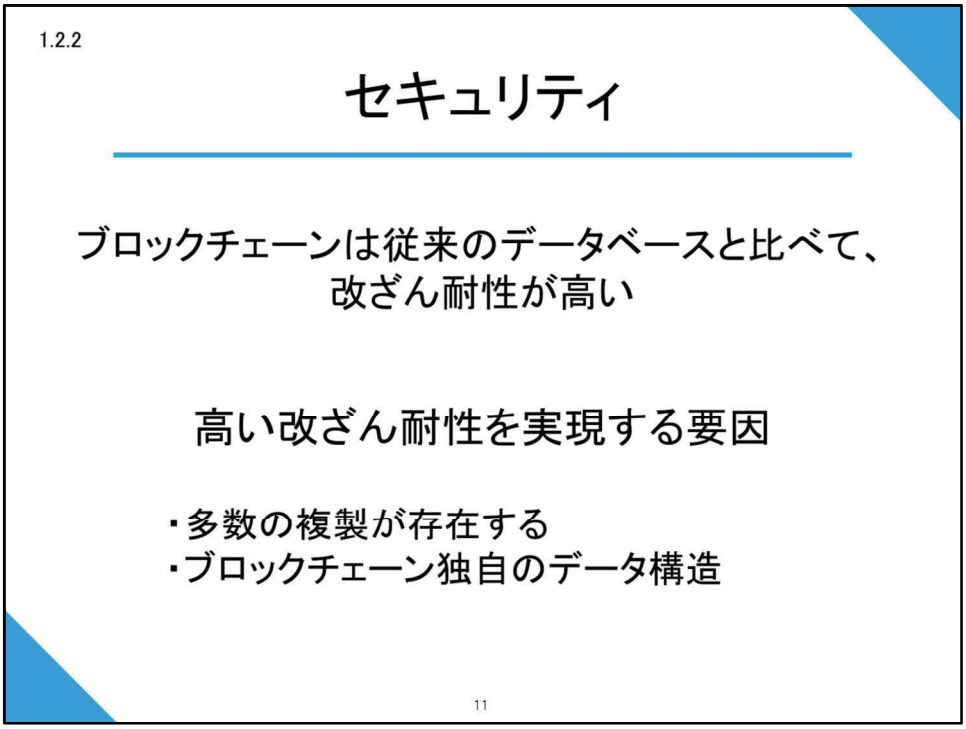
- 分散型台帳の仕組み自体は以前から存在していたものであり、新しい技術ではない。
- ブロックチェーンが実現した分散型台帳は、「管理者が存在せず、参加者により自律的に運営」されることが大きな特徴である。
- 悪意のある参加者によって、台帳に対して不正が行われる可能性があったため、これまでは実現することが難しかった。



- ブロックチェーンでは管理者不在の分散型台帳を、「参加者が経済的合理性に基づいて行動することで、正しい記録のみが台帳に残る」という仕組みを作ること実現した。
- 言い換えると、「参加者が自身にとって”得”になる行動を繰り返すことで、ブロックチェーンのシステムは正常に稼働する」。
- 特定の”誰か”が責任を持って管理するのではなく、ブロックチェーンに貢献するとお得なのでたくさんの参加者が管理してくれる。



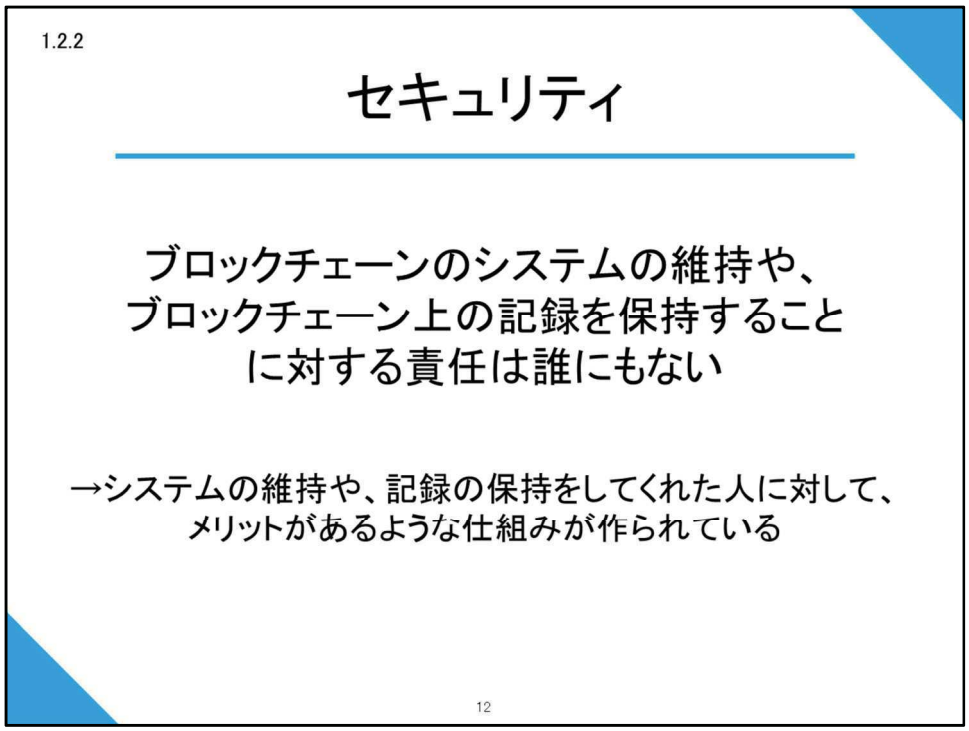
- 管理者が存在せず、参加者のみでシステムを維持管理している状態を「非中央集権的な状態」と呼ぶ。
- 一方で、従来のシステムに用いられている管理者が存在するシステムは「中央集権的なシステム」である。
- 世の中の大半の仕組みは、中央集権的な仕組みの上で成り立つ。(IT、非ITに関わらず)



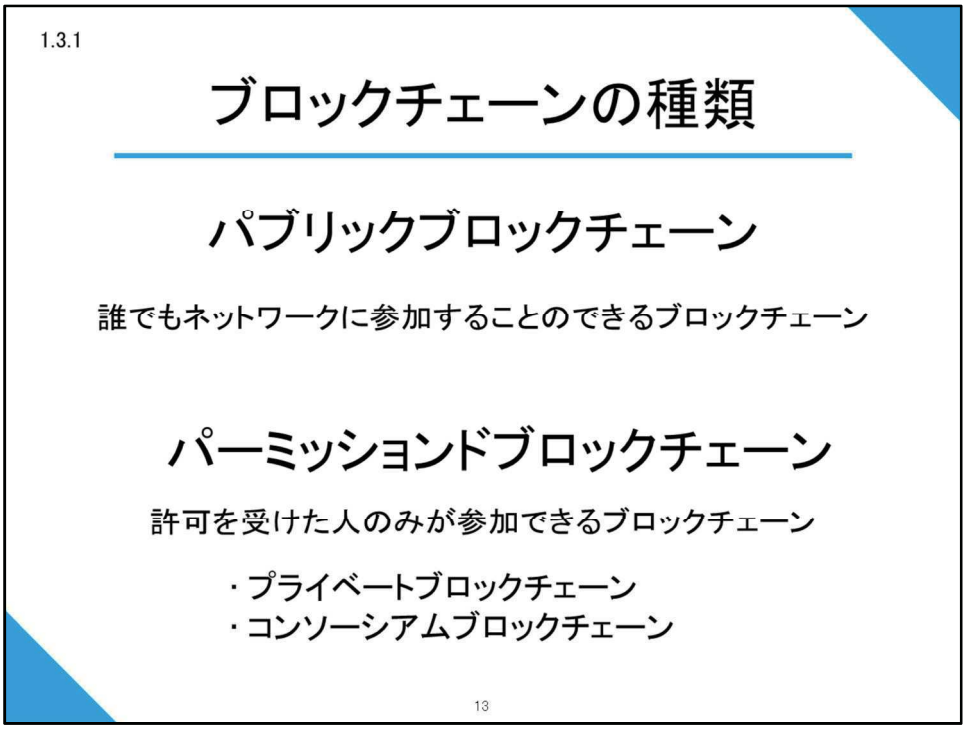
ブロックチェーンを記録を保存するデータベースとして捉えたとき、既従の仕組みに比べて改ざん耐性が高い特徴があり、この特徴はブロックチェーンの以下の性質により生まれる。

- ネットワーク内に多数の複製が存在する。
- ブロックチェーン独自のデータ構造とデータを記録するための仕組み

- ブロックチェーンのデータ構造については3章、データを記録するための仕組みについては6章で説明する



- ブロックチェーンは管理者が存在しないシステムであることから、誰にもシステムの維持管理や、記録の保存に対する責任はない。つまり、システムの停止や、データが紛失改ざんも誰のせいにすることもできない。
- 以上の問題を解決するために、ブロックチェーンではシステムの維持や記録の保持を行なった参加者にメリットがあるような仕組みを作っている。
- 実際にブロックチェーンの１つであるBitcoinは運営開始以来10年間1度も停止していない。



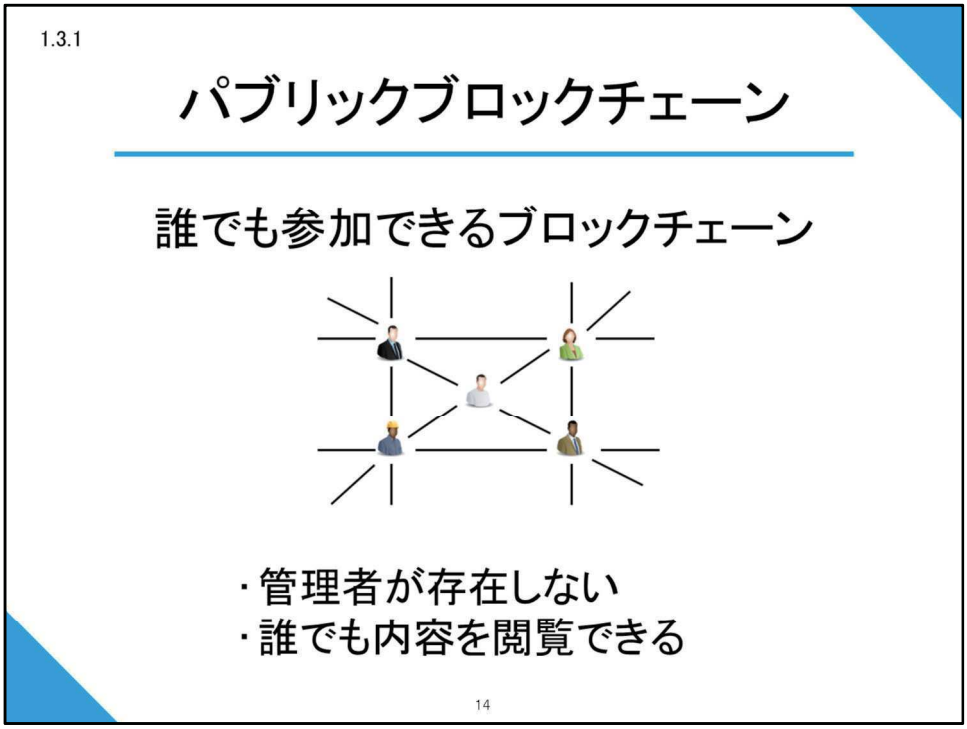
ブロックチェーンは管理者の有無で大きく2種類に分けることができる。

パブリックブロックチェーン

- 管理者が存在しない、誰でも参加することができるブロックチェーン

パーミッションドブロックチェーン

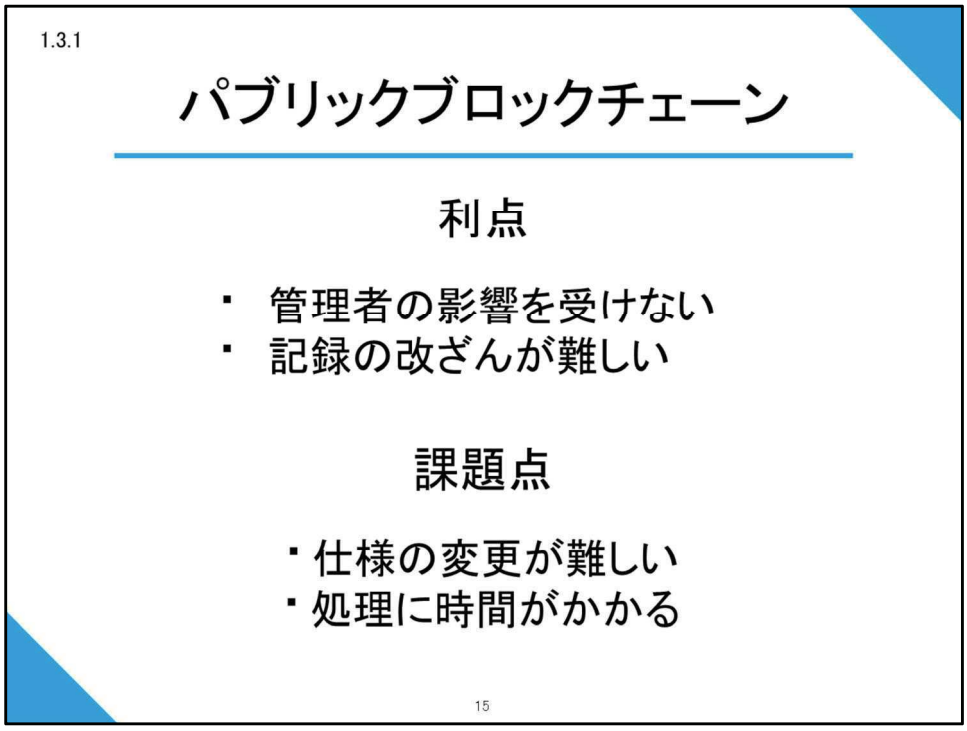
- 管理者が存在し、参加には許可が必要なブロックチェーン
- パーミッションドブロックチェーンは管理者の数によって、「プライベートブロックチェーン」と「コンソーシアムブロックチェーン」に分けることができる。



- パブリックブロックチェーンは言葉の通り、「パブリック（公的な,開かれた）」なブロックチェーンであり、ブロックチェーンネットワークに誰でも参加することができる。
- ブロックチェーンに参加するとはネットワーク内の１つのノードになるということを言う。

パブリックブロックチェーンの特徴

- 管理者が存在せずに、参加者により自律的にシステムが運営される。
- ブロックチェーン(台帳)に記録されている取引の記録は誰でも閲覧することができる。



利点

- 管理者による影響を受けない

管理者の存在するシステムでは運営者が運営を辞めることや、独断による仕様の変更などによりユーザーが不利益を被ることがある。パブリックブロックチェーンでは管理者が存在せず、参加者により自律的に管理されているため、独断でのシステムの停止や、仕様の変更などはない。

- 記録の改ざんが難しい

パブリックブロックチェーンは世界中の多数のコンピュータによってシステムが支えられているため、従来のデータベースシステムやパーミッションドブロックチェーンに比べて改ざん耐性が高い。

課題点

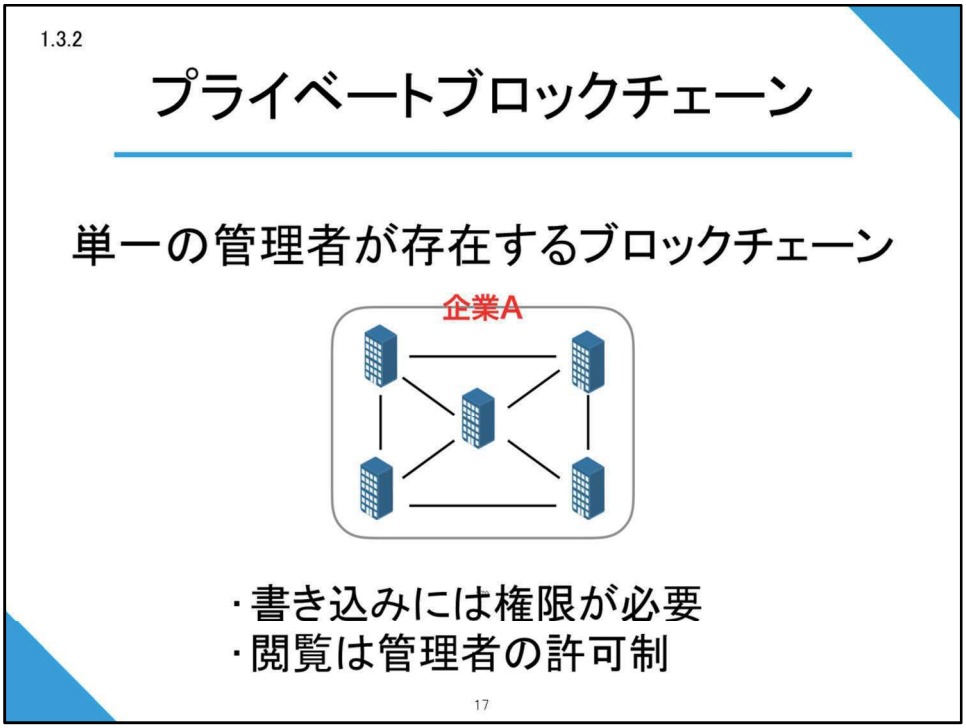
- 仕様の変更が難しい

管理者の存在せず、全員が同等な権限を持つシステムでは、多数の参加者による同意を取り、仕様の変更を行うことにコストがかかる。

- 安全な取引を行うためには時間がかかる

パブリックブロックチェーンの多くでは、時間の経過とともに台帳には正しい記録のみが残る仕組みになっているものが多いため、安全な取引を行うためには時間がかかる。このような理由から即時性の必要な処理には向いていない。

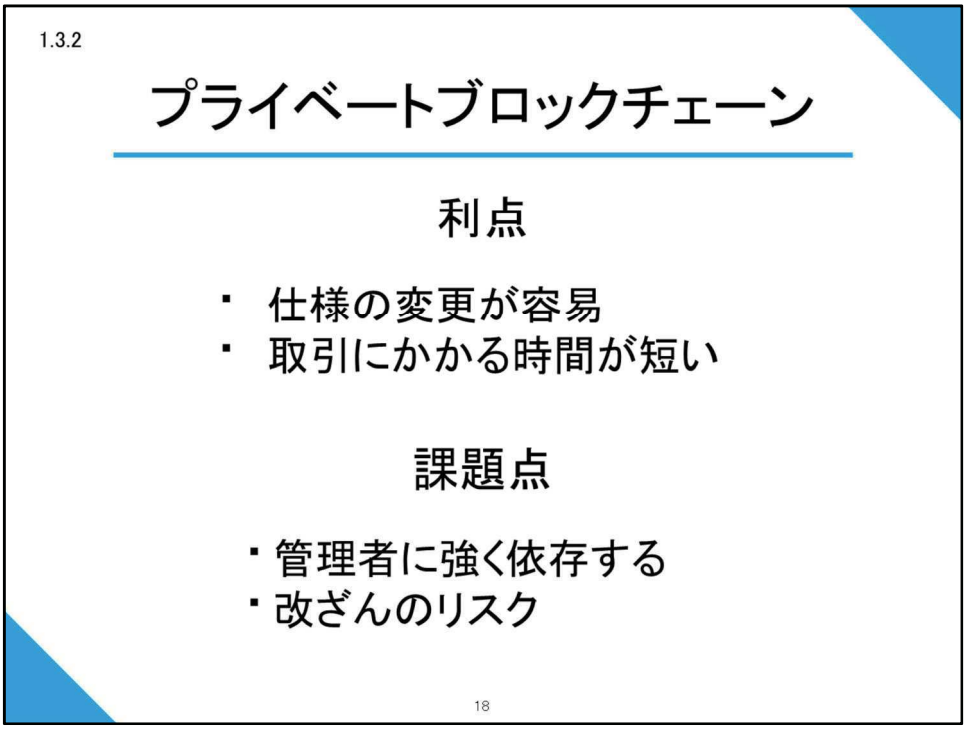
- クライアントソフトと呼ばれるソフトウェアを利用することで、ブロックチェーンのネットワークに参加することができる。
- Bitcoinのクライアントソフトの１つにBitcoinCoreがある。このクライアントソフトはBitcoinネットワークの中で最もシェアが高い。
- Bitcoinの仕様を満たしていれば、どんなソフトを利用しても構わない。自分で作成したソフトで参加することもできる。
- クライアントソフトを利用してネットワークに参加することで、取引が正しいものであるかの検証や、台帳への記入が行えるようになる。



- 単一の管理者が存在するブロックチェーン
- 特定の組織や企業内での運用が想定される
- プライベートブロックチェーンに参加するためには、管理者が提供するソフトが必要になる。

プライベートブロックチェーンの特徴

- ネットワークに参加するためには、管理者の許可が必要になる。
- ブロックチェーン(台帳)に記入されている内容の公開範囲は管理者によって決められる。



利点

- 仕様の変更が容易

管理者が存在するため、仕様の変更は管理者の判断により、比較的簡単に行うことができる。

- 取引にかかる時間が短い

台帳への書き込みは管理者が行うため、パブリックブロックチェーンに比べて処理が単純であり、取引にかかる時間は短い。

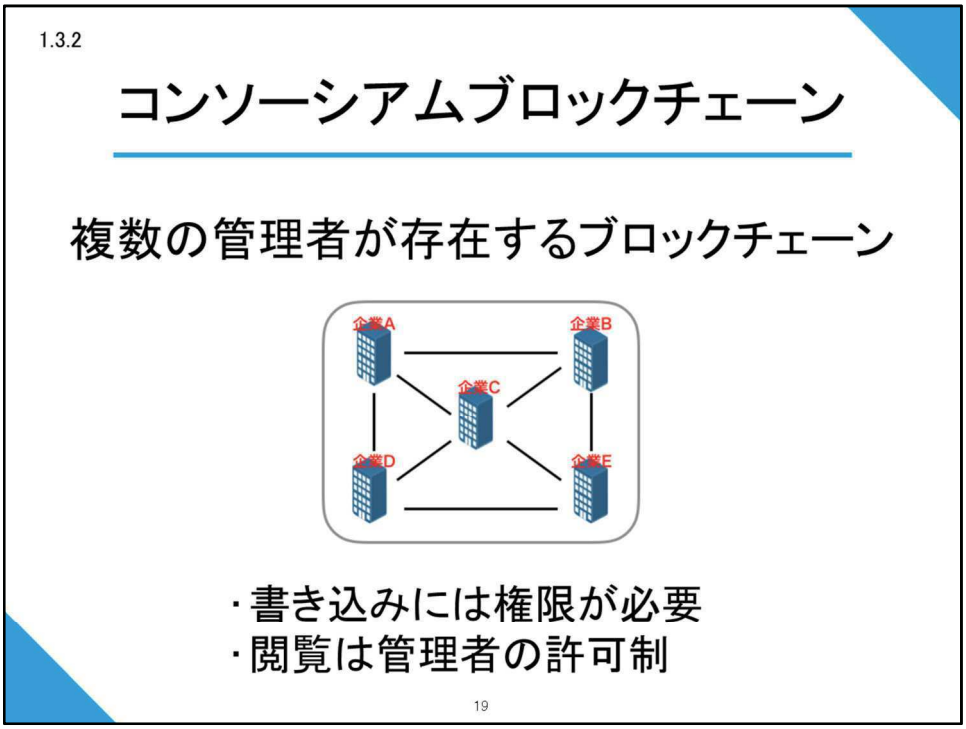
課題点

- 管理者に強く依存する

管理者に強く依存した中央集権的なシステムになる。

- 改ざんのリスク

パブリックブロックチェーンに比べて参加者が少なく管理者が存在するため、複数のコンピュータで同時に不正が行われることや、管理者権限が奪われることで、改ざんが発生するリスクがパブリックブロックチェーンに比べると高い。

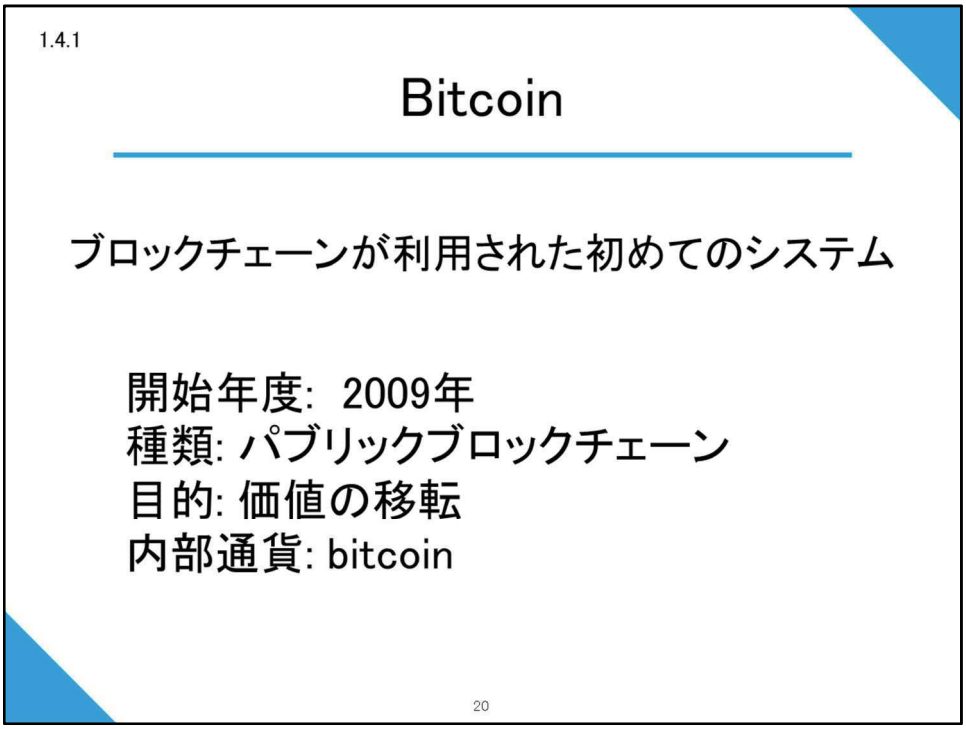


- 複数の管理者が存在するブロックチェーン
- 複数の組織や企業間での運用が想定されるブロックチェーン

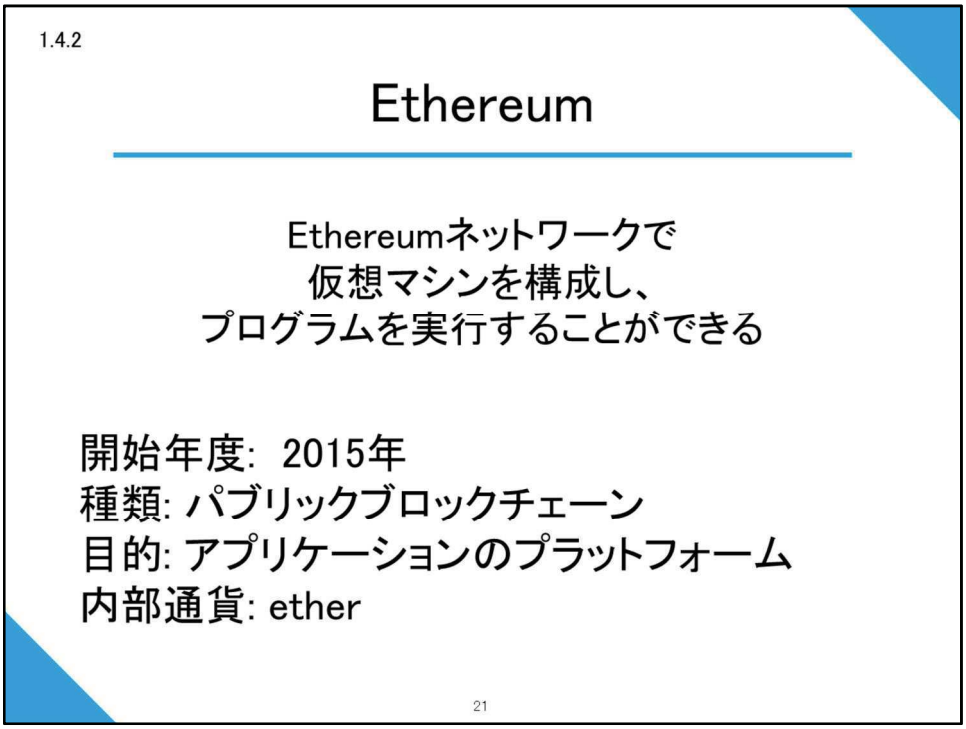
コンソーシアムブロックチェーンの特徴

- 参加には許可が必要
- 閲覧には管理者の許可が必要

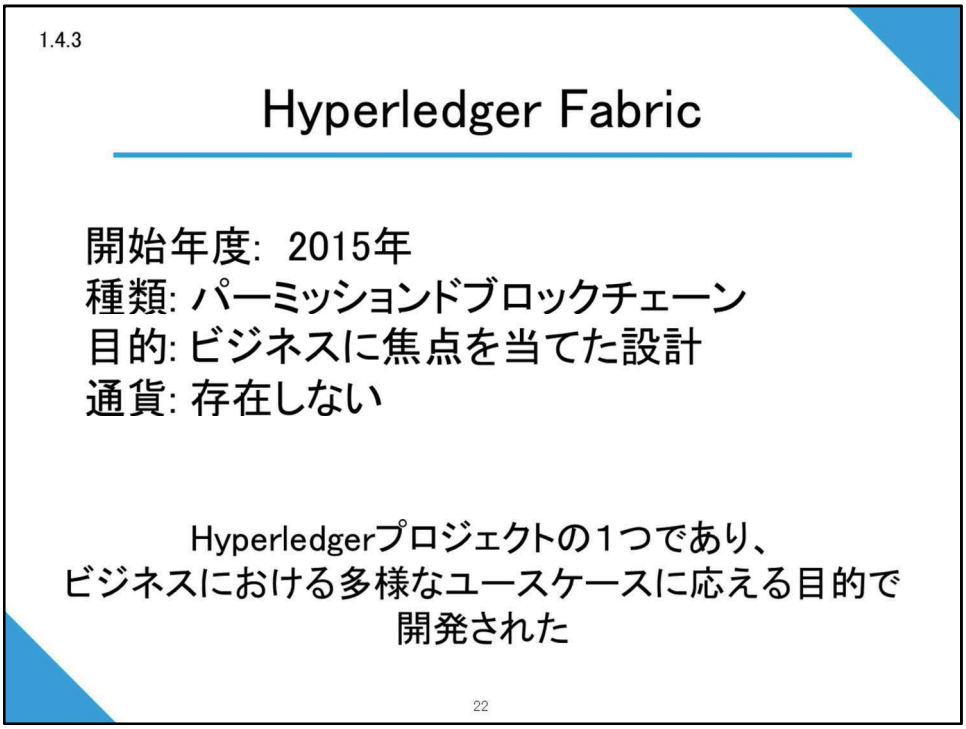
- 管理者が複数存在するという点は異なるものの、プライベートブロックチェーンと似たような性質を持つ。



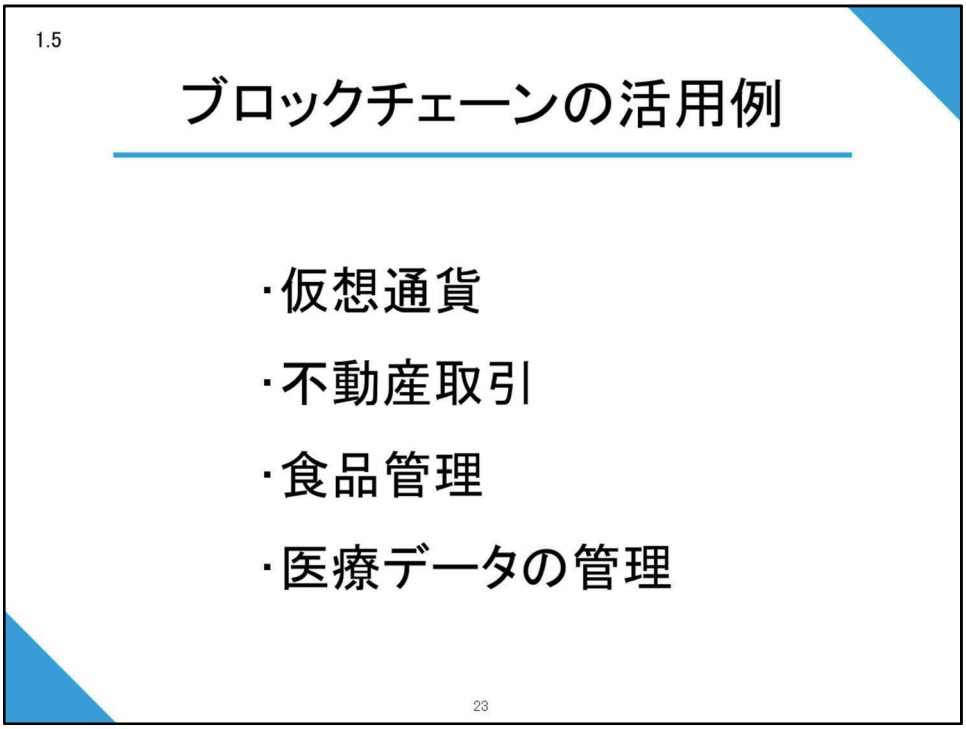
- ブロックチェーンが用いられた初めてのシステム
- 内部通貨であるbitcoinを用いて、価値の移転を行うことに特化したブロックチェーン
- パブリックブロックチェーンであり、ネットワークには1万以上のコンピュータが参加している。
- Bitcoinのノードの分布は次のサイトで確認することができる。(https://bitnodes.earn.com/)



- 2015年に誕生したパブリックブロックチェーン
- Ethereumは非中央集権的に運営される分散型アプリケーションのプラットフォーム
- Ethereumネットワークで仮想マシンを作成し、それを動かすための燃料として内部通貨のetherが存在する。
- Bitcoinに比べて、様々な処理を行うことができる。



- Hyperledgerプロジェクトの1つ
- オープンソースのブロックチェーンプラットフォームであり、Hyperledger Fabricを用いることで、様々な用途に応じたブロックチェーンを作成することができる。
- パーミッションドブロックチェーンでの利用が想定されている。



仮想通貨

- ブロックチェーンの最大の活用例
- 管理者を必要とせず、自律的にデジタル通貨の取引ができるようになった。

不動産管理

- 管理者を必要とせずに安全な取引を行うことができる点を利用して、不動産取引を不動産業者などの仲介者を必要とせずに行うことができる。
- 不動産の所有権をブロックチェーンに記録することで、ブロックチェーンの高い改ざん耐性を利用して安全に管理することができる。
- 不動産に限らず”権利”の管理はブロックチェーンの利用が期待されている分野である。

食品管理

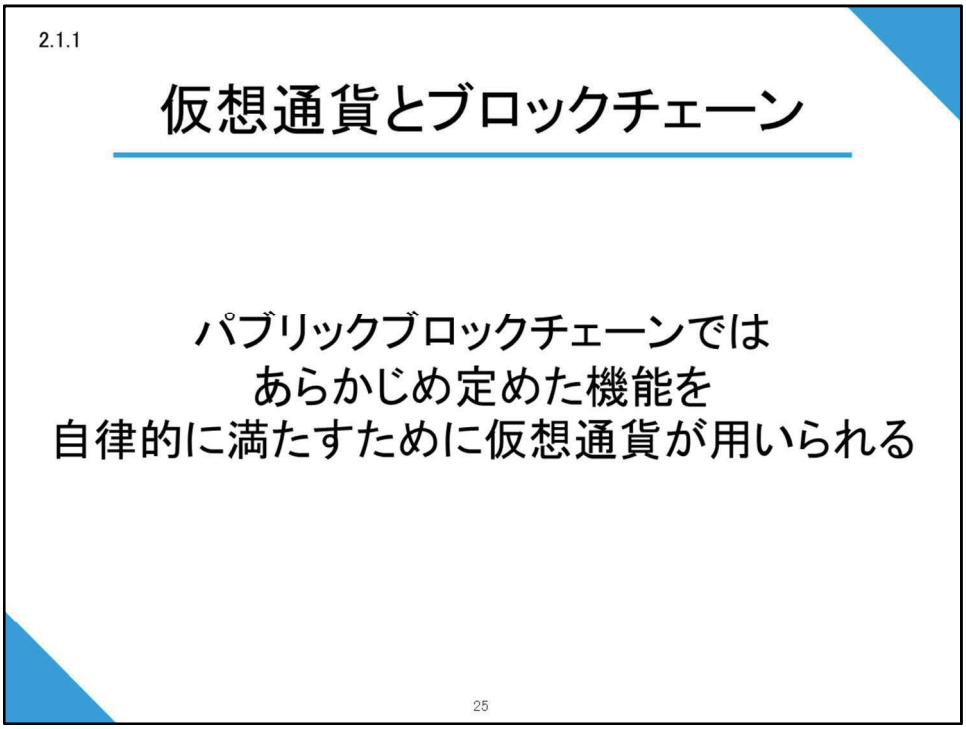
- 農場から消費者に届くまでの流通経路をブロックチェーンに記録することで、生産地や輸送業者などの食品関する情報を簡単に知ることができる。現在は、流通に関わる企業が持つそれぞれのデータベースに情報が記録されているので、照会が難しい。
- 農作物を生産した土壌の情報などをブロックチェーンに記録することで、有機野菜であることの証明をすることもできる。

医療データの管理

- 電子カルテや処方箋の情報をブロックチェーン管理することで、どこの病院に行った場合にも過去の怪我や病気の記録、処方された薬の情報を医者は正確に知ることができる。極めて秘匿性の高い情報であるので、アクセス制限、暗号化などが必要になる。
- 改ざん耐性の高さを利用して、新薬の治験のデータの改ざんの防止や、遺伝子データなど複雑な利権の絡むデータの管理などにも利用される。

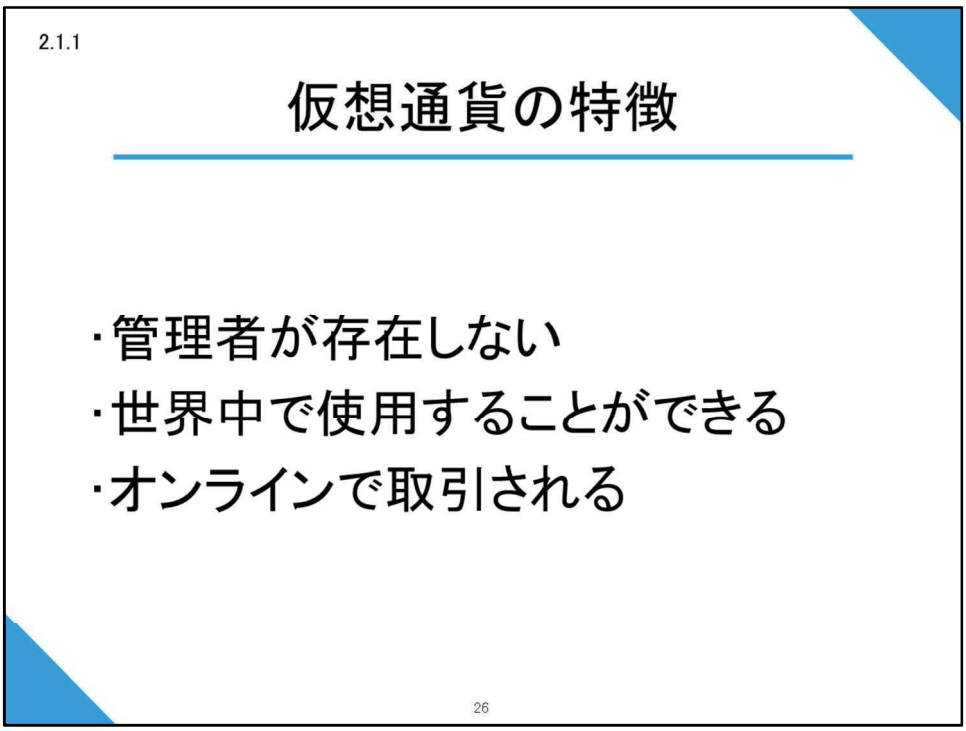
2.ブロックチェーンと仮想通貨

24



- BitcoinやEthereumをはじめとしたパブリックブロックチェーンでは、あらかじめ定めた機能を管理者不在で実現するために、仮想通貨が用いられる。つまり、現在のところパブリックブロックチェーンを運営するためには、仮想通貨が必要不可欠である。
- Bitcoinというブロックチェーンを動かすためにbitocinという通貨が利用され、Ethereumというブロックチェーンを動かすためにetherという通貨が利用されている。

- ブロックチェーンのシステムの構成要素として存在するものではなく、ブロックチェーン上のアプリケーションとして存在する仮想通貨もある。



- 管理者が存在しない

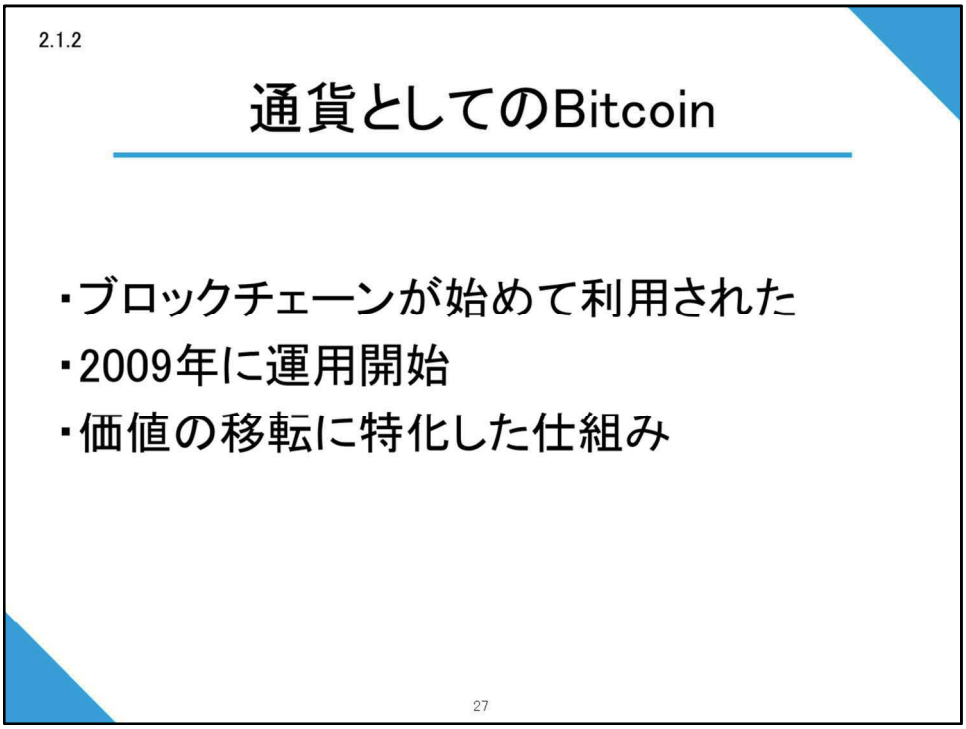
ブロックチェーンをベースとした仕組みであるため、管理者は存在しない。この点が仮想通貨の最大の特徴と言うことができる。すべての仮想通貨が必ず管理者不在で、非中央集権的に運営されているわけではない。(Rippleは企業が運営する仮想通貨、LibraはFacebookをはじめとした複数の企業が合同で運営する仮想通貨)

- 世界中で使用することができる

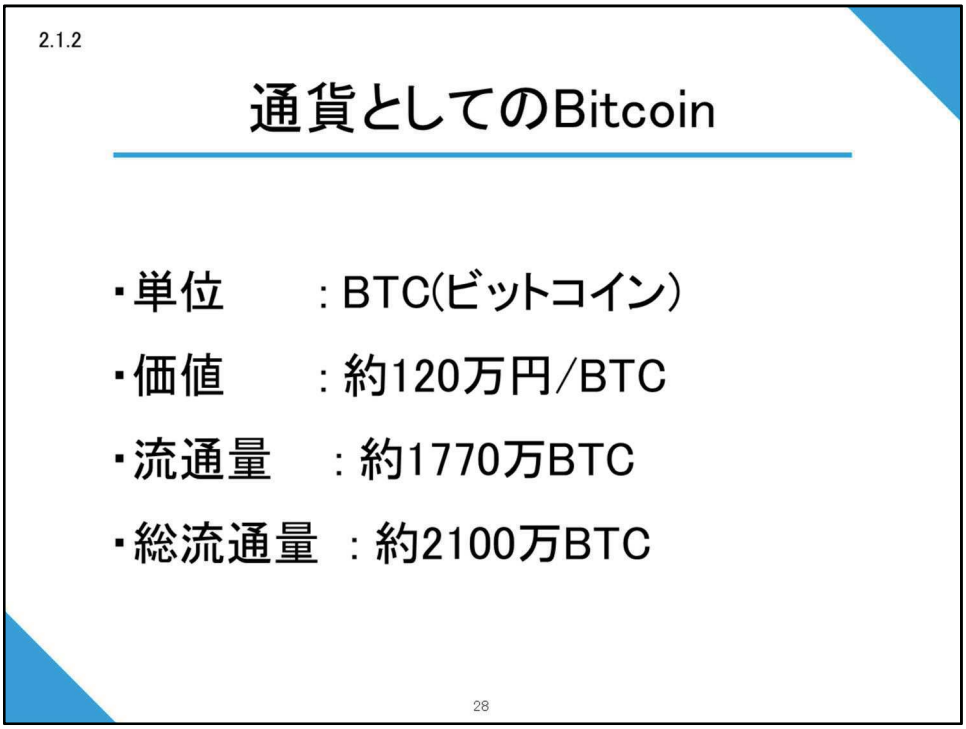
日本円やアメリカドルなどの法定通貨と異なり、世界中どこでも利用することができる。

- オンラインで取引される

仮想通貨はオンライン上で取引が行われるため、紙や金属などの物質として存在しない。ここでこれが「ビットコインですよ！」と手に持って見せることはできない。

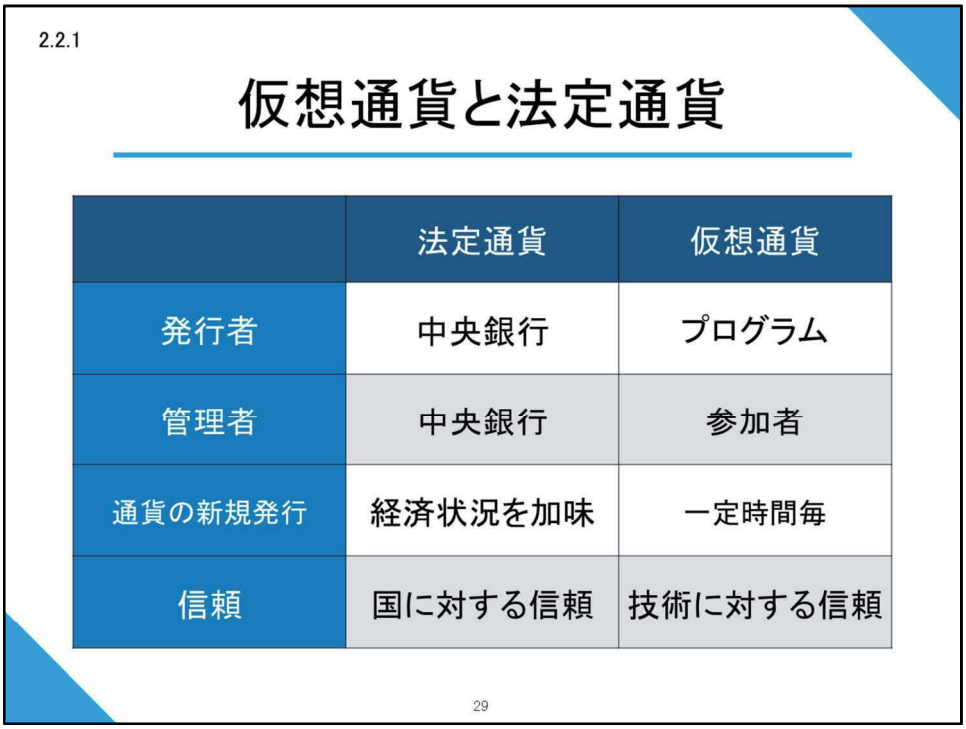


- ブロックチェーンが初めて利用されたシステムがBitcoin。Bitcoinを作るためにブロックチェーンが作られたとも言うことができる。
- 2009年1月に運用が始まり、現在(2019年8月)まで一度も止まらず、稼働している。
- それぞれのブロックチェーンには作られた目的があり、それぞれに特徴がある。Bitcoinはデジタル通貨を誰にも止められることなく利用することを目的に作られた「価値の移転に特化した仕組み」であり、ネットワーク内に流通する仮想通貨bitcoinにより価値の移転が行われる。
- 「ビットコイン」という言葉は、システム全体、ネットワーク、通貨など様々なものを示すことがあるので注意が必要である。



- Bitcoinの単位は「BTC」と書いて「ビットコイン」と読む。
- 単位はBTCだけでなく、最小単位に「satoshi」がある。(1satoshi = 1.0 × 10 ^ -8 BTC)。
- 2019年8月初旬の段階では1BTCには約120万円の価格がついている。
- Bitcoinの総流通量はあらかじめ約2100万BTCに定められている。これは通貨の発行量が多くなりすぎると、需要と供給の関係から通貨の価値が下落してしまうことを防ぐためである。
- Bitcoinの流通量や価格などについては、以下のサイトから確認することができる。

(https://www.blockchain.com/ja/charts)



仮想通貨と法定通貨の最大の相違点は「管理者」の有無であり、この点を踏まえて表を確認すると理解しやすい。

- **発行者**

法定通貨はその通貨が利用される国や地域が発行を行う。仮想通貨の発行はプログラムにより自動的に行われる。

- **管理者**

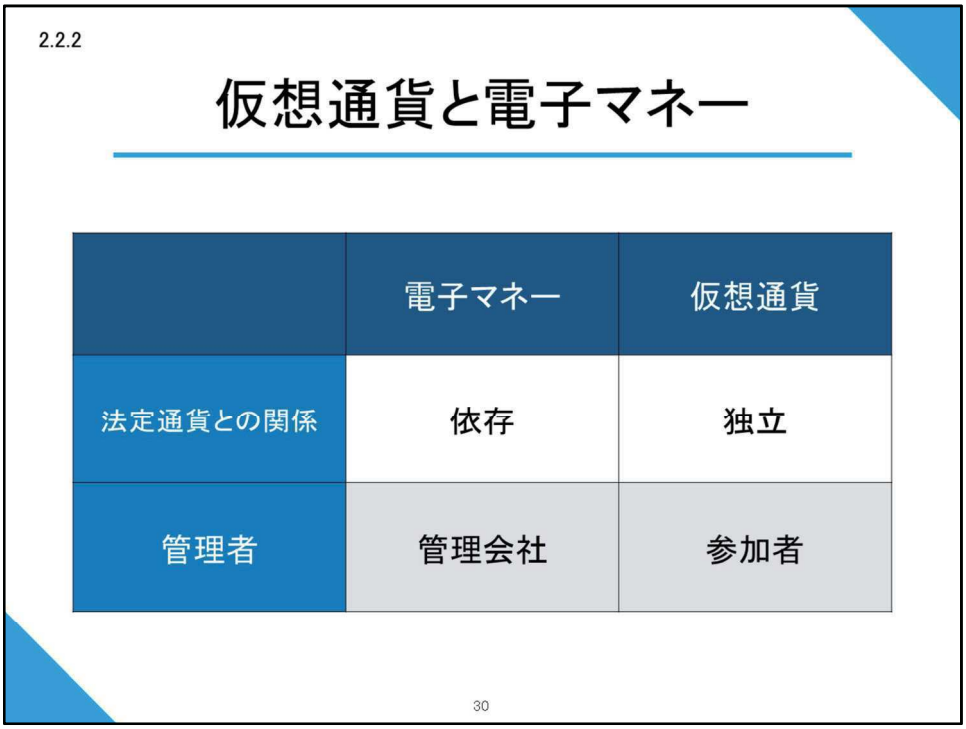
法定通貨は通貨の発行者である国により管理が行われている。仮想通貨は管理者に依存することなく、参加者により自律的に管理が行われる。

- **通貨の新規発行**

法定通貨は経済状況や流通している通貨量などを考慮して、国により発行量が決められる。仮想通貨は通貨の価値などに関係なく、一定時間ごとにあらかじめ定められた額が発行される。

- **信頼**

通貨の価値は、通貨の発行主体に対する信頼により担保される。法定通貨はその発行主体である国に対する信頼を担保に価値を持っている。一方で仮想通貨は、その仕組みを実現しているブロックチェーンをはじめとした技術に対する信頼を担保に価値を持っている。



仮想通貨と電子マネーの共通点

- 仮想通貨も電子マネーも物質として存在するのではなく、取引の記録が台帳に記録されることで価値の移転が行われる。

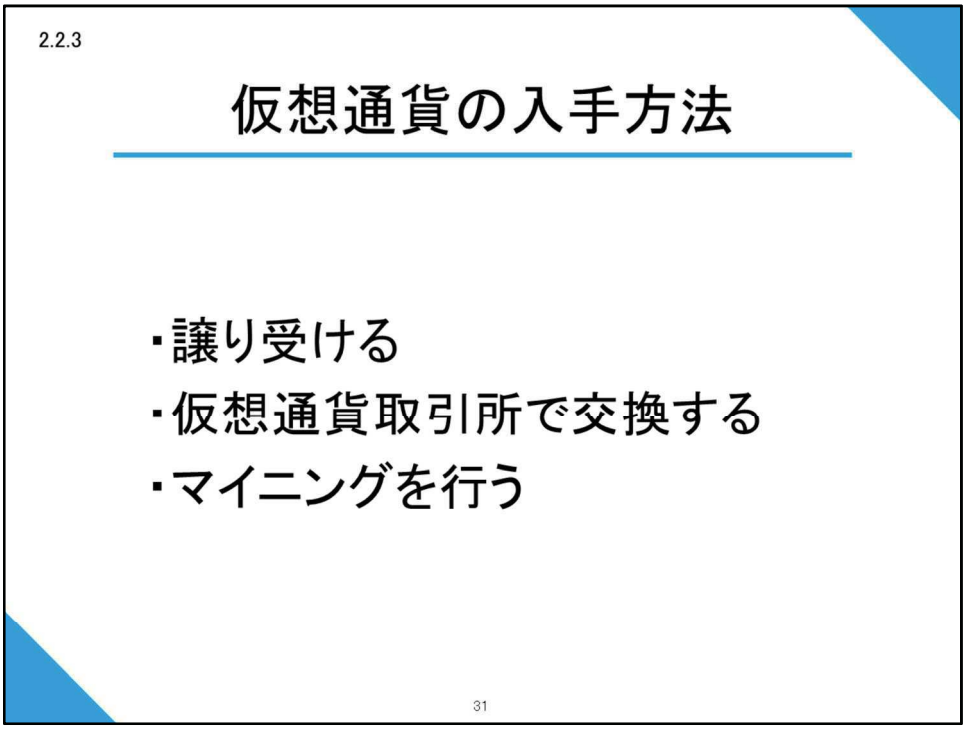
仮想通貨と電子マネーの相違点

- 法定通貨との関係

電子マネーは法定通貨に依存し、決済を便利に行うための「代替通貨」であると言うことができる。suicaを例にすると、suicaに日本円をチャージする際には1円あたり1ポイントのレートとなっており、このレートが変更されることは基本的にはない。
BitcoinやEthereumを始めとした仮想通貨は一般的には法定通貨には依存していない。そのため、価値も自由に変動する。仮想通貨の一部には特定の通貨と価値の連動するStableCoinと呼ばれるものもある。

- 管理者の有無

私たちが利用している様々な電子マネーは、それぞれに管理企業が存在する。これに対して、仮想通貨には管理者が存在しない。



- 譲り受ける

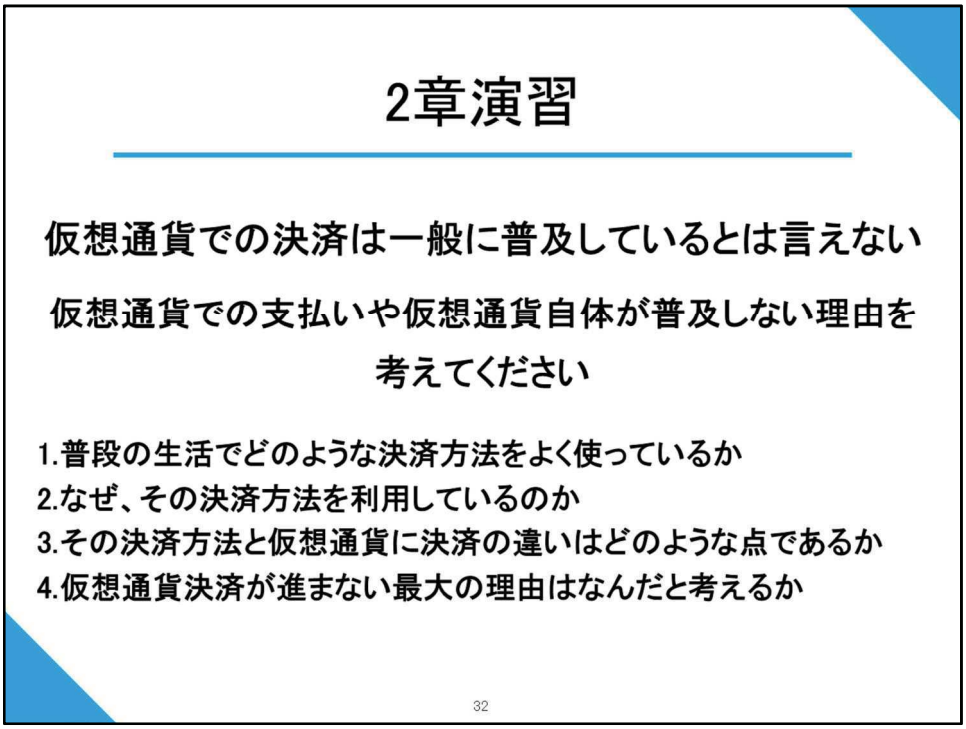
既に仮想通貨を持っている人から譲ってもらう方法。仮想通貨を保有するためには、銀行口座のような「アドレス」というものを準備する必要がある。アドレスはアプリやwebサイトで簡単に作ることができる。

- 仮想通貨取引所で交換する

法定通貨と仮想通貨を交換することで仮想通貨を入手する。仮想通貨取引所では、仮想通貨と法定通貨の交換だけでなく、仮想通貨同士の交換も行うことができる。取引所で口座を開設するためには身分証などでの身分確認が必要になるため、少し手間がかかる。

- マイニングを行う

既に流通している通貨を入手するのではなく、ブロックチェーンのシステムに貢献することで、その対価として仮想通貨をもらうことができる。マイニングに関しては6章で詳しい説明を行う。



発表の形式

- 普段の生活でどのような決済方法をよく使っているか　→　現金
- なぜ、その決済方法を利用しているのか　→　他の決済方法に比べて～～～であるから
- その決済方法と仮想通貨による決済の違いはどのような点であるか　→　他の決済方法は～～～であるが、現金は～～～である。ただし、～～～という難点もある。
- 仮想通貨決済が進まない最大の理由はなんだと考えるか　→　仮想通貨の～～～という特徴により、～～～～という問題があるため普及しないのではないか

正答例

- 日常の決済にはsuicaを頻繁に利用しています。理由としてはお金を持ち歩くことなく、様々な場所で決済を行うことができるためです。また、様々な場所でポイントのチェージをすることができる点も大きな魅力の1つです。これに対して仮想通貨は、利用することのできる場所が少なく、取引所から購入する際にも身分の証明が必要になるなど、手間がかかる点が不自由であると考えます。

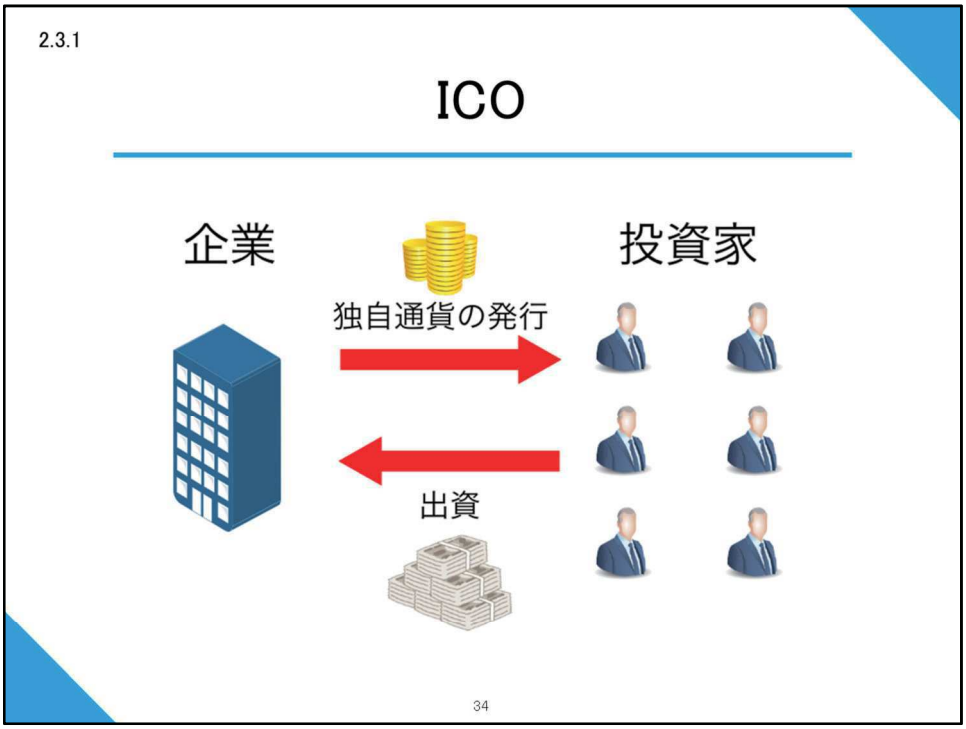
ICOとSTOは仮想通貨を用いた新しい資金調達法であり、仮想通貨が注目される1つの要因となった。

- **ICOについて**

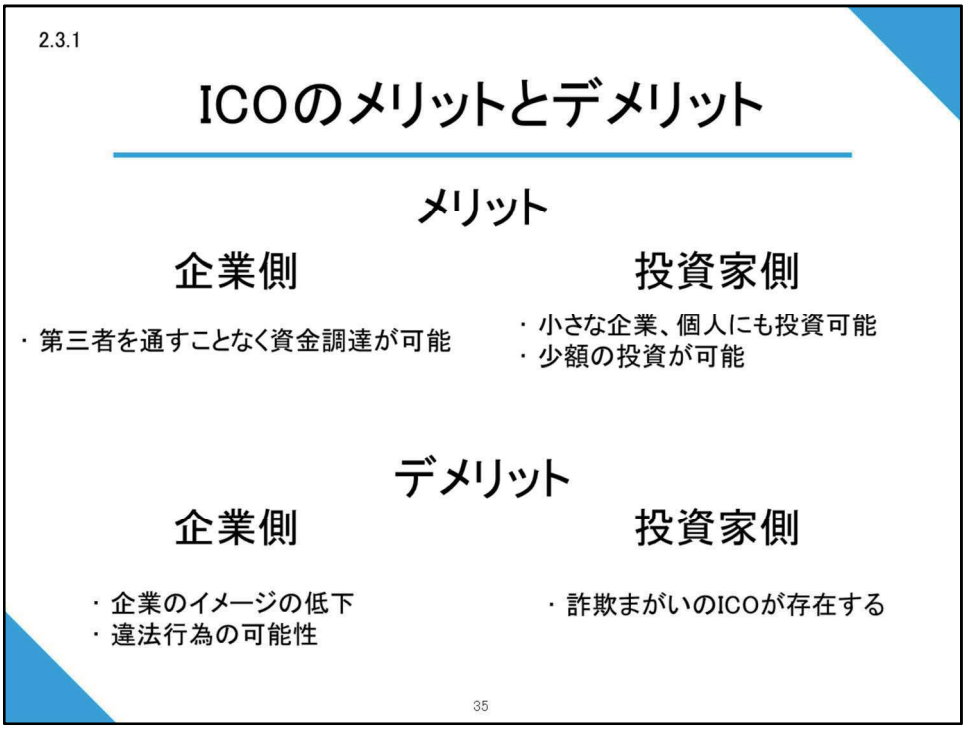
日本語で「新規仮想通貨公開」と呼ばれ、企業の立ち上げや新たな事業を始める際に資金の調達を行うための仕組みやその行為自体の事を言う。

- **STOについて**

資金調達の仕組みであることは、ICOと変わらないが、発行されるトークンが証券としての条件を満たす点が異なる。



- 事業を始めるために資金調達がしたい企業が独自のトークンを発行する。
- 投資家にそれらを売り出し、資金を集める。
- ICOで売り出されたトークンは、出資が行われた企業や事業により提供されるサービスに利用することができる。また、事業が成長しサービスの利用者が増えるとトークンの価値が上がり、投資家はトークンの売却により利益を得ることもできる。



企業側のメリット

ICOでは証券会社などの第三者機関を通すことなく資金の調達が可能であり、仲介者を省くことにより取引の手数料を抑えることができる。また、証券取引所で株を扱ってもらえない、小さな企業でも資金を調達することができる。

投資家側のメリット

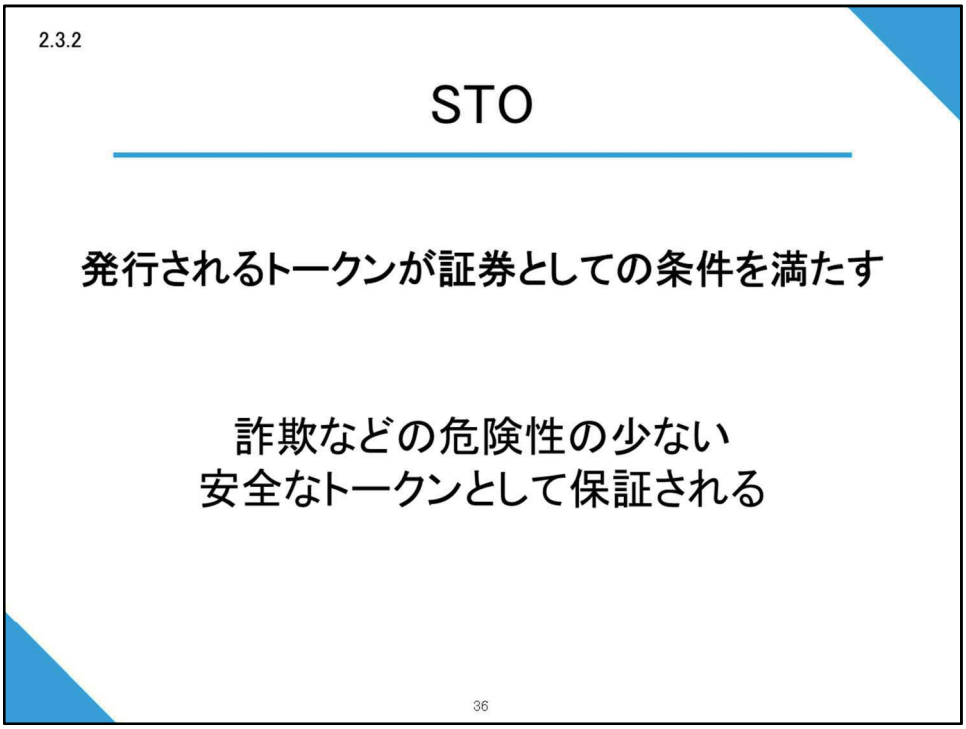
証券取引所への上場が難しい小さな企業や、個人にも投資することができ、少額から気軽に投資を行うことできる。

企業側のデメリット

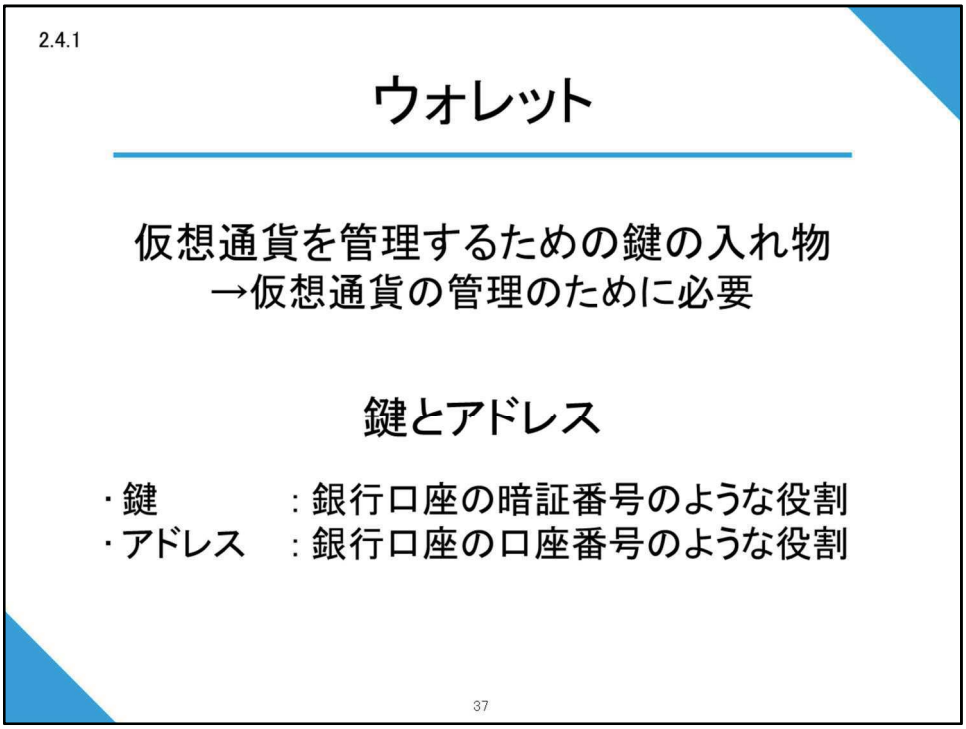
ICOはまだ社会に浸透した仕組みであるとは言えず、ICOを行うことにより企業のイメージが低下する可能性がある。2019年現在ICOに関する法律は整備されていない部分が多いのが現状であり、法律や税務に関連した予期しないトラブルに巻き込まれる可能性がある。

投資家側のデメリット

企業に対しての第三者機関による審査がなく誰でも行う事ができることから、資金の持ち逃げや詐欺まがいのICOが存在する。投資を行う際には企業が出す事業の計画書をよく読み、自己責任で行う必要がある。



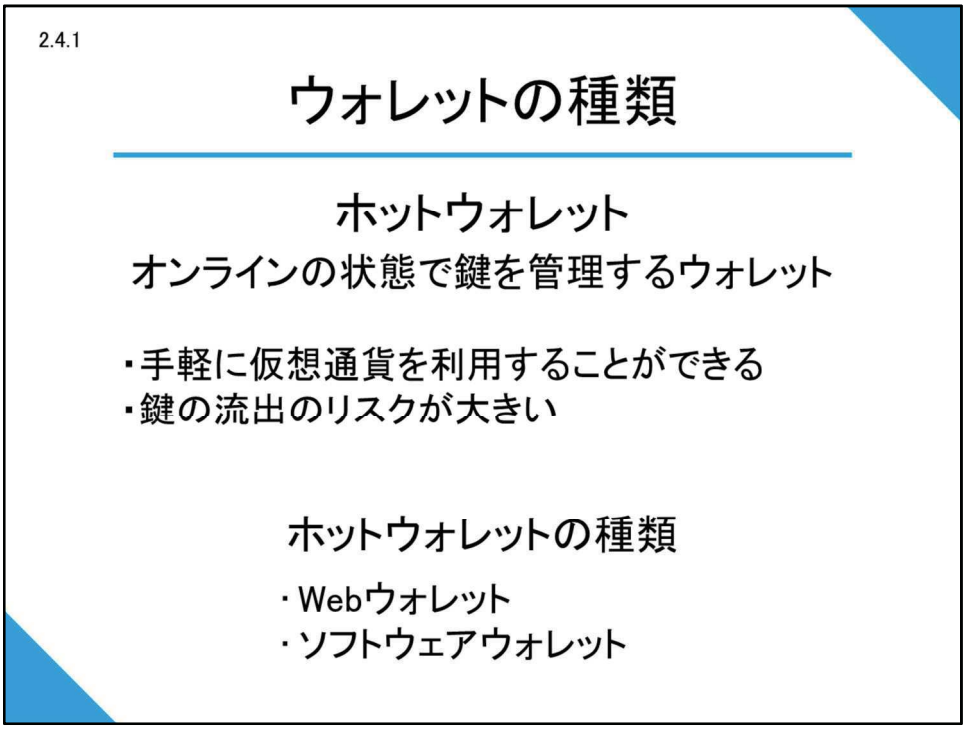
- ICOと同じ企業の資金の調達方法の1つ。
- 詐欺などの危険性の少ない安全なトークンとして保証される点がICOと異なる。
- 証券としての条件を満たす事で気軽なトークンの発行はできないが、詐欺などの危険性の少ない安全なトークンとして保証される。



- ウォレットは、仮想通貨を管理するための「鍵」の管理を行う。鍵とは所有する通貨を利用する際に必要な文字列であり、鍵から「アドレス」という文字列が作成される。

- 「鍵」と「アドレス」をそれぞれを身近なものに例えると、”鍵”は銀行口座の”暗証番号、”アドレス”は銀行口座の”口座番号″である。2つ揃っていないと通貨を利用することができない。

- 銀行口座の暗証番号を忘れた際には、身分の照会などを行うことで、暗証番号の再発行を行なってもらうことができるが、仮想通貨は管理者が存在しないため、再発行を行なっている機関は存在しない。このような理由から鍵の管理には細心の注意を払わなければならない。



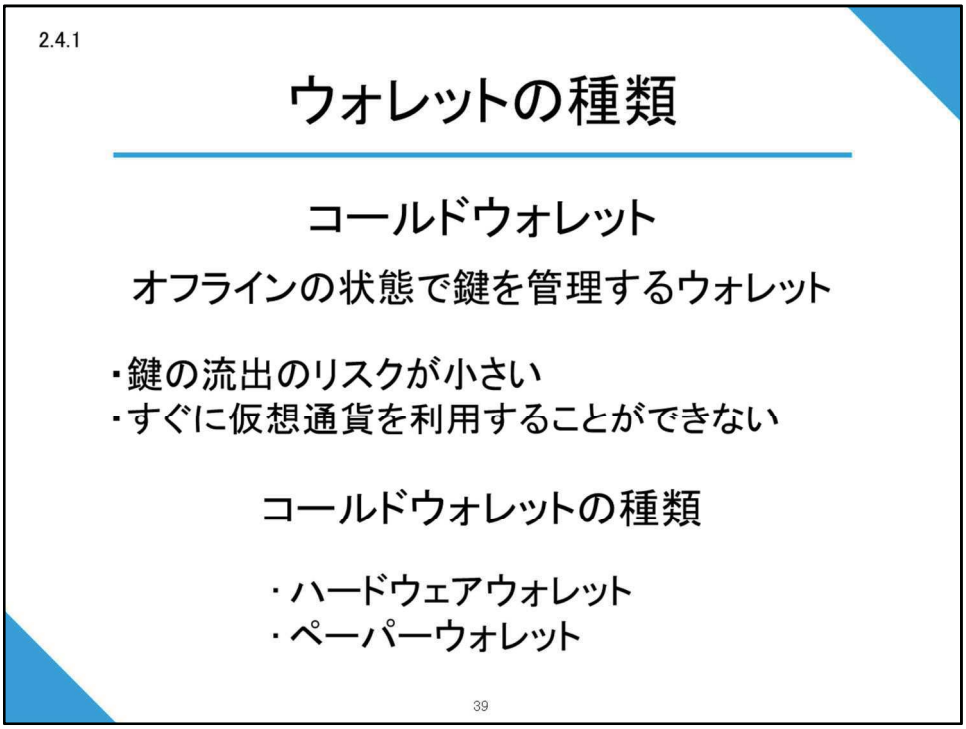
ウォレットには鍵の保管方法が異なる複数の種類が存在する。

ホットウォレット

- オンライン状態で鍵を保存するウォレット
- オンラインで鍵を管理しているので素早く通貨の送金などを行うことができる。
- オンラインにあることでサイバー攻撃などで鍵が流出する可能性がある。鍵が流出すると、その鍵に紐づいたアドレスで管理していた通貨は流出してしまう。

ホットウォレットの種類

- ウォレット機能を提供するwebサービスであるwebウォレットや、ソフトウェアとして提供されるソフトウェアウォレットがある。



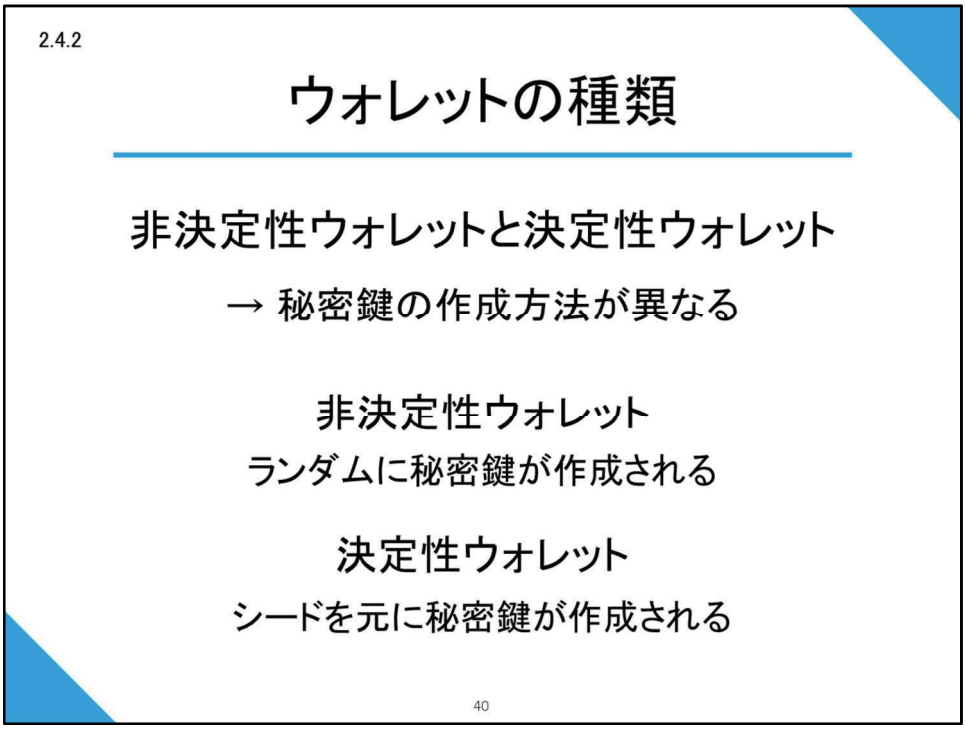
コールドウォレット

- オフラインの状態で保存するウォレット
- 鍵を利用する時だけ、オンラインにするので鍵の流出の可能性は低い。
- オフラインで保存しているので、ホットウォレットに比べると、利用までに時間がかかる。
- コールドウォレットは鍵の管理を自身で行うため、細心の注意を払う必要がある。

コールドウォレットの種類

- 鍵を管理するための専用のデバイスに保存するハードウェアウォレット
- 鍵を紙に書いて保存するペーパーウォレット
- 鍵を覚えて管理するブレインウォレット

- ハードウェアウォレット、ペーパーウォレットには物理的な盗難、紛失、破損の可能性があるので注意する必要がある
- ペーパーウォレットは普通の紙に書いて鍵を保存しても良いが、鍵を関するための専用の紙も販売されている。



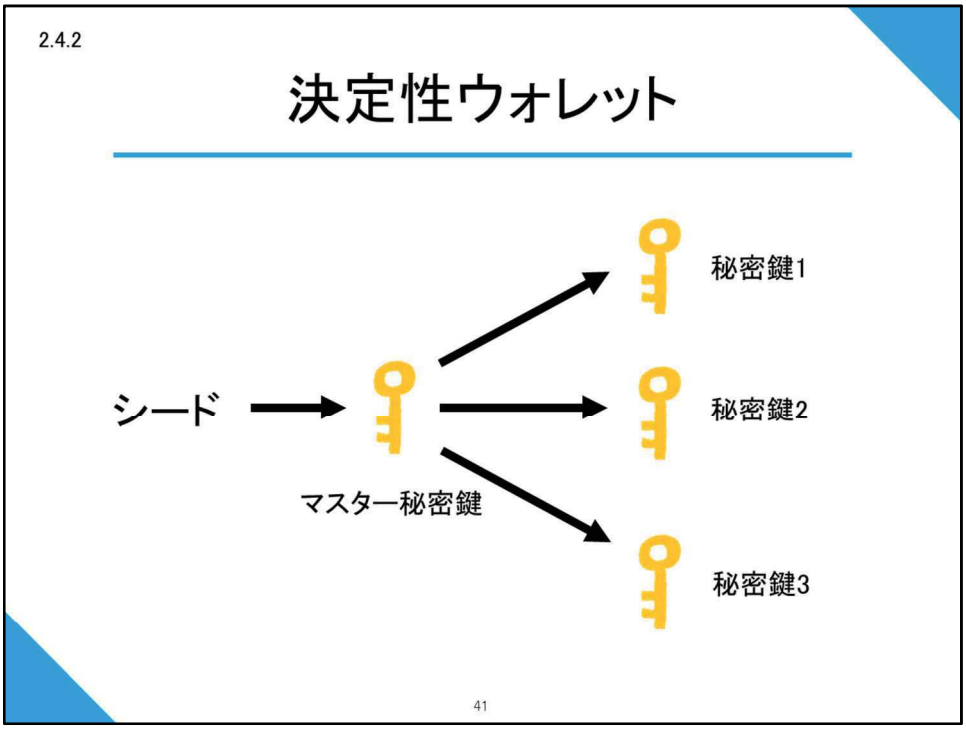
ウォレットは「非決定性ウォレット」と「決定性ウォレット」に分類することもできる。これらは秘密鍵の作成のプロセスが異なる。

非決定性ウォレット

- ランダムに秘密鍵が作成される。
- 鍵同士に関連はないので、作成した全ての鍵を管理しなければならない。

決定性ウォレット

- シードと呼ばれる値を元に複数の秘密鍵が作成される。



決定性ウォレットの鍵の作成について

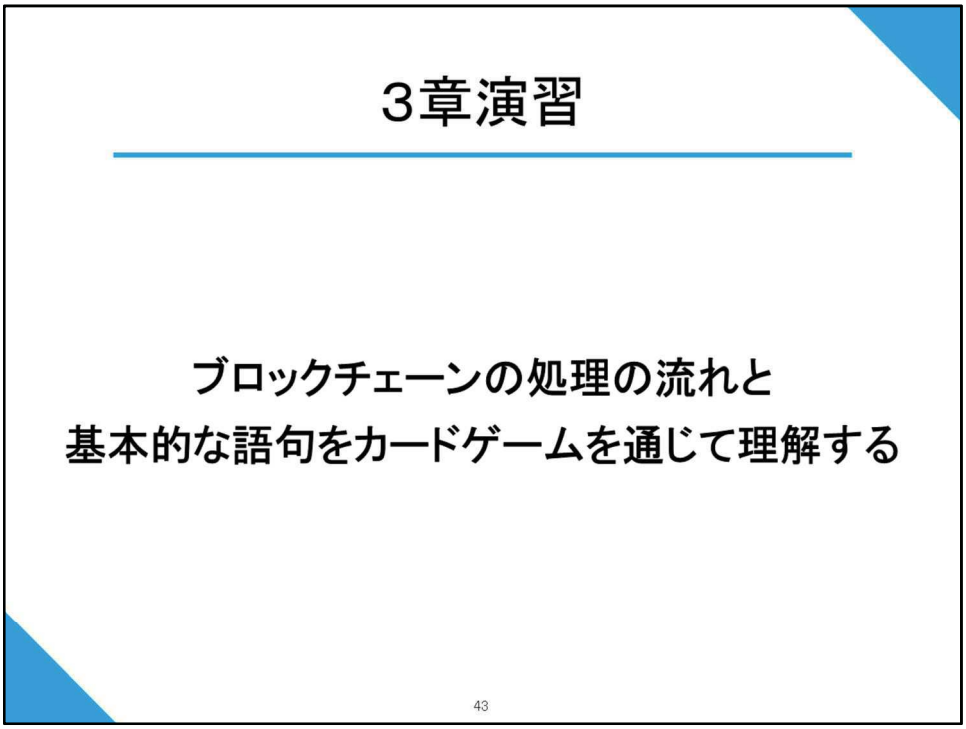
- 「シード」と呼ばれる文字列からランダムに生成された1つの数値を元に多数の鍵が作成される
- 全ての鍵を管理する必要はなく、シードから全ての鍵の情報を復元することができる。

ニーモニックコード

- シードを「Mnemonic Code」と呼ばれる12から24個の英単語で表す。
- ランダムな文字列に比べて、英単語の方が可読性が高く、転写のミスが少ないためこのような方法がとられる。

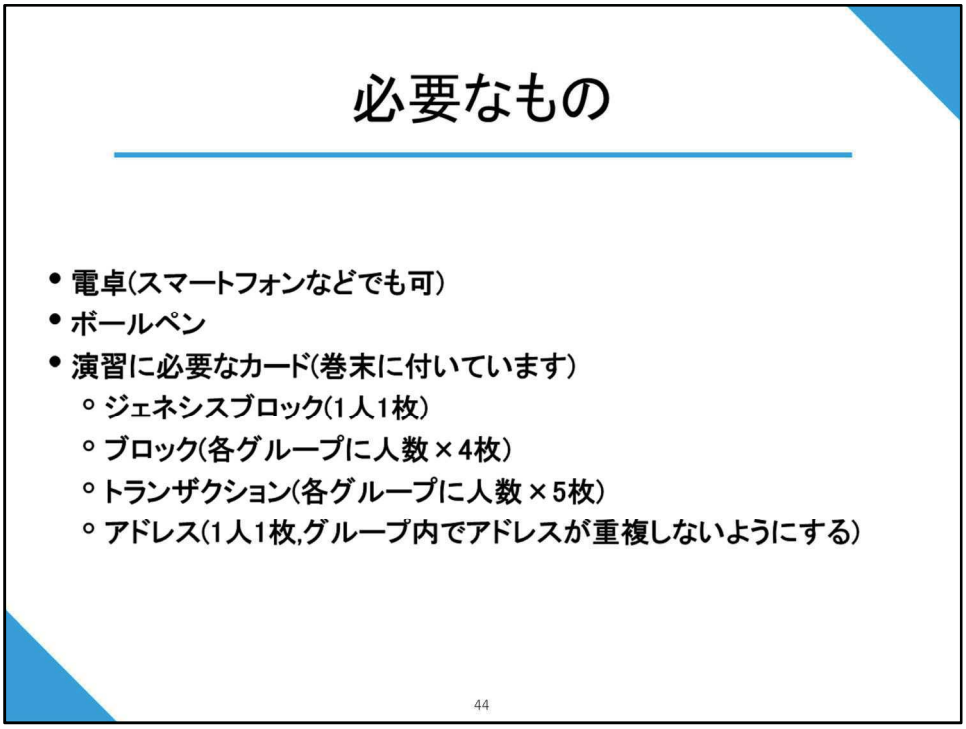
3. ブロックチェーンの構成要素

42

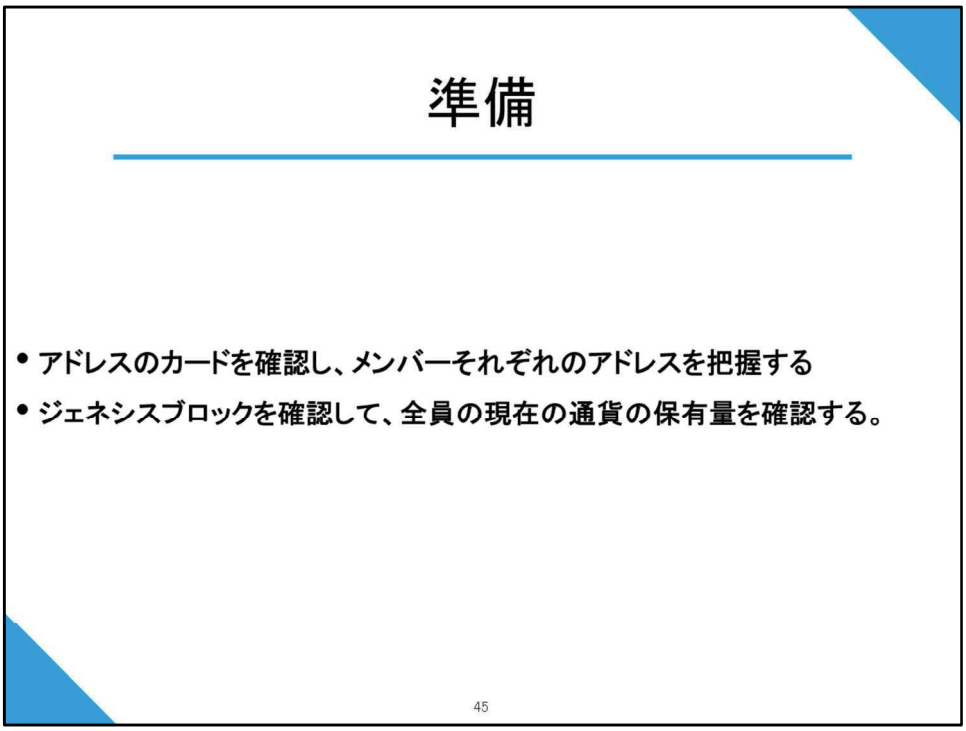


ブロックチェーンの処理の流れをカードゲームを通じて理解する

- 4～5人のグループを作成する。



巻末のブロックチェーンゲームのためのカードを事前に印刷しておき、このタイミングで配布する。



- 自身に配布されたアドレスのカードから、自身に割り振られたアドレスを確認する。
- 確認が終わるとグループ全体で全員のアドレスを共有する。
- このゲームではブロックが通貨の取引の記録が書かれた台帳として機能する。
- 配布されたジェネシスブロックから全員が保有している通貨の額を確認する。
- このテキストではアドレス10が100BTC所有していることを確認できる。

ジェネシスブロックの確認

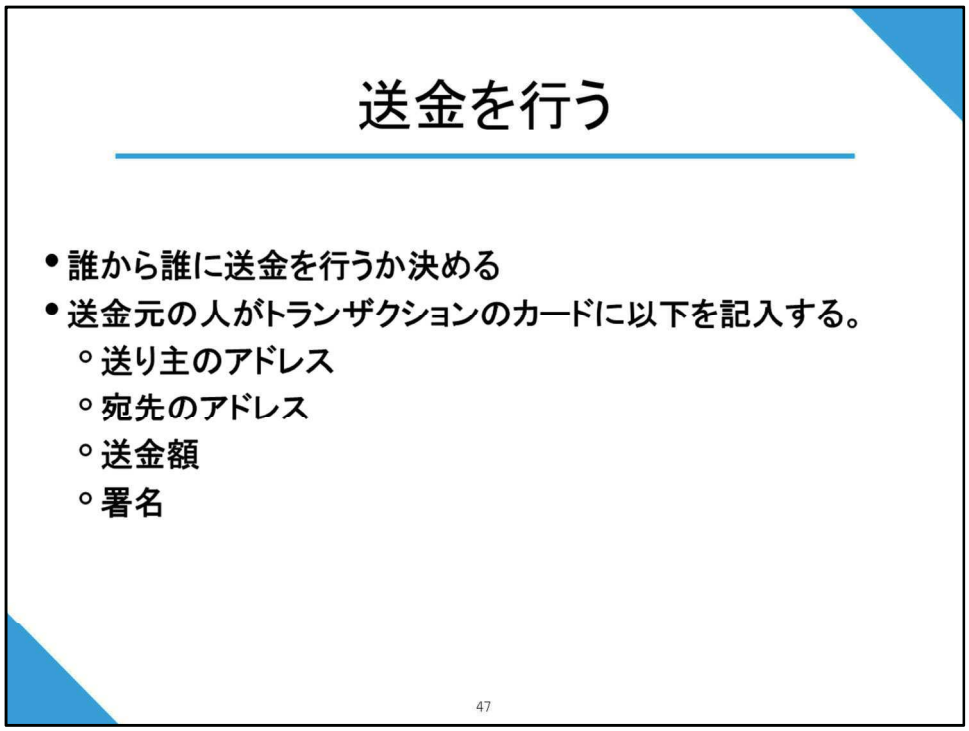
ジェネシスブロック

このブロックの合計値	131	①	2,248,091 ①の3乗
前のブロックの合計値	0		②
ナンス	21		③
送り主	宛先		送金額(BTC)
新規発行通貨	10	④	100 ⑤
⑥		⑦	⑧
⑨		⑩	⑪
⑫		⑬	⑭

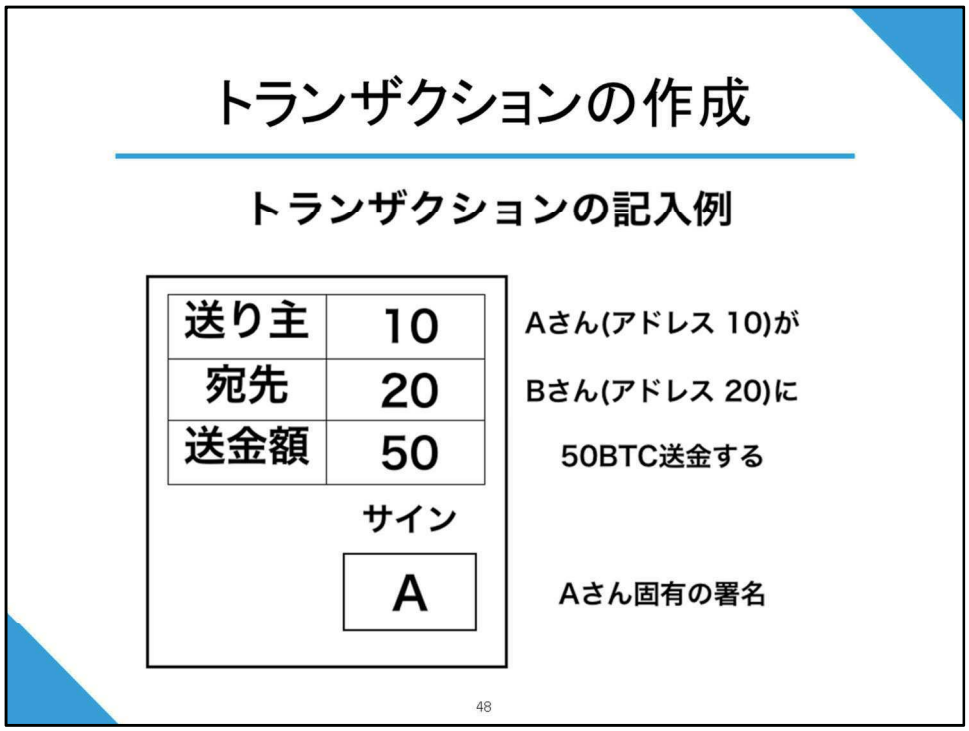
計算スペース

ここから誰がいくら持っているか確認する

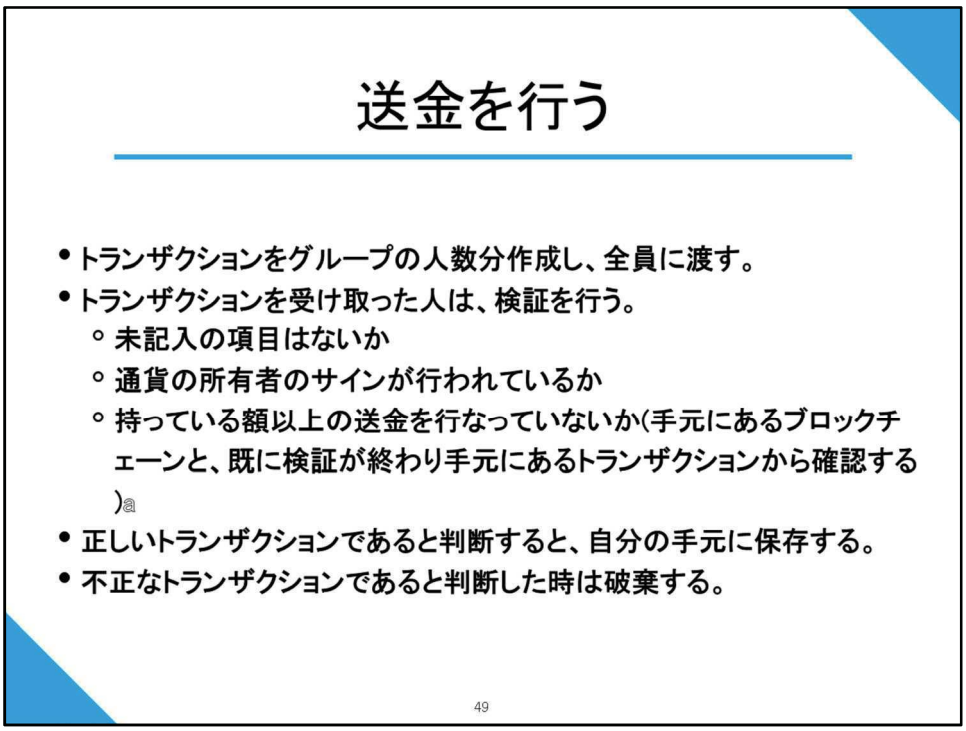
46



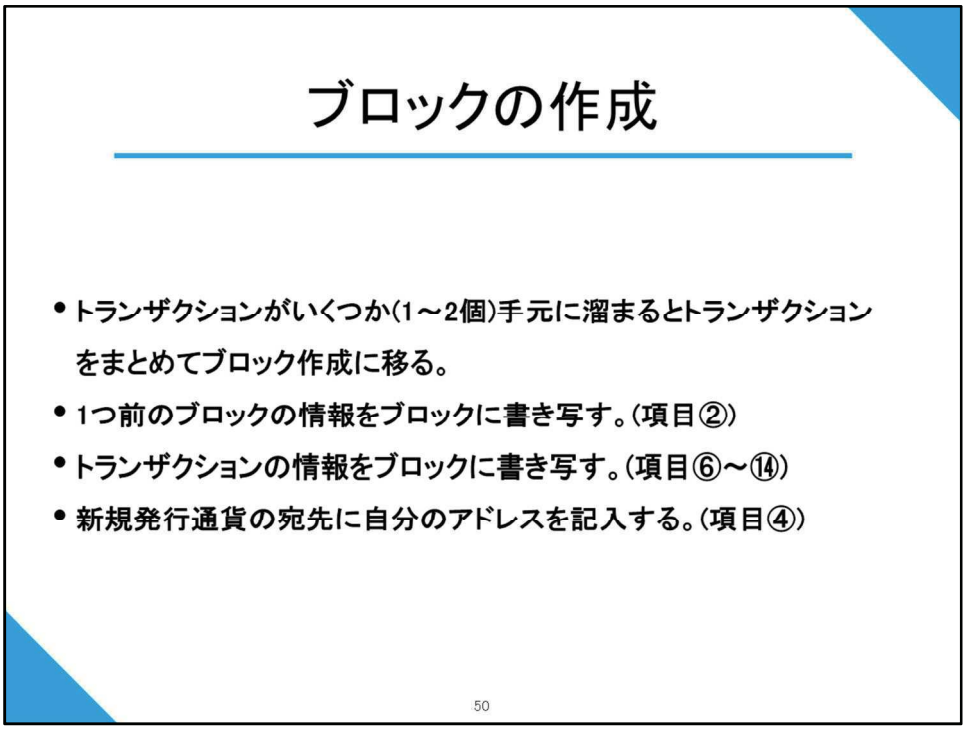
- 送金作業を行う。
- 初めに送金することができるのは、通貨を所有しているAさんのみである。
- トランザクションの記入方法は次のスライドで示す。



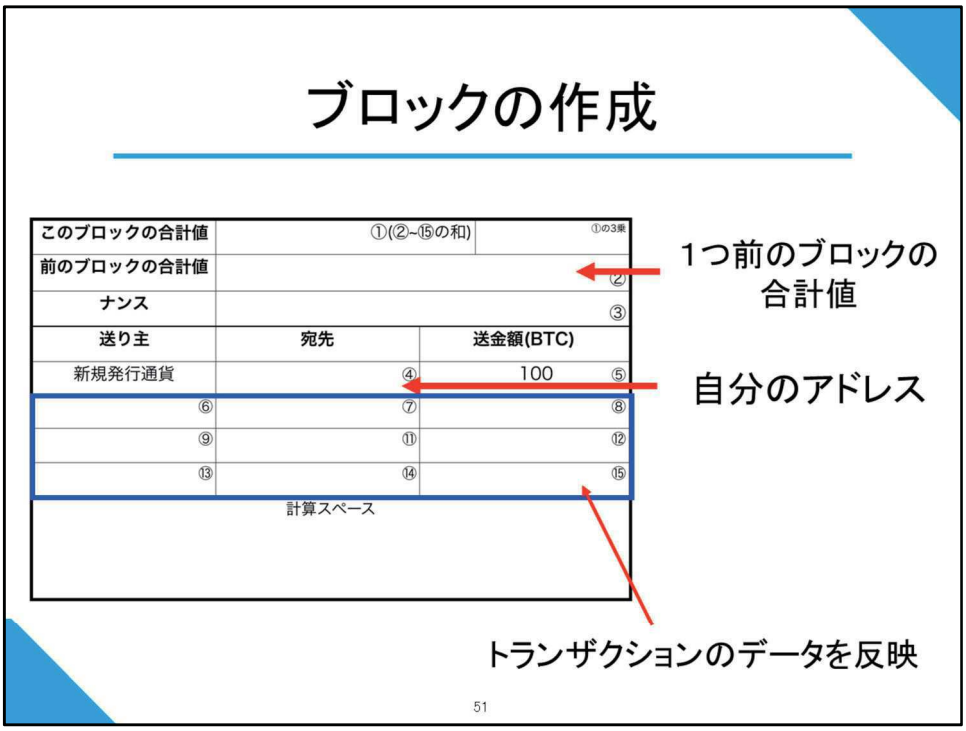
- AさんがBさんに50BTC送金するトランザクションを例に示す。
- サインの欄にはAさんがトランザクションを発行したことが確認できるようにAさん固有のサインを行う。



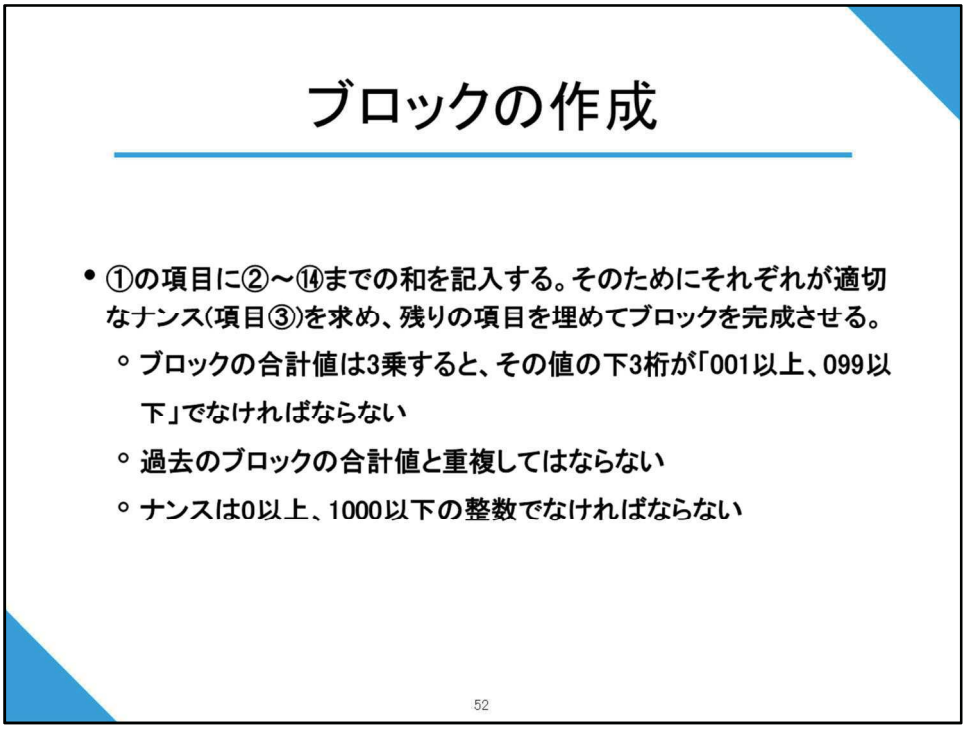
- トランザクションはグループの人数分発行を行う。
- トランザクションを受け取った人は、そのトランザクションが正当なものであるか検証を行う。検証の項目については、スライドに記述してある。
- 検証の結果正しいトランザクションであると判断すると、そのトランザクションは手元に保存しておく。
- 仮に不正なトランザクションであると判断した場合には、そのトランザクションを破棄し、破棄したことをトランザクションの発行者に通知する。



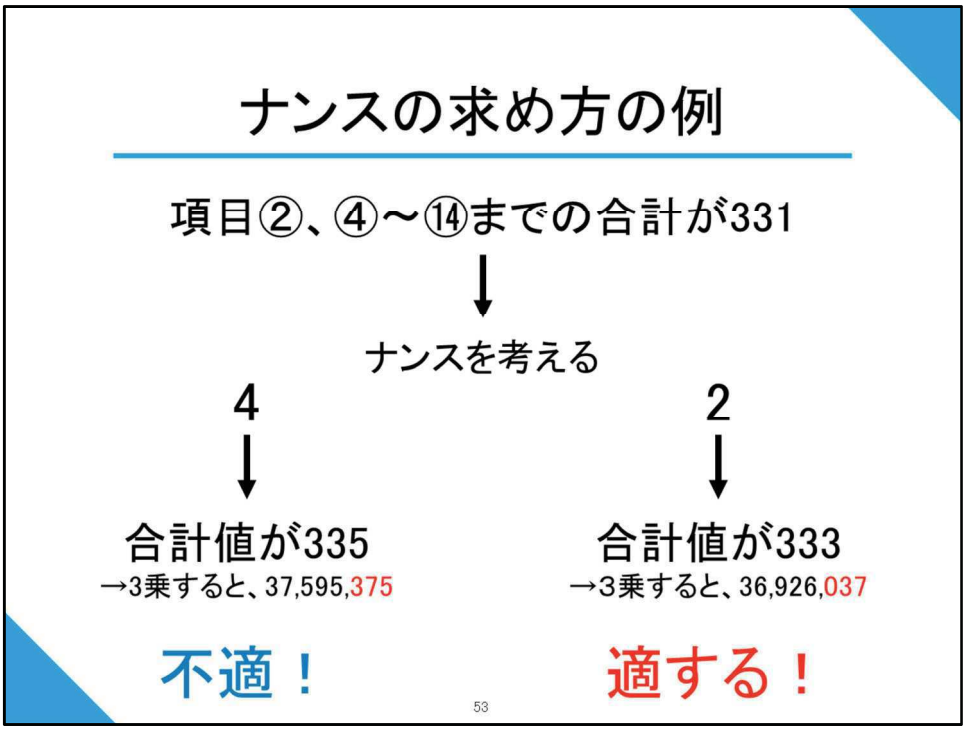
- 数回取引を行い、トランザクションが複数手元に溜まると、グループ全員がブロックの作成作業に入る。
- 一つの前に作ったブロックの情報を作成するブロックに書き写す。作成するブロックが一つ目であれば、ジェネシスブロックを参照する。
- 手元に保存しているトランザクションの情報をブロックに書き写す。
- 新規発行通貨の宛先の欄に自身のアドレスを記録する。
- ここまでのブロックの作成方法については、次のスライドに具体例を示す。



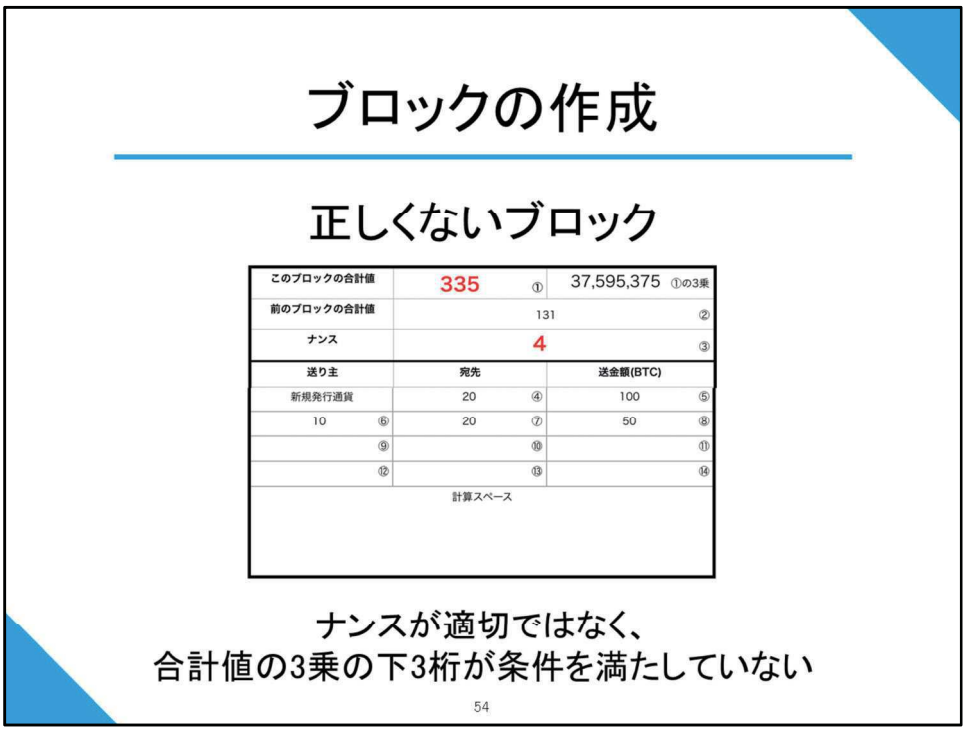
- ここまでに説明したブロックの作成方法について
- 手元に保存していたトランザクションの数によって、トランザクションの項目をどこまで埋めるかは変わってくる。



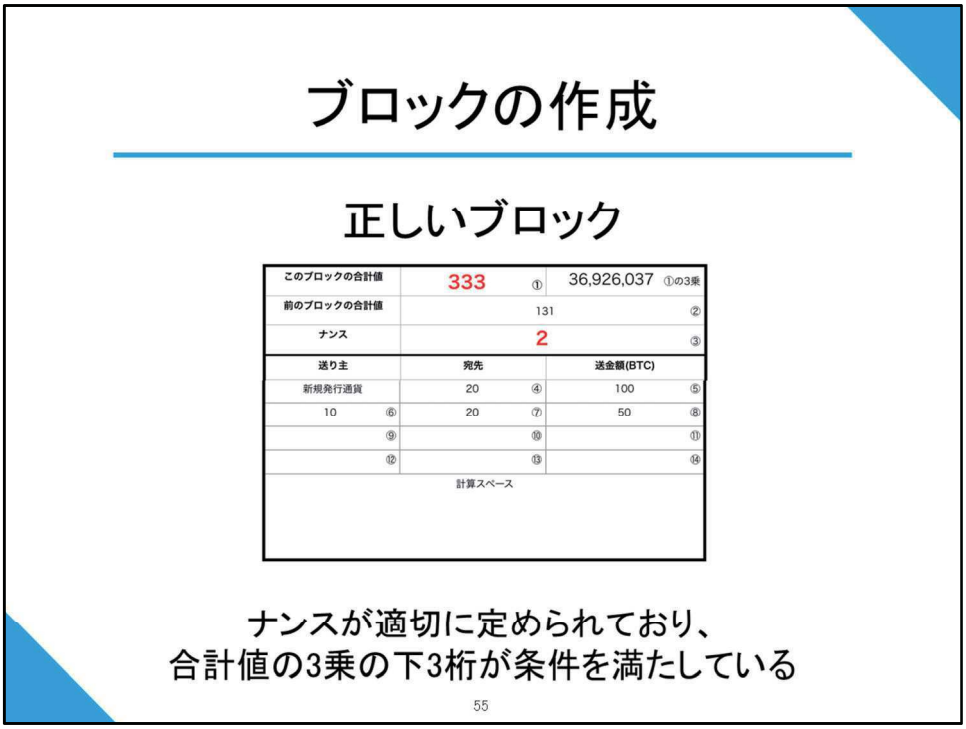
- ブロックの項目①に項目②から⑭までに記入されている数字の和を計算して記入する。ブロックの合計値はスライドに示されている条件を満たす必要がある。



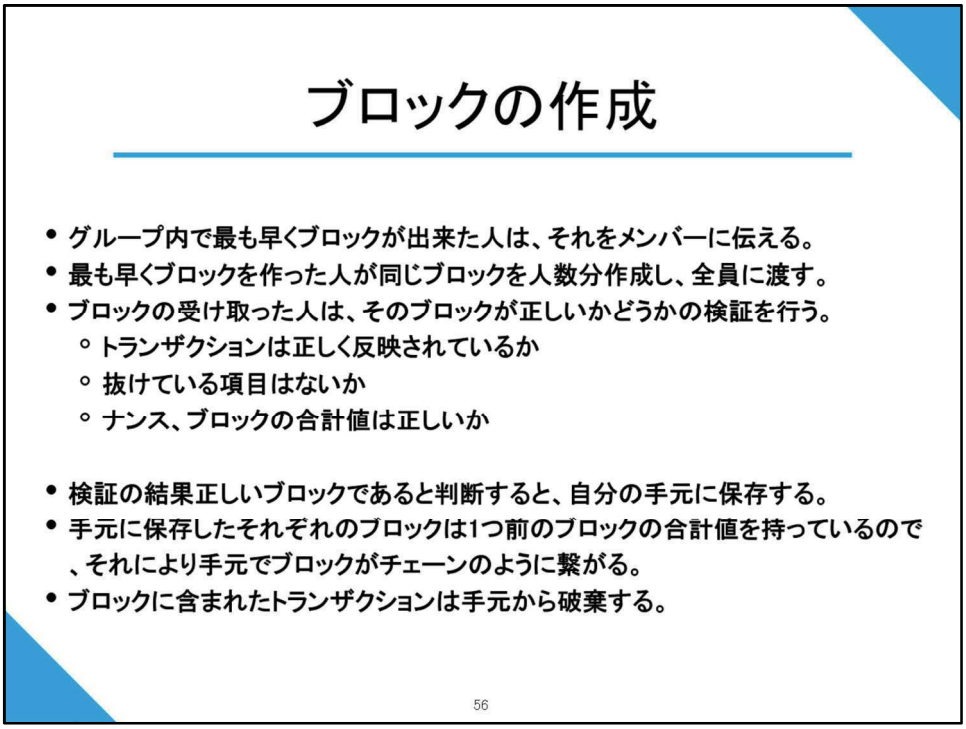
- ブロック合計値の計算の際に、ナンスを求める必要がある。
- ナンスの求め方をテキストの具体例に従って、スライドで説明する。



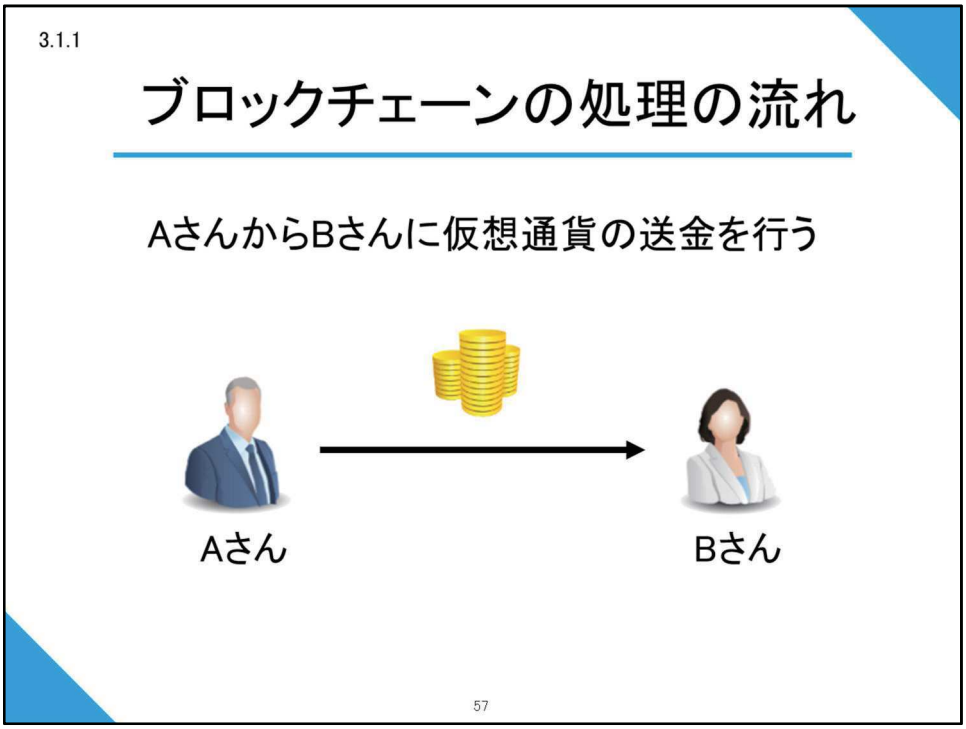
4というナンスを試し、計算すると合計の3乗の値の下3桁が375となり、これはブロックの作成条件に当てはまらないので、このナンスは不適である。



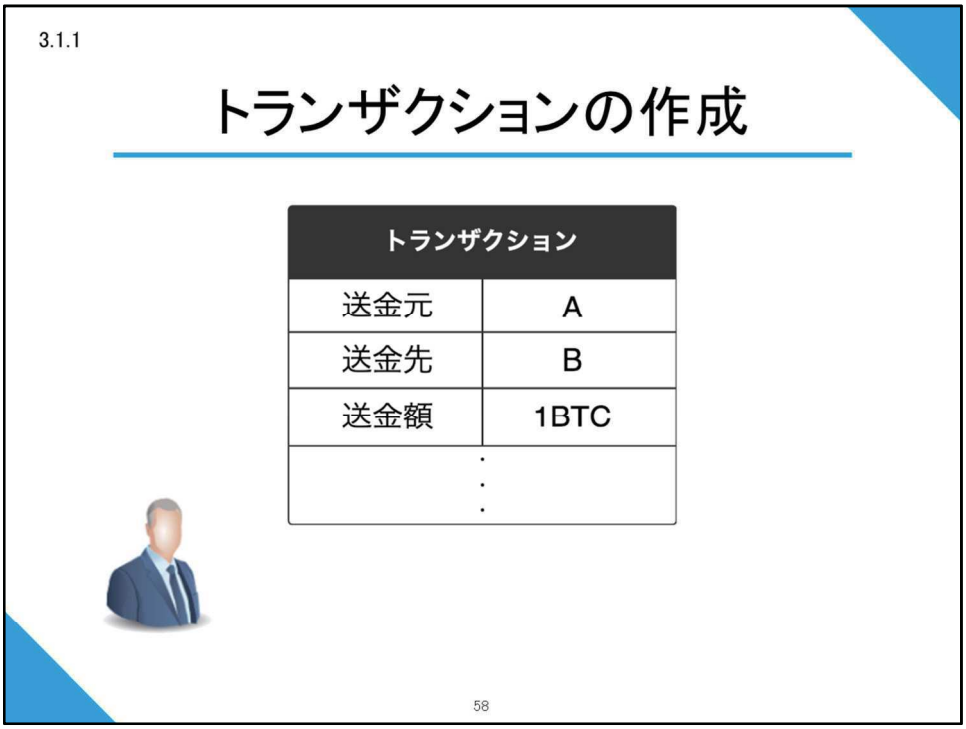
- ナンスに2を試し、計算するとブロックの合計値の3乗の値の下3桁が037となり、これはブロックの作成条件に当てはまり、ブロックの作成が完了する。



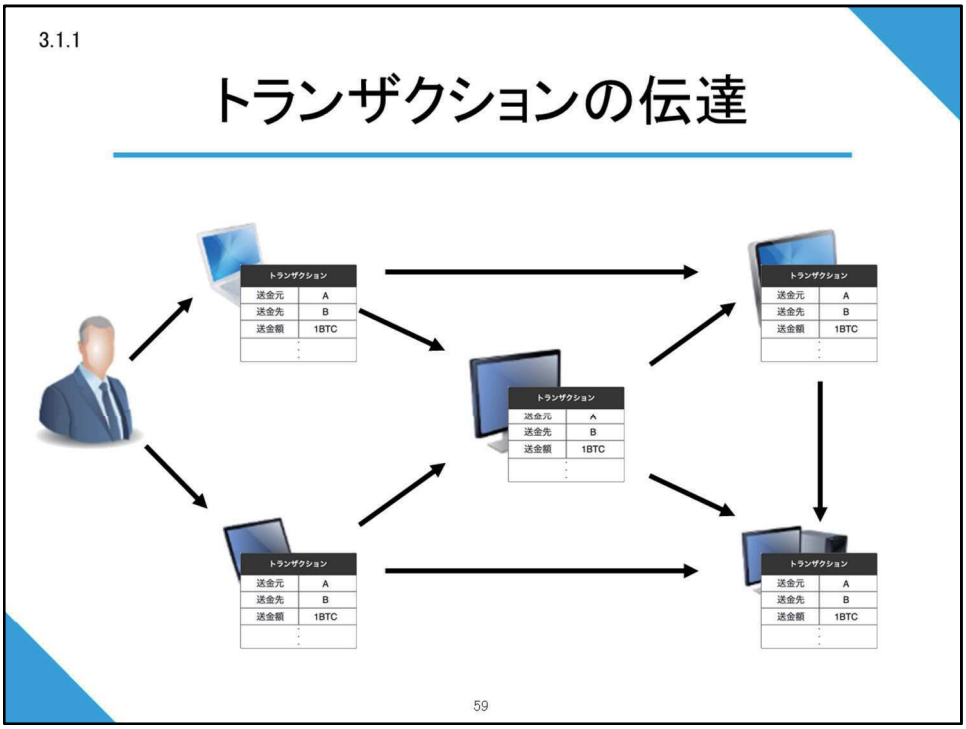
- ナンスの繰り返し計算を終えて、ブロックが完成すると、トランザクションの時と同様に、人数分ブロックを複製し全員に配布する。
- ブロックを受け取ると、ブロックの検証作業を行い、正しいブロックであると判断すると手元に保存し、不正なブロックであると判断すると破棄し、再度ナンスの計算作業に戻る。



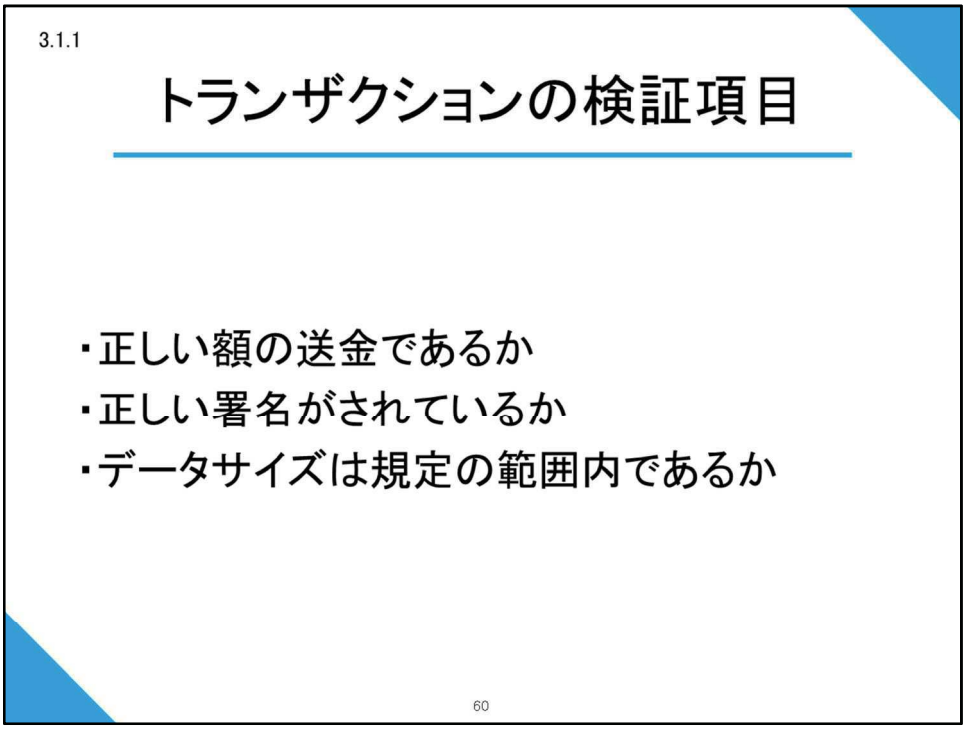
AさんからBさんへ仮想通貨を送金することを例にして、ブロックチェーンの処理の流れについて紹介する。



- Aさんがトランザクションを作成する。
- トランザクションには「誰から」「誰に」「いくら」の送金を行うか記述されている。
- 実際のトランザクションはこれら以外に複数の項目があるが、今回は省略する。
- ブロックチェーンには様々な種類があるが、大半はトランザクションが発行されることから全ての処理が始まる。



- Aさんはトランザクションを作成すると、そのトランザクションをブロックチェーンのネットワークに伝達する。
- ブロックチェーンのネットワークはP2Pネットワークと呼ばれるネットワークで、バケツリレー的にトランザクションは伝達される。中央集権的な機能を果たすサーバーは存在しない。
- トランザクションは誰でも発行することができるため、不正なものが紛れている可能性もある。そのため、トランザクションを受け取ったノードは、そのトランザクションが正当なものであるか自律的に検証作業を行なう。
- 検証作業はクライアントソフトを利用してネットワークに参加した人により行われる。検証作業自体は、ソフトウェアが行う。



トランザクションの検証項目の一例を以下に示す。Bitcoinではトランザクションの検証は20項目程度ある。

- **正しい額の送金であるか**

Aさんが送金額以上の通貨を保有しているかブロックチェーン(台帳)から確認する。

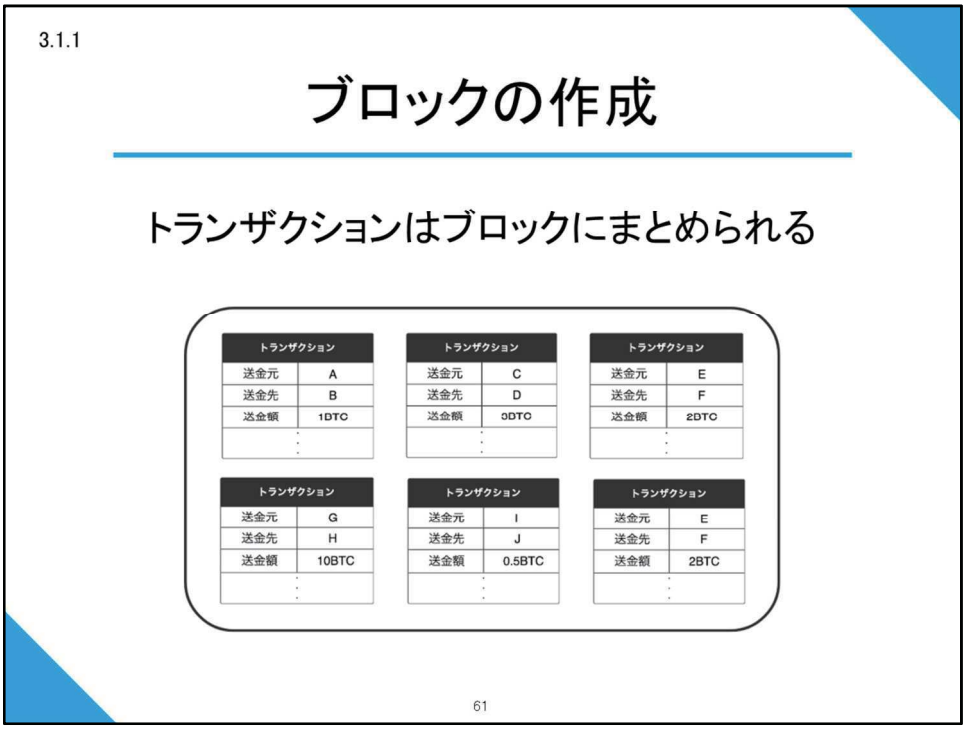
- **正しい署名がされているか**

Aさんが発行したトランザクションであるか署名から確認する。

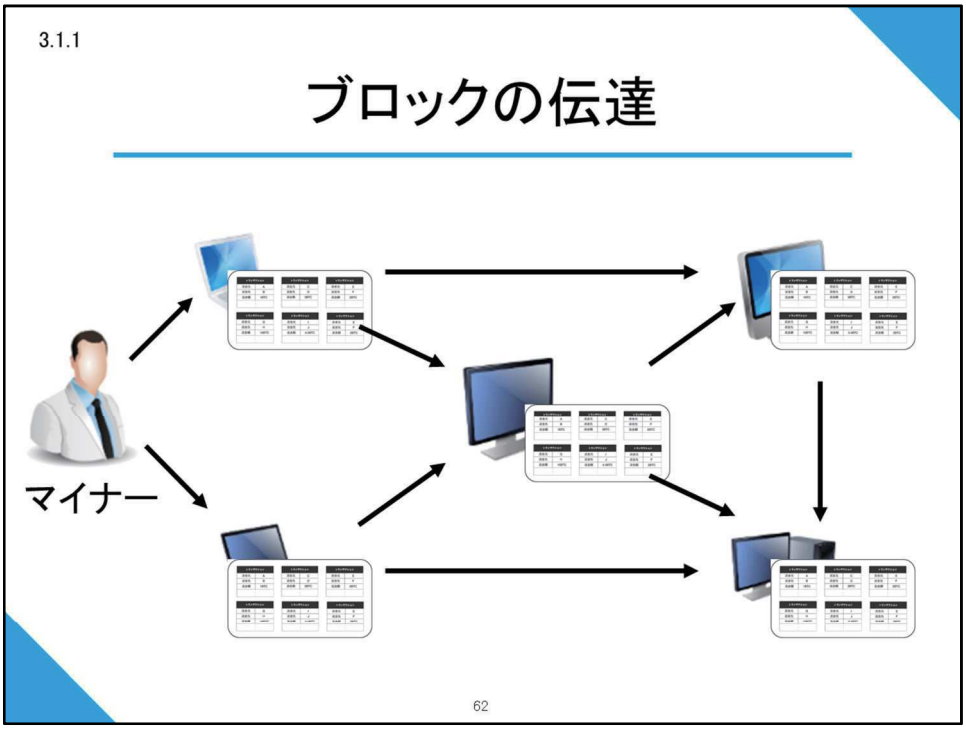
- **データサイズは規定の範囲内であるか**

トランザクションにはデータサイズの規定があるので、この範囲内に収まっているか確認する。

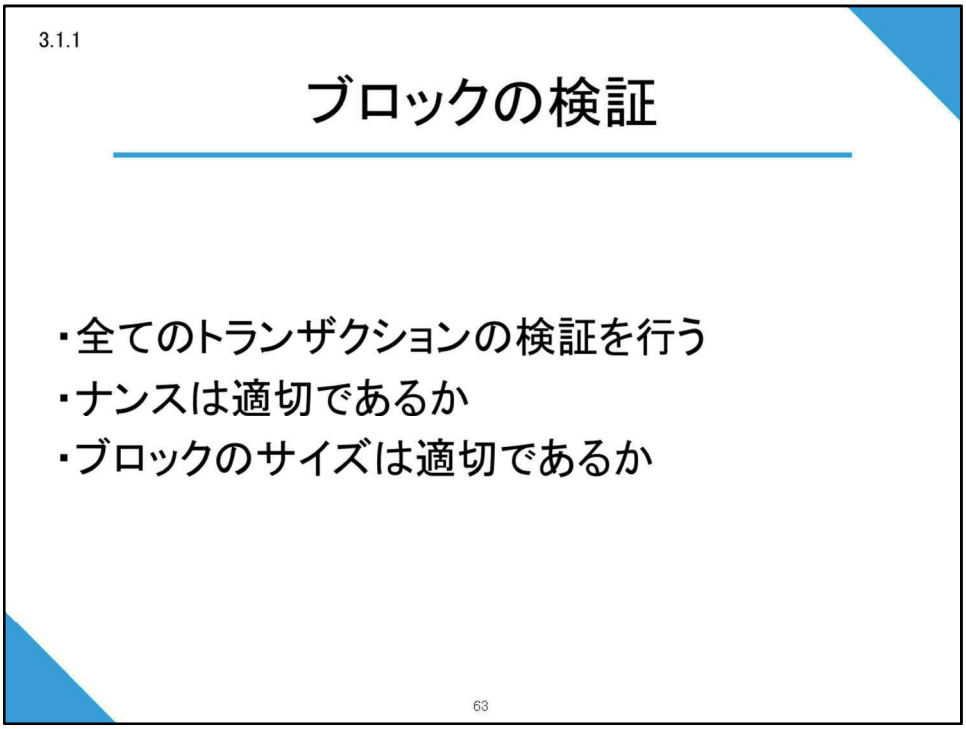
すべての検証クリアしたトランザクションのみが隣のノードに伝達される。検証の過程で不正なトランザクションであると判断されたものは、その場で棄却され、その旨がトランザクションの発行者に通知される。



- 1つのトランザクションが検証伝達されている間にも、次々とトランザクションは発行される。
- Bitcoinでは現在1秒間に2～4件のトランザクションが発行され続けている。次のサイトで、リアルタイムに発行されたトランザクションを確認することができる。
  (https://chainflyer.bitflyer.jp/)
- それぞれのノードはトランザクションを検証し、隣のノードに伝達する際に、自身の手元にもトランザクションを保有しておく。
- 溜まったトランザクションは一定時間ごとに、「ブロック」という単位にまとめられる。
- Bitcoinでは2000～3000個のトラザクションが1つのブロックに含まれている。



- 作成されたブロックはトランザクションと同様にネットワークに伝達される。
- ブロックを受け取ったノードは、そのブロックが正当なものであるか検証作業を行う。



ブロックの検証項目の一例を以下に示す。Bitcoinではトランザクションの検証は20項目程度ある。

- **全てのトランザクションの検証を行う。**

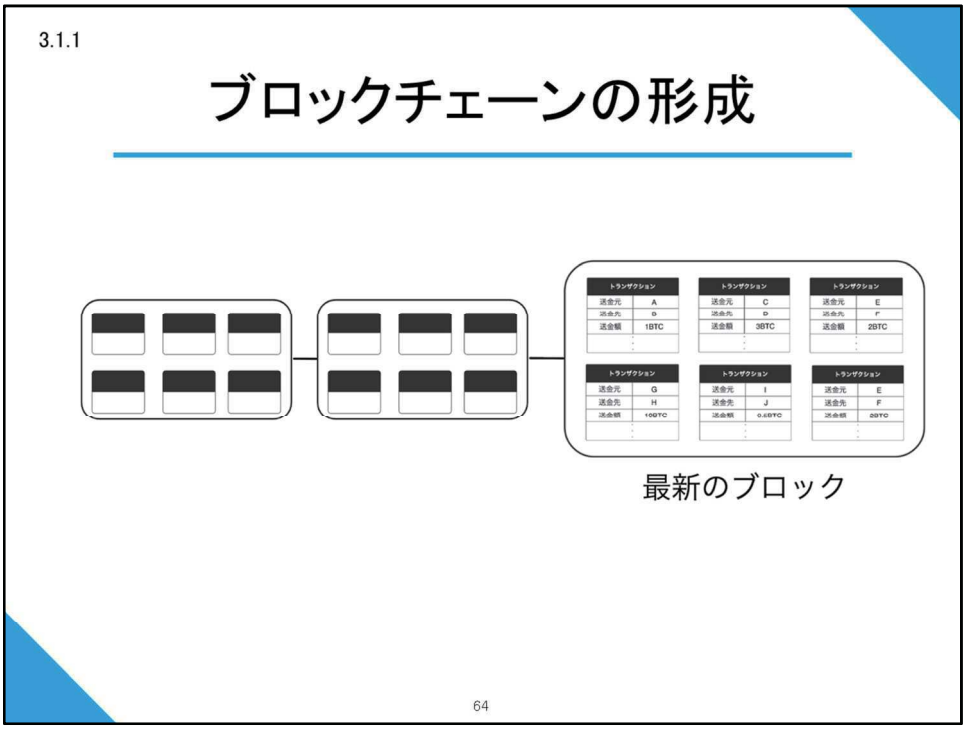
ブロックに含まれているトランザクションがすべて正しいものであるか確認する。

- **ナンスは適切であるか**

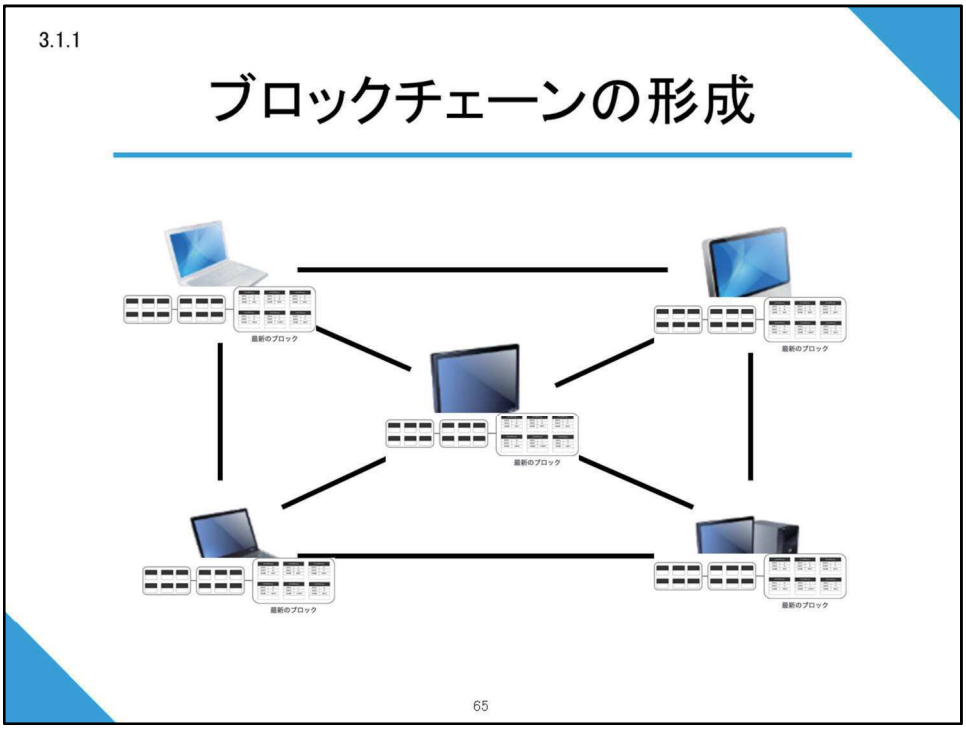
作成されたブロックのナンスが適切なものであるか、計算を行ない確認する。

- **ブロックのサイズは適切であるか**

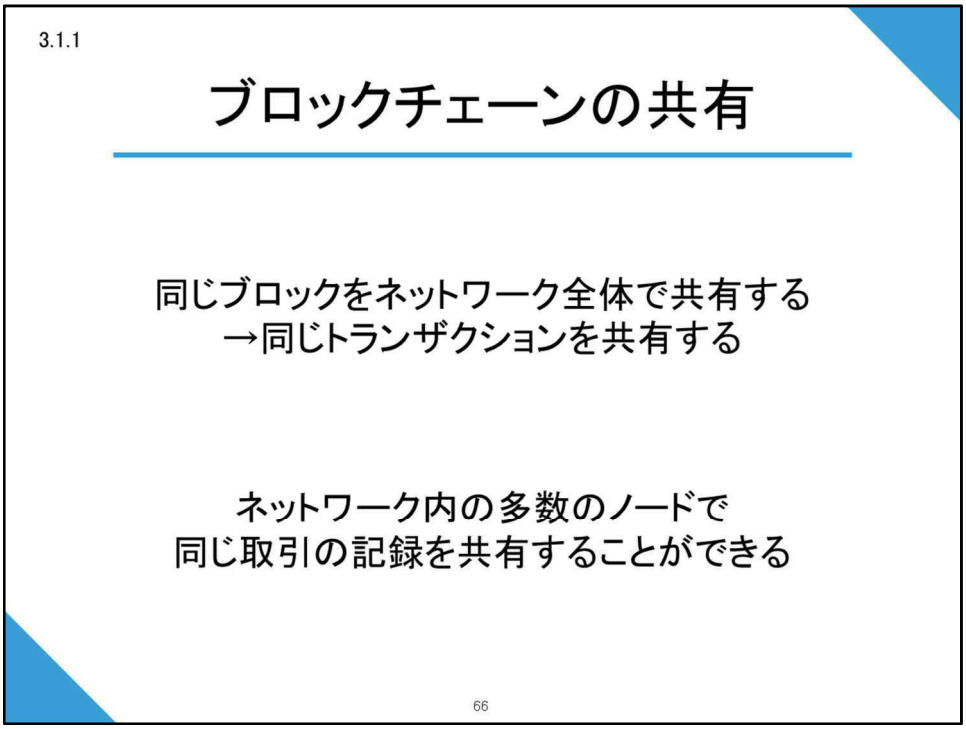
ブロックチェーンによって、ブロックのサイズに制約がある。作成されたブロックがこの範囲内に収まっているか確認する。



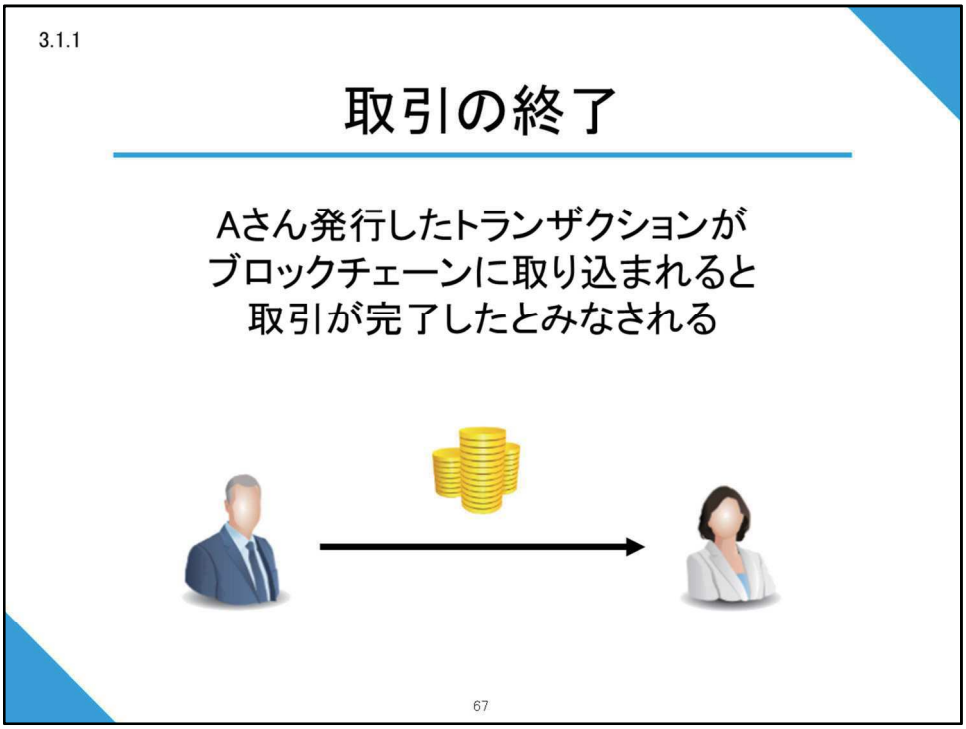
- ブロックの検証作業を行ない、正当なブロックであると判断すると、ブロックを伝達すると同時に自身の手元に保存する。
- それぞれのブロックは、自身の親となるブロックの識別子をブロックの中に持っているため、これによりブロックが鎖状に繋がる。これを狭義のブロックチェーンと呼ぶ。
- システム全体もブロックチェーンと呼び、ブロックの列もブロックチェーンと呼ぶことに注意する。



- 以上のような処理を経て、ネットワーク内のすべてのノードが同じブロックチェーンを保有している状態が出来上がる。

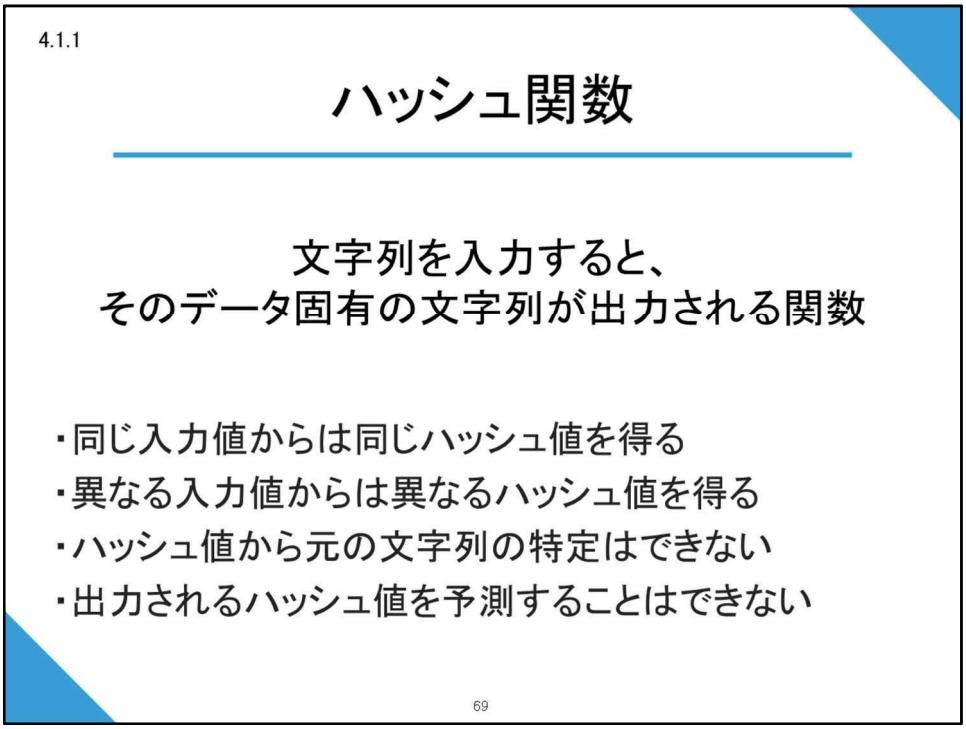


- ネットワーク内の全てのノードが同じブロックチェーンを持っているということは、同じブロックを持っているということ。同じブロックを持っているということは、同じトランザクションを持っているということ。
- トランザクションとは個別の取引の記録であるため、ネットワーク全体で同じ取引を正しいものとして認め、共有している状態が出来上がる。



- Aさんが発行したトランザクションは、ブロックに取り込まれた後に、ブロックチェーンの一部となる。
- これにより、AさんからBさんへの仮想通貨の送金は終了する。注意しなければならないのは、AさんからBさんへ直接通貨が移動するのではなく、通貨の保有権の移動が台帳に書き込まれるだけだということである。

4. ブロックチェーンを支える暗号技術



- 文字列を入力すると、そのデータ固有の文字列が出力される関数
- ブロックチェーンでは様々な箇所で利用されているので、スライドに表示した特徴を知っておく必要がある。

4章演習1

ハッシュ関数を利用する

1.ハッシュ関数SHA-256を用いてハッシュ値を求める
2.ハッシュ関数RIPEMD-160を用いてハッシュ値を求める
3.SHA-256を用いて少し長い文章のハッシュ値を求める

70

準備

- 1人1台PCを利用する
- 巻頭で準備した仮想マシンを立ち上げる
- 仮想マシン上でターミナルを開く
- ターミナルで irb と入力する
- require ‘digest’ と入力すると、ハッシュ関数が利用できるようになる

ハッシュ関数SHA-256を用いてハッシュ値を求める

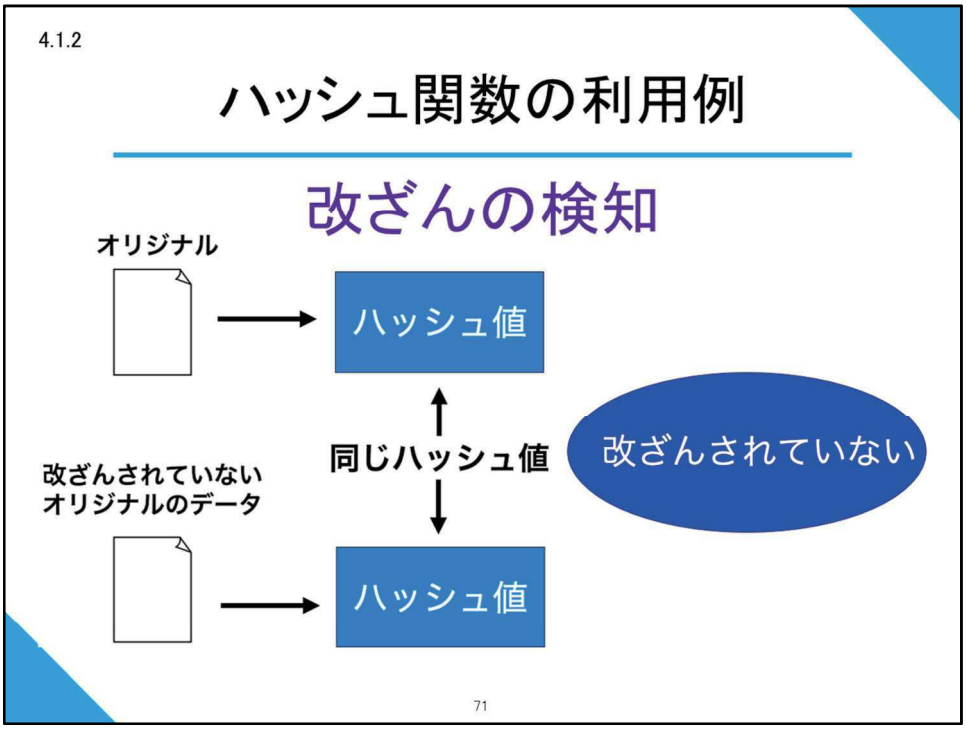
- テキストに従い、ハッシュ値を求める。様々な文字列のハッシュ値を求め、異なるハッシュ値が同じ長さで出力されることを確認する。

ハッシュ関数RIPEMD-160を用いてハッシュ値を求める

- テキストに従い、ハッシュ値を求める。様々な文字列のハッシュ値を求め、異なるハッシュ値が同じ長さで出力されることを確認する。
- SHA-256とRIPEMD-160を使った時のハッシュ値の違いについて考え、挙手で発表する。（A.出力されるハッシュ値の長さが違う）

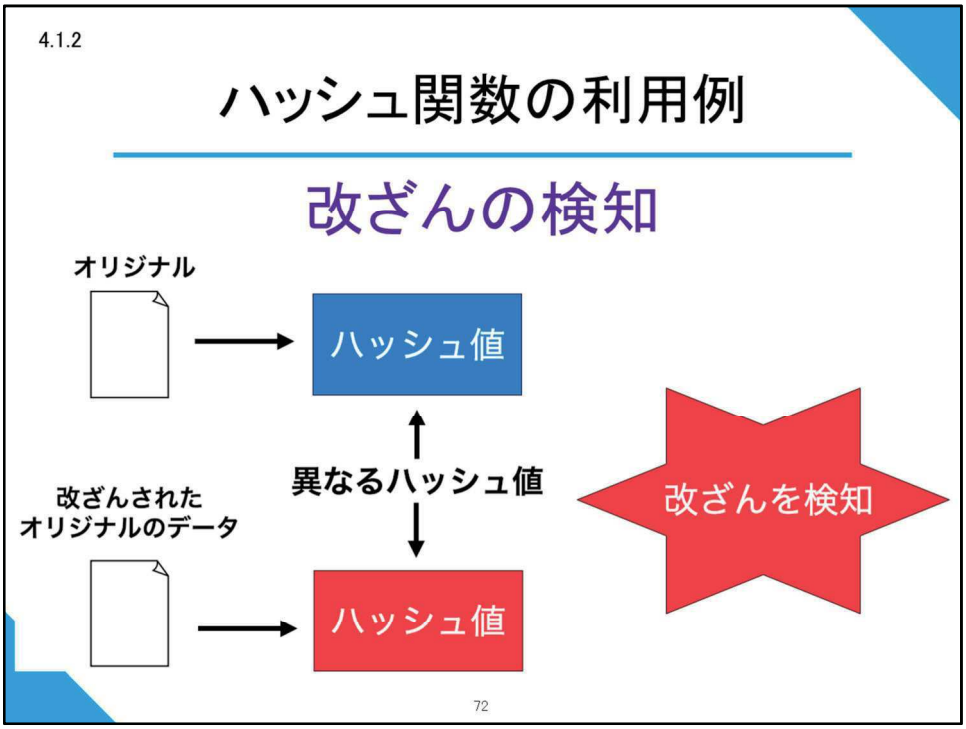
ハッシュ関数SHA-256を用いて少し長い文章のハッシュ値を求める

- 長い文章の一部分を変更しただけでも、出力されるハッシュ値は大きく変わることを確認する。

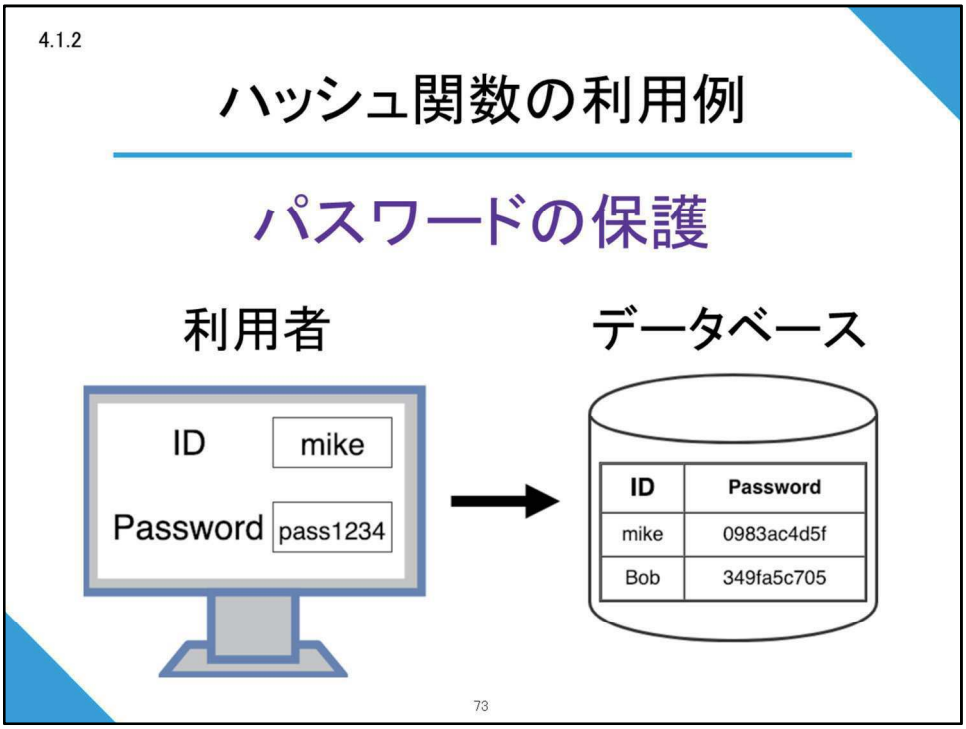


改ざんの検知への利用

- データに改ざんや変更がされていないか確認をするとき、データサイズが大きいと、比較に長い時間がかかる。この際に、データをハッシュ関数にかけて、そのハッシュ値を比較することで、素早く改ざんや変更の確認を行うことができる。
- 2つのデータが全く同じならば、出力されるハッシュ値も同じになる。

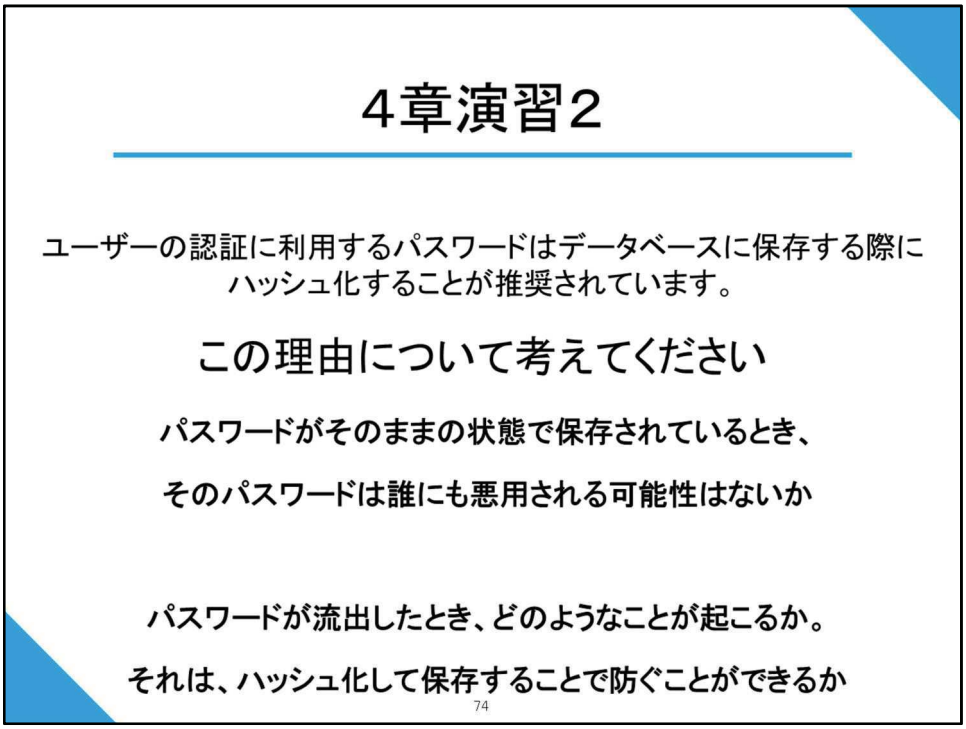


- データの内容が異なる、つまり改ざんや更新がされていれば、出力されるハッシュ値は異なる。
- ハッシュ関数では改ざんや変更の検知できるものの、どの部分がどのように変更されたかはわからない。



パスワード保護

- 様々なサービスにおいて、ユーザーの認証でIDとパスワードが使われている。
- サービスの提供者側は、このパスワードをハッシュ化してデータベースに保存しておくことが推奨されている。



準備

- 4～5人のグループを作成する

Q.1

パスワードがそのままの状態で保存されているとき、そのパスワードは誰にも悪用される可能性はないか。

A.1

データベースの管理を行う人は、パスワードとIDを確認することができる。そのため、管理者が悪用しようとすればできてしまう。

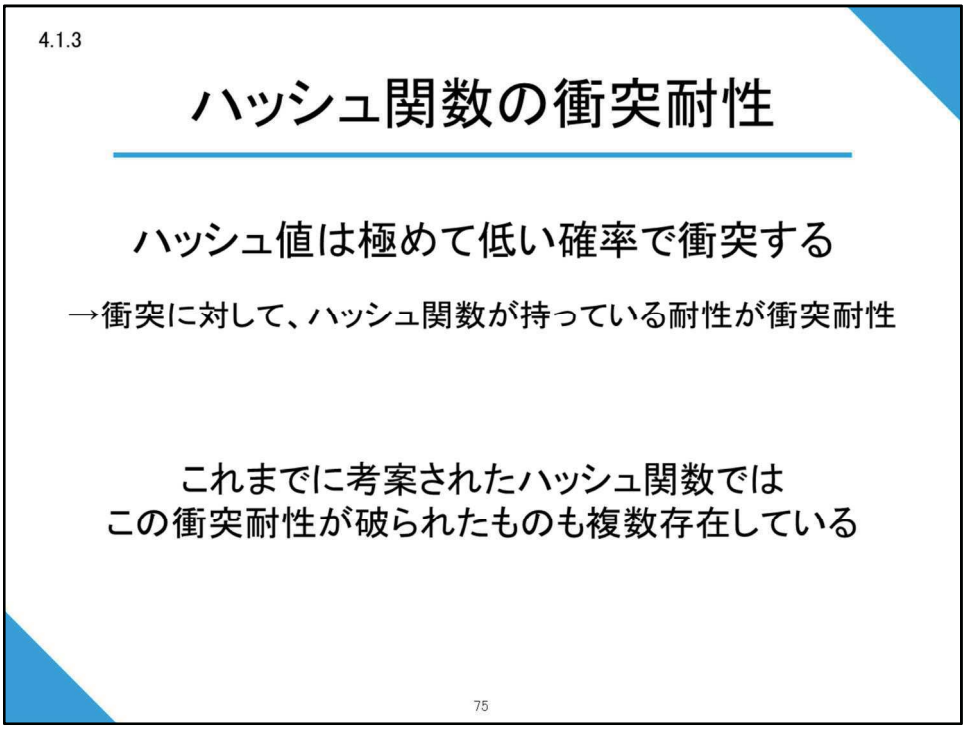
Q.2

パスワードが流出したとき、どのようなことが起こるか。それは、ハッシュ化して保存することで防ぐことができるか

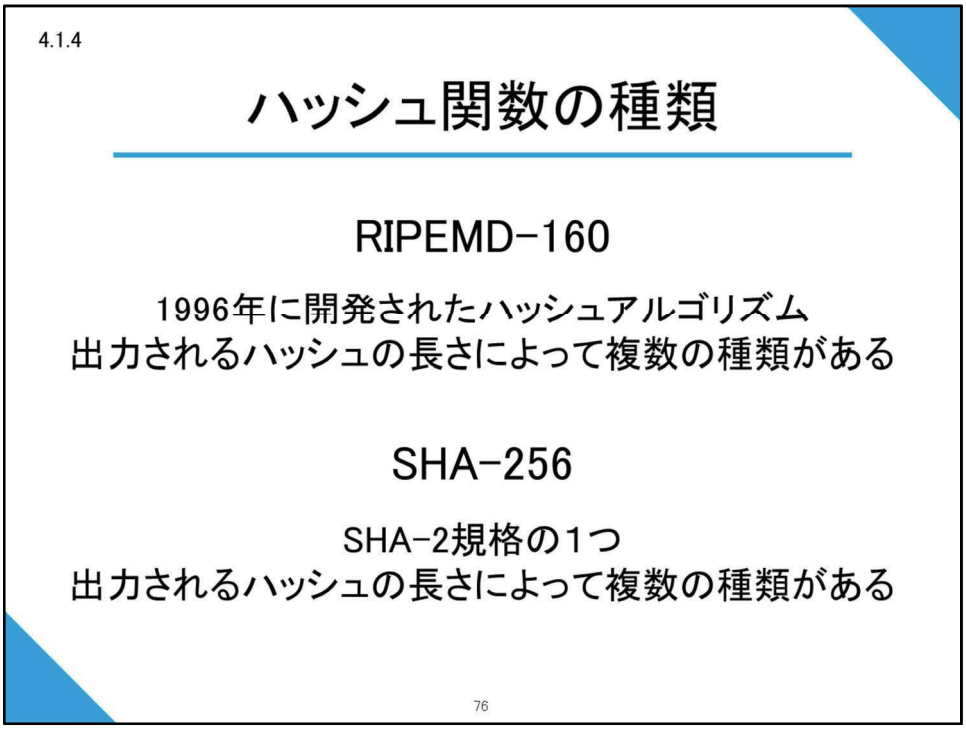
A.2

パスワードをハッシュ化して保存することで、情報が流出した際に、パスワードとIDがセットとなって流出することを防ぐことができる。仮に、ハッシュ化していない場合には、当該のサービスだけでなく、同じIDとパスワードを利用しているサービスにも影響がある。

それぞれについてグループで10分程度考えてもらい、代表者に発表してもらう。



- 出力されるハッシュ値のパターンは有限であることから、ハッシュ値は衝突する可能性がある。
- 衝突に対してハッシュ関数が持っている耐性を衝突耐性と言う。
- これまでに衝突耐性が破られたハッシュ関数も存在する。



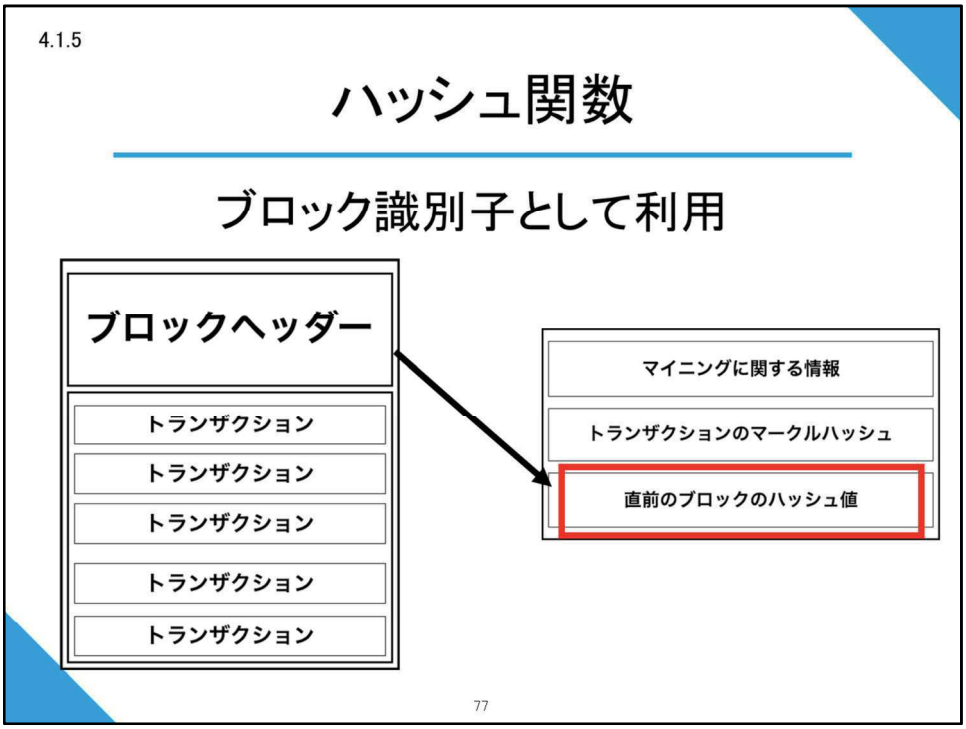
- Bitcoinに利用されているハッシュ関数を紹介する。

RIPEMD-160

公開鍵からアドレスを作る際に利用される。

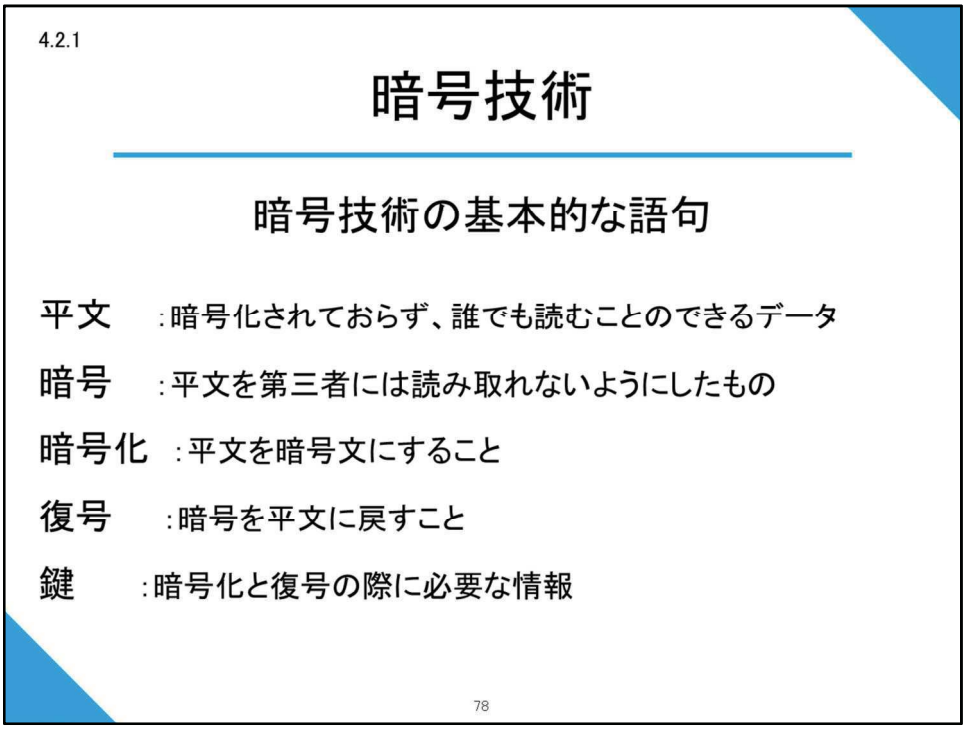
SHA-256

公開鍵からアドレスを作る際や、ブロックの識別子を作る際に利用される。

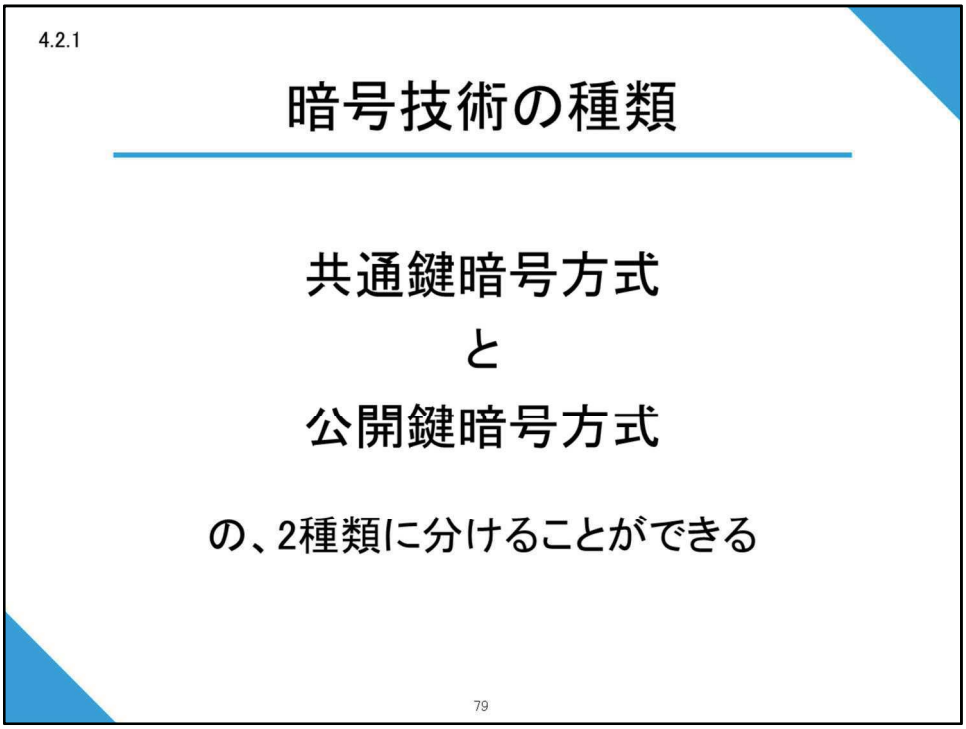


ブロックチェーンでのハッシュ関数の利用について

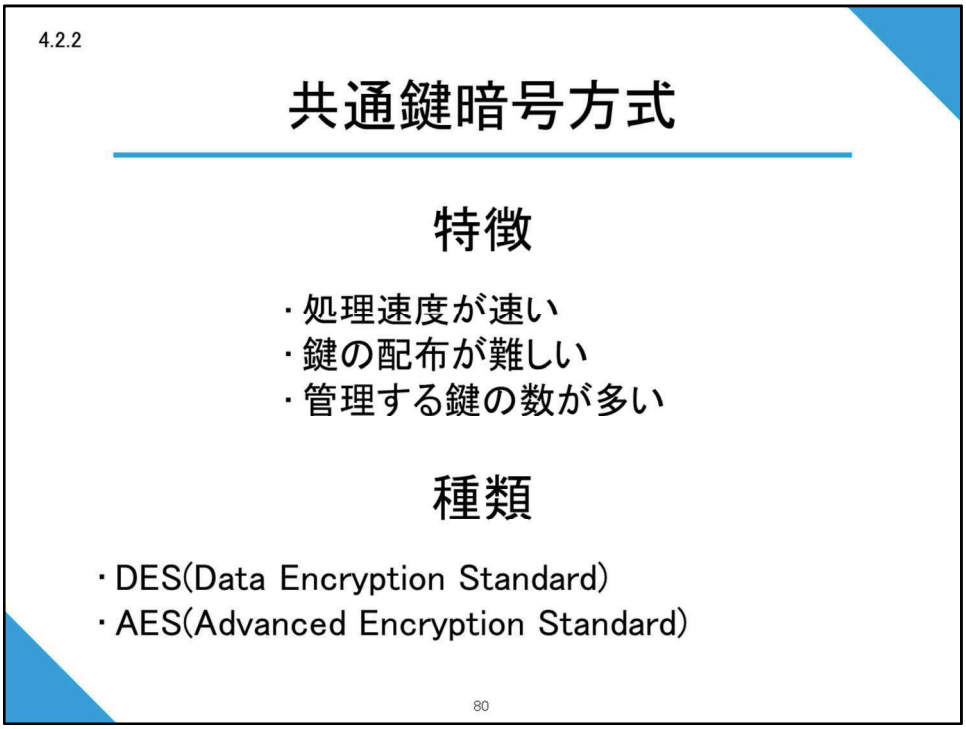
- ハッシュ関数はブロックの識別子を作成する際に利用されている。
- それぞれのブロックを識別する際には、ブロックの構成要素の1つであるブロックヘッダの情報をまとめてハッシュ関数に入力し、それにより得られたハッシュ値をそのブロックの識別子としている。
- Bitcoinではブロックヘッダの情報をSHA-256を2回用いてハッシュ化し、識別子として利用している。



- 仮想通貨は別名「暗号資産」とも呼ばれている。この名前から分かるように暗号技術はブロックチェーンについて理解する上で非常に重要である。
- スライドに表示した暗号技術に関連した語句はすべて把握することが必要である。



- 暗号技術は大きく「共通鍵暗号」と「公開鍵暗号」に分類することができる。



- 処理速度が速い

公開鍵暗号に比べて、暗号化、復号の処理が単純であるため、処理速度が速い。

- 鍵の配布が難しい

暗号化と復号に同じ鍵を用いるため、鍵を通信相手に送らなければならない。この過程で、通信が盗聴され鍵が盗まれる可能性がある。

- 管理する鍵の数が多い

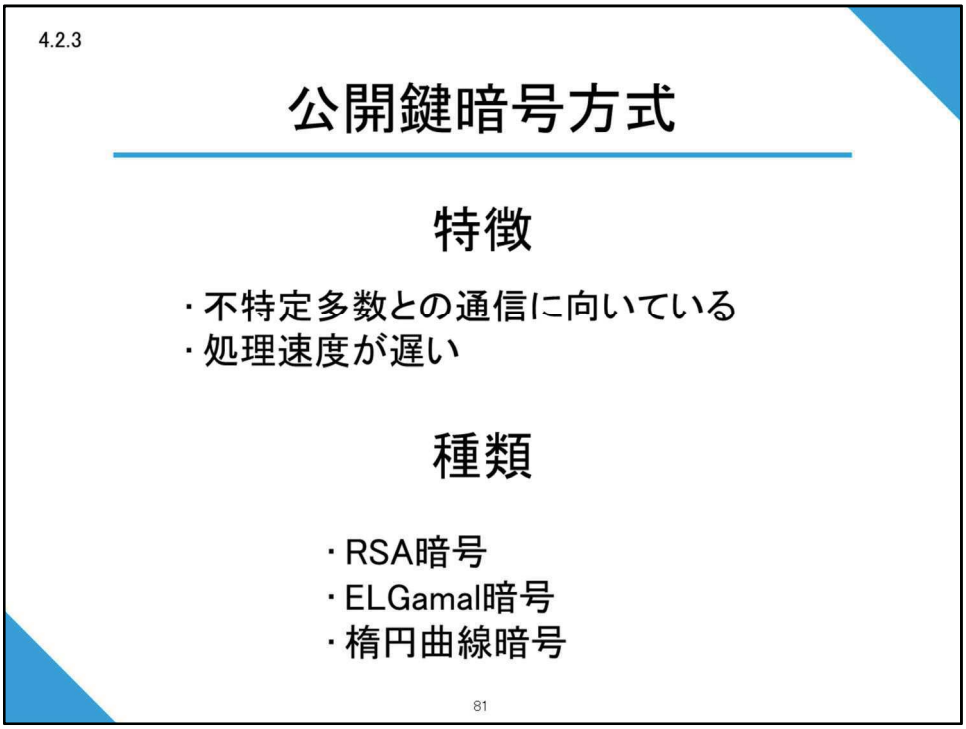
共通鍵暗号では安全性の問題から、取引相手ごとに異なる鍵を用いなければならない。そうなると、通信相手の数だけ鍵を管理する必要があり、管理しなければならない鍵の個数が多くなる。

- DESについて

以前は主流であった共通鍵暗号のひとつ。現在は、総当たりにより現実的な時間内に解読が行えるようになったため、安全に使用することはできない。

- AESについて

DESの強度の低下に伴って登場した暗号方式。2019年現在安全に使用することができる。



- 不特定多数との通信に向いている

公開鍵を配布し、それを用いて暗号化を行う。復号は公開鍵に対応する秘密鍵でしか行うことができない。そのため、管理する鍵の個数が少なくて良い。不特定多数との通信に向いている。

- 処理速度が遅い

共通鍵暗号に比べて暗号化、復号の処理が複雑であるため、処理に時間がかかる。
このような点を補うために、共通鍵を公開鍵暗号方式で送信し、実際のデータは共通鍵暗号方式で伝達する、ハイブリッド型暗号方式も利用されている。

- RSA

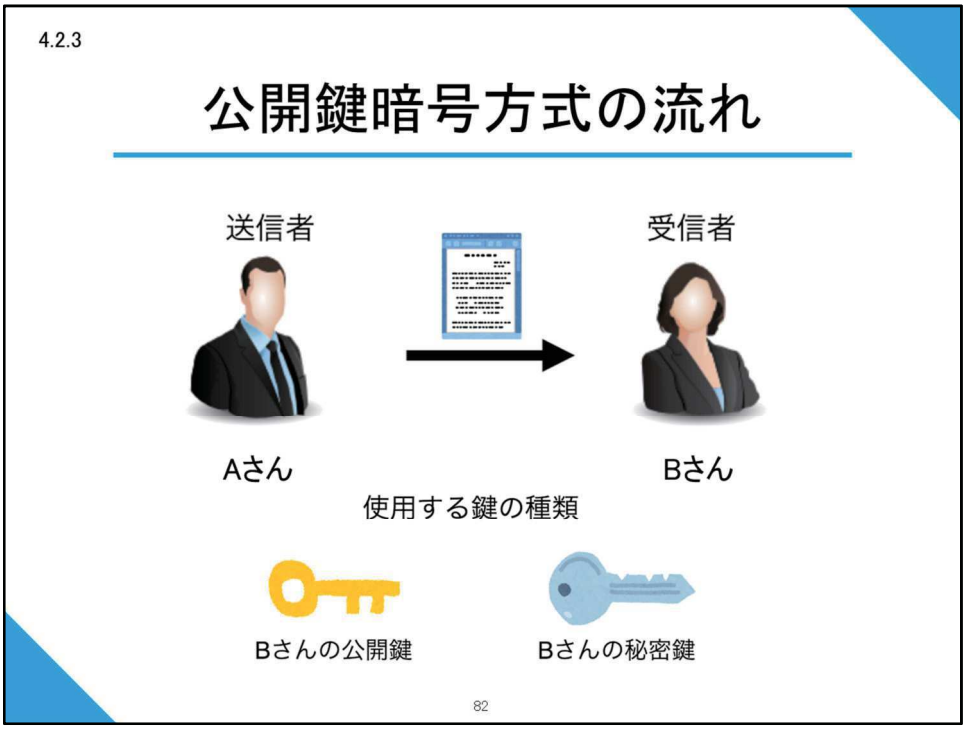
2つの大きな素数の積を求めることは簡単だが、積を素因数分解することは難しいという性質を利用した暗号方式。2019年現在安全に使用することができる。

- ElGamal暗号

離散対数問題という計算を利用した暗号方式。2019年現在安全に使用することができる。

- 楕円曲線暗号

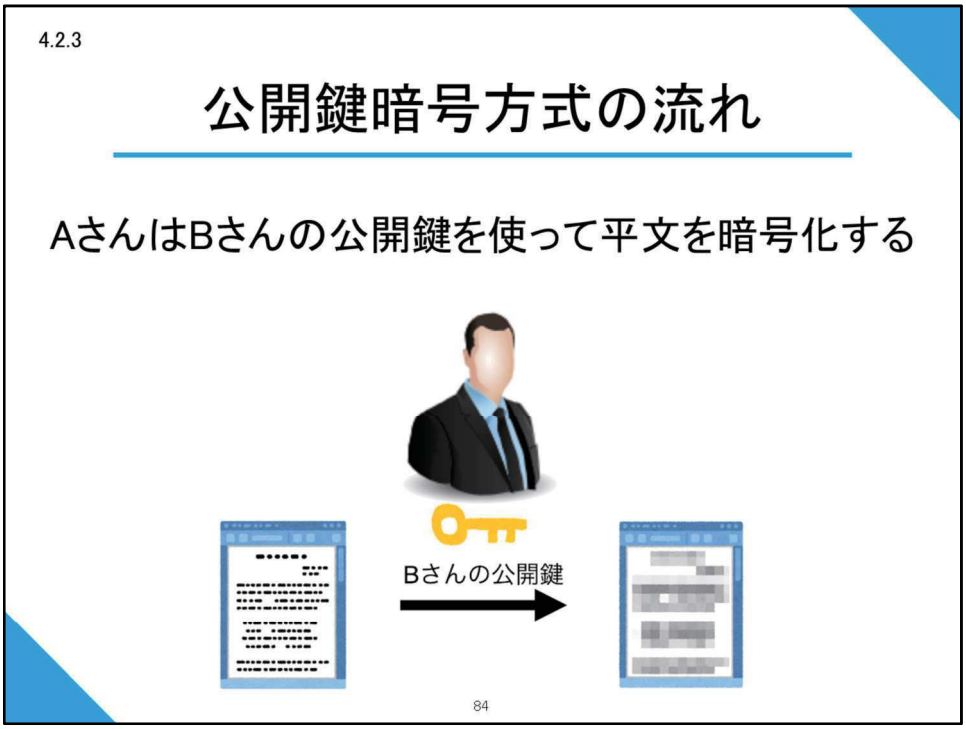
楕円曲線と呼ばれる曲線を用いた暗号化技術。RSAやElGamalよりも安全性が高く、計算速度も速いのが特徴。Bitcoinに利用されている。2019年現在安全に使用することができる。



AさんからBさんにデータを送る際に、公開鍵暗号方式を利用するとして説明する。

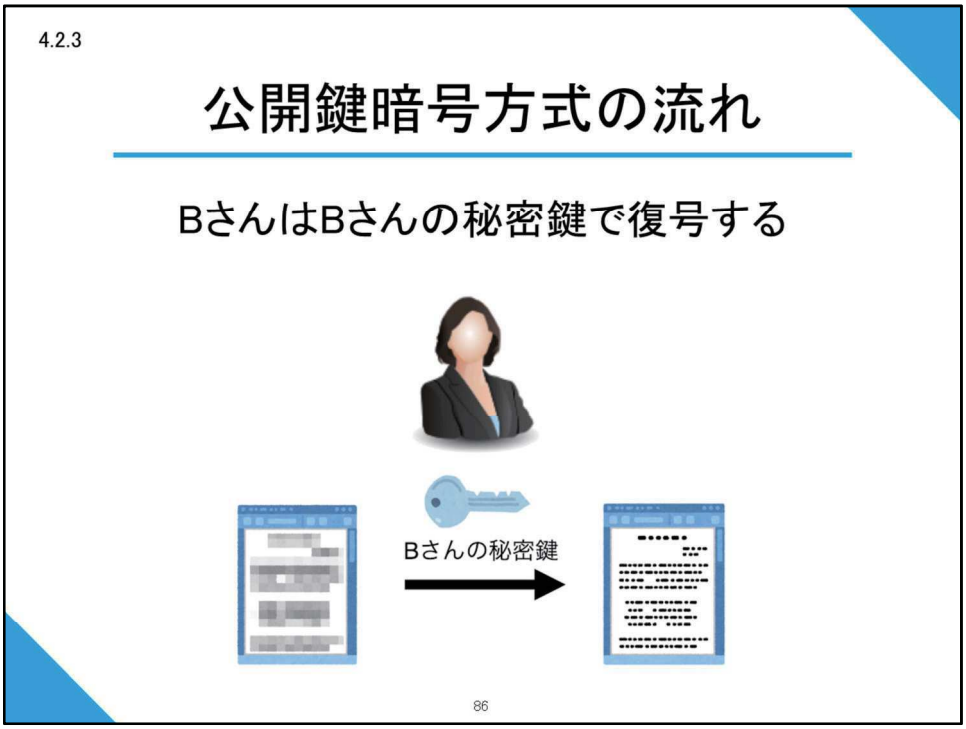
- Bさんは自身の秘密鍵と公開鍵を作成しておく。

- Bさんはあらかじめ自身の公開鍵をAさんに知らせておく。

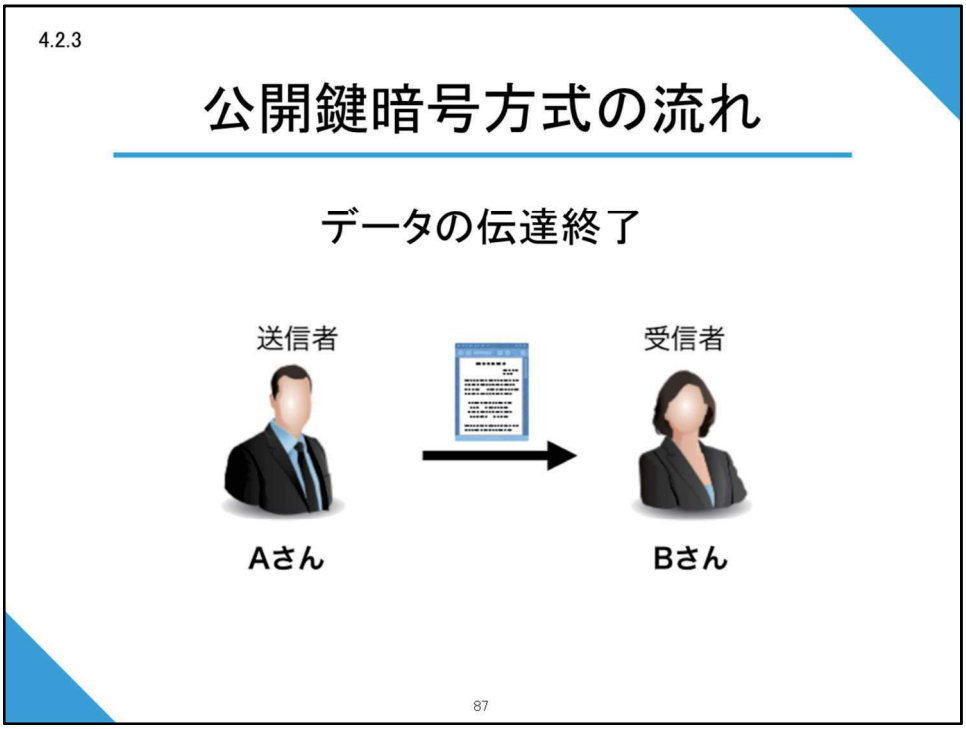


- AさんはBさんの公開鍵を使って、送りたいデータを暗号化する。

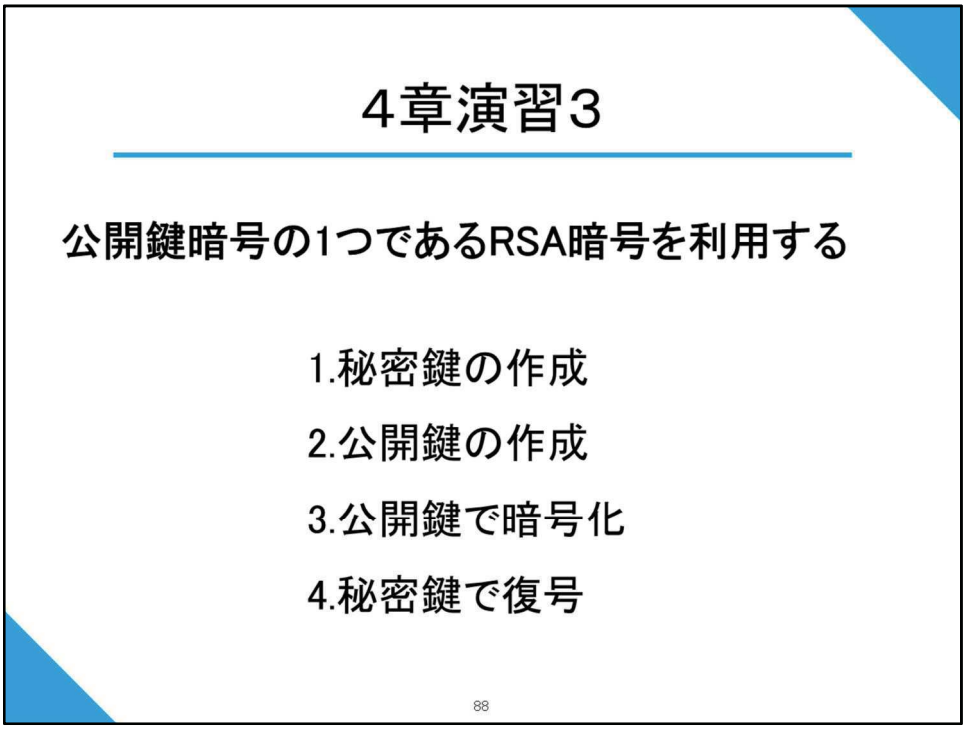
- 暗号化したデータを送信する。



- Bさん受け取った暗号を自身の秘密鍵で復号し、平文を得る。



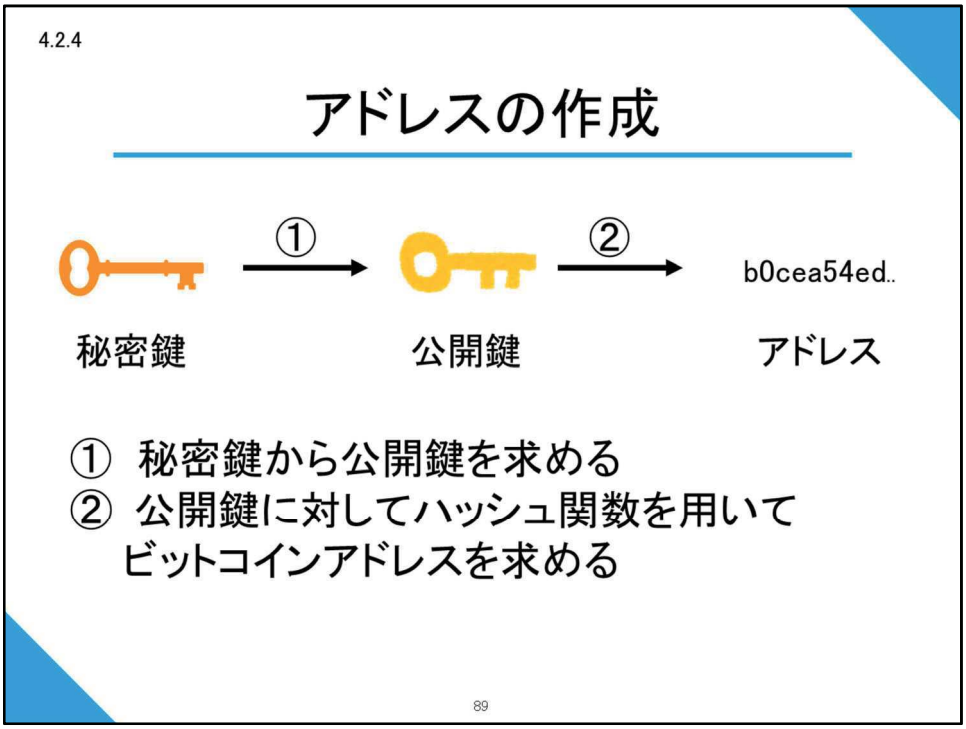
- データ送信完了
- 通信経路で暗号が盗聴された場合でも、暗号を復号できるのは秘密鍵を持っているBさんのみであるため、問題ない。



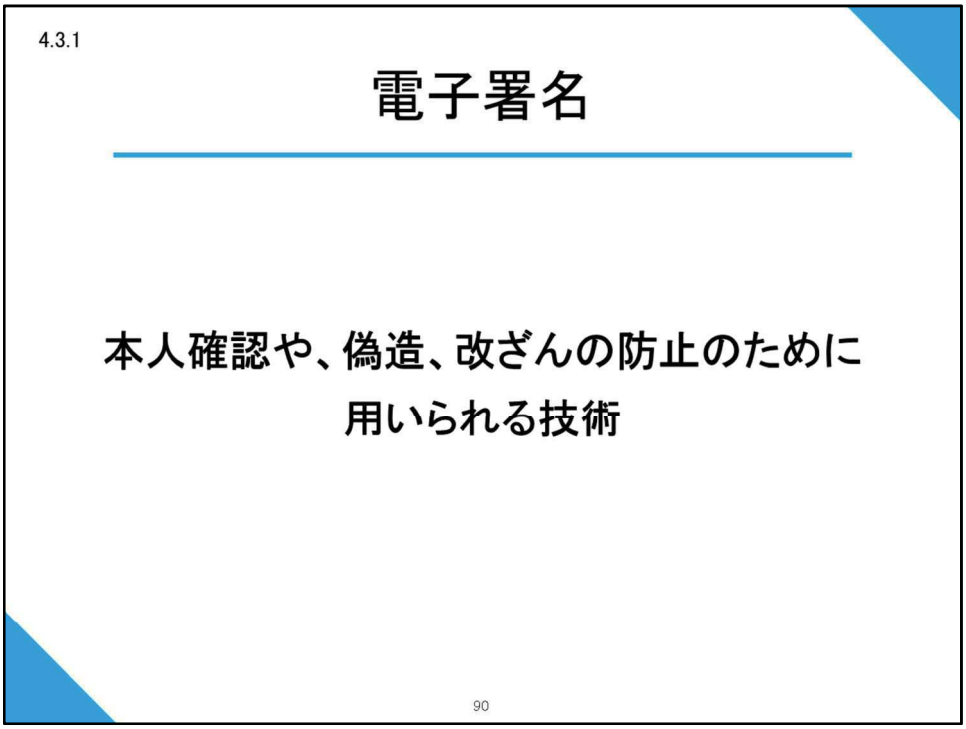
準備

- 1人1台PCを利用する
- 巻頭で準備した仮想マシンを立ち上げる
- 仮想マシン上でターミナルを開く

- テキストに従い、順にコマンドを実行し、秘密鍵の作成、公開鍵の作成、暗号化、復号の作業を行ってもらう。
- この過程で、実際の秘密鍵、公開鍵、暗号文の中身を確認する。

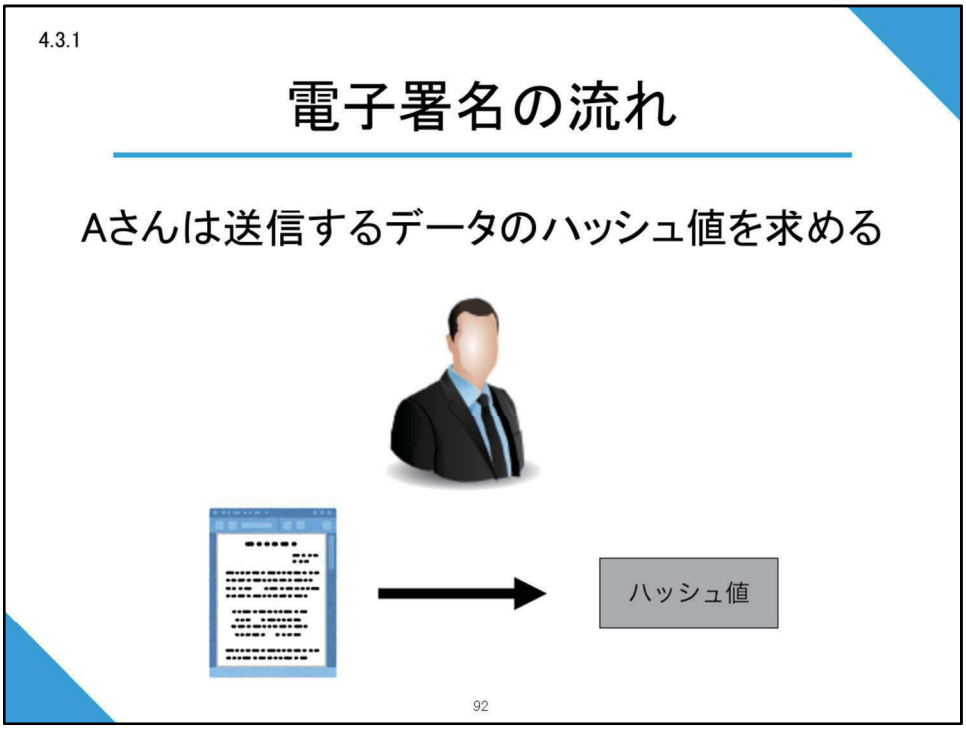


- 仮想通貨を保有するために必要なアドレスの作成方法をBitcoinを例にして説明を行う。
- Bitcoinで使用される暗号技術は楕円曲線暗号
- 秘密鍵から公開鍵を求める流れは通常の暗号技術と変わりない。
- 公開鍵をハッシュ関数SHA-256に入れてハッシュ値を求め、さらにそのハッシュ値をハッシュ関数RIPEMD-160に入れてハッシュ値を求める。
- これにより得られたハッシュ値をBitcoinアドレスのフォーマットに従って、エンコードすることで、アドレスが作成される。

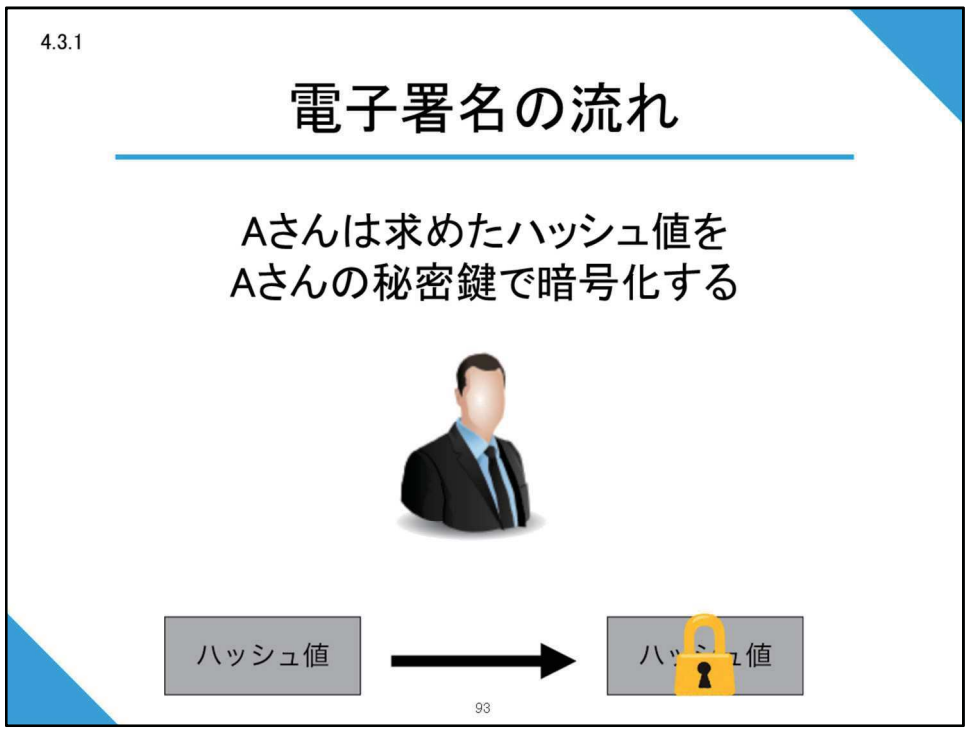


- 電子署名を用いることで、送信者の本人確認と、改ざんの検知を行うことができる。
- 公開鍵暗号方式で使用される秘密鍵と公開鍵を使用する。

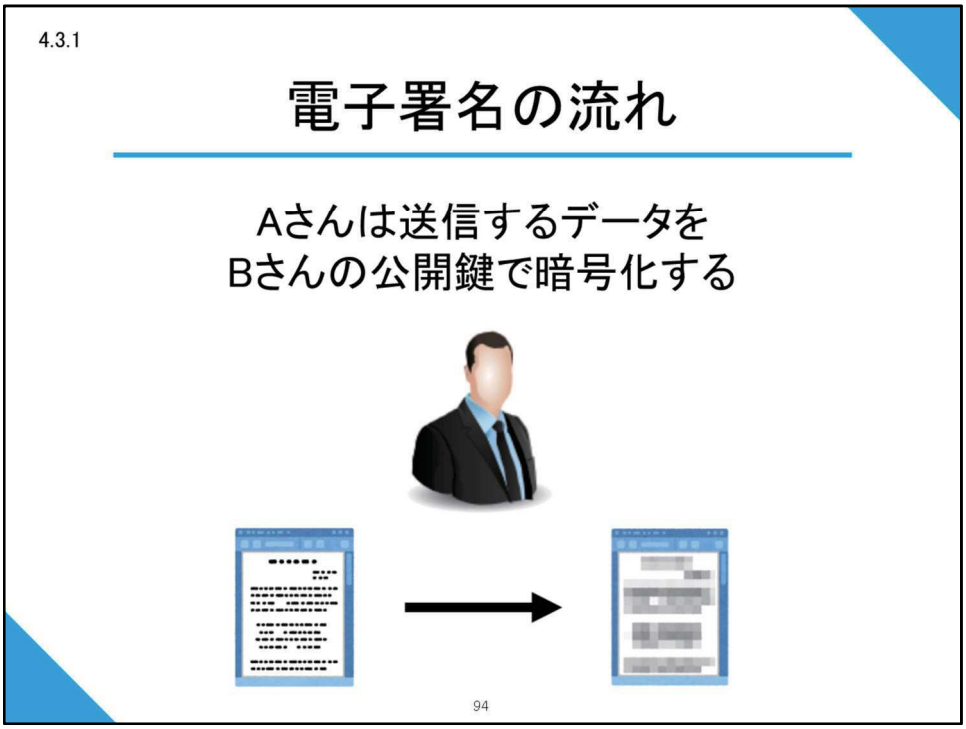
AさんがBさんに電子署名をつけてデータを送信することを例にして説明する。



- 送信者であるAさんは、Bさんに送りたいデータのハッシュ値を求める。



- Aさんは、求めたハッシュ値を自身の秘密鍵を使って暗号化する。

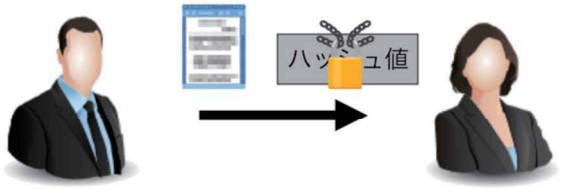


- Aさんは、Bさんに送りたいデータをBさんの公開鍵で暗号化する。

4.3.1

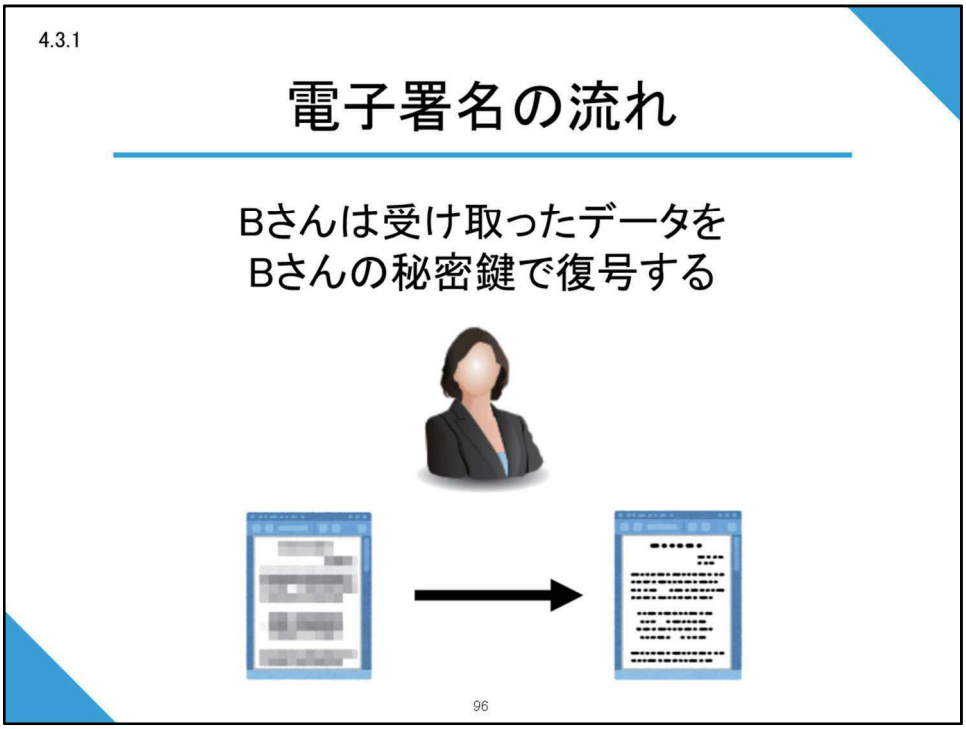
電子署名の流れ

AさんからBさんに
暗号化したデータとハッシュ値を送信する

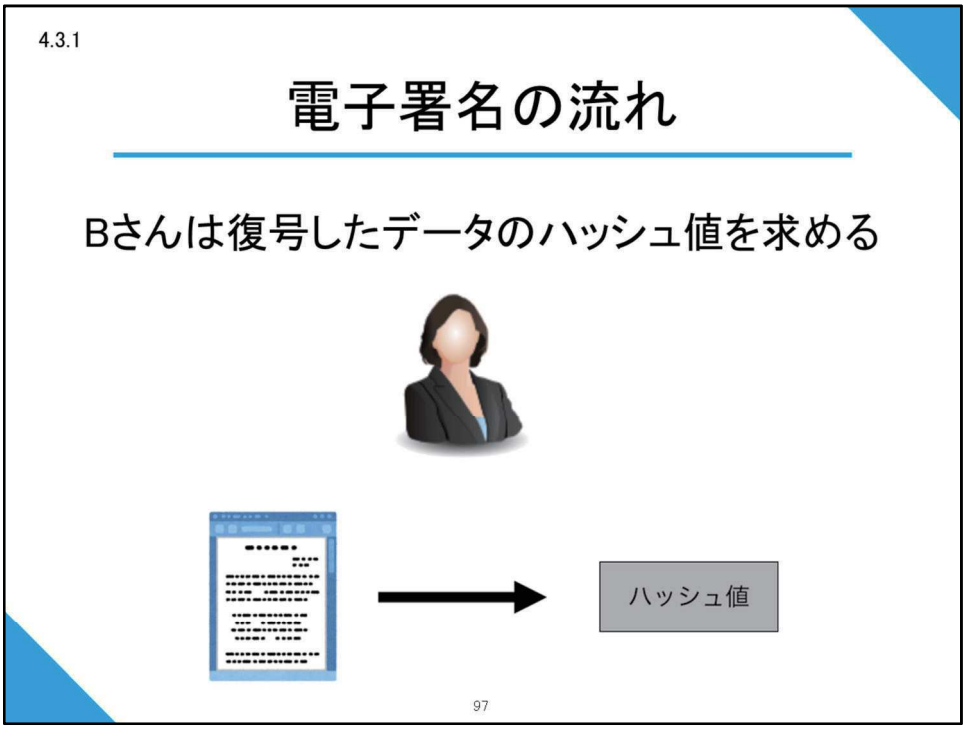


95

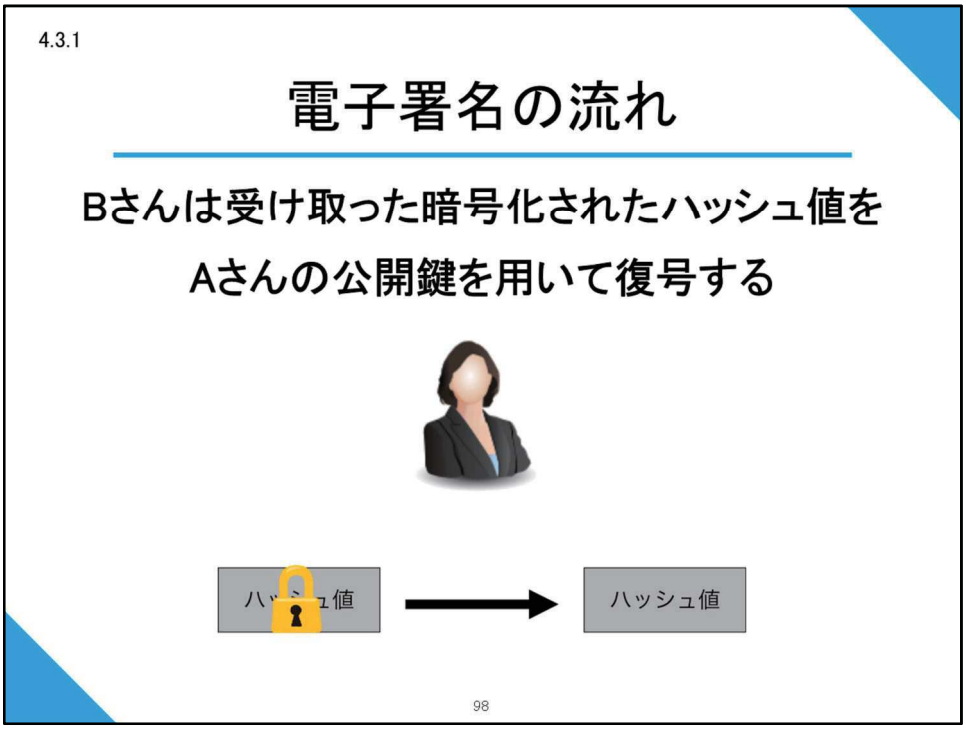
- Aさんは、平文のハッシュ値と暗号文を送る。



- Bさんは受け取った暗号を自身の秘密鍵で復号する。この作業は通常の公開鍵暗号と同じである。



- Bさんは復号したデータのハッシュ値を求める。



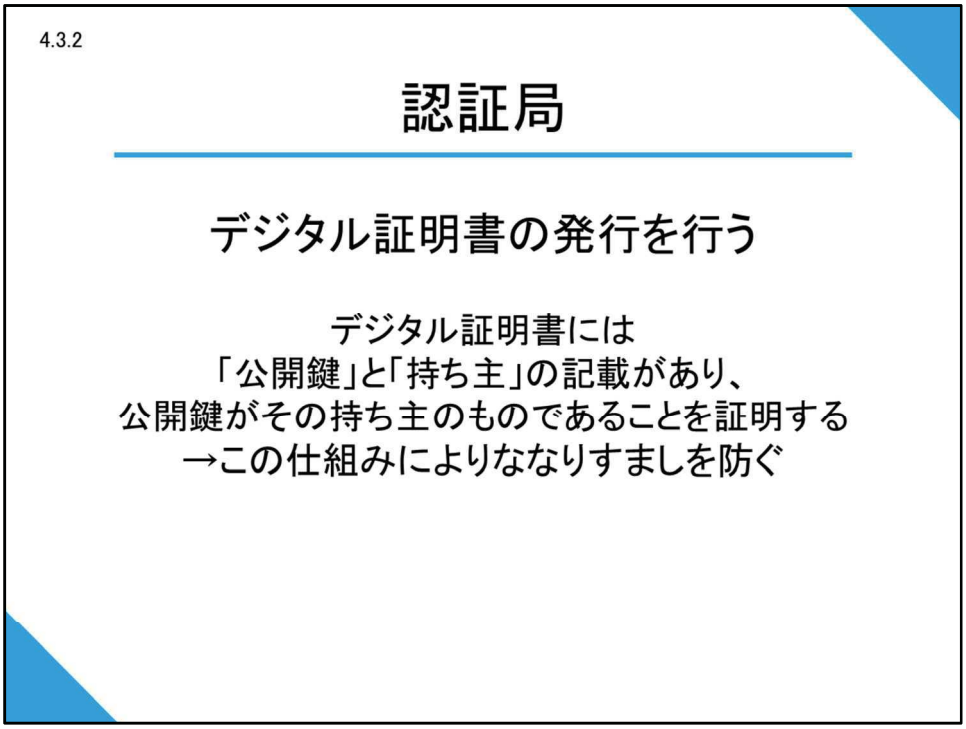
- BさんはAさんから受け取った暗号化されたハッシュ値をAさんの秘密鍵を用いて、復号する。

- 改ざんの検知

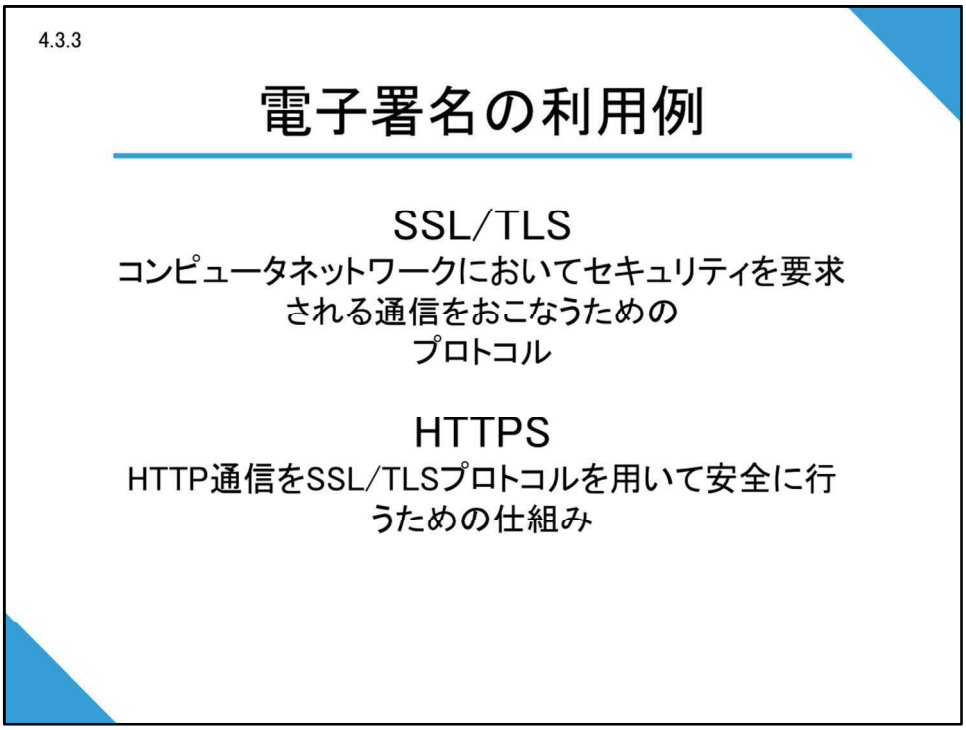
Aさんが送信前に求めたハッシュ値と、Bさんが受け取ったハッシュ値が同じであれば、通信の過程でデータが改ざんされていないことがわかる。

- 送信相手がAさんであることの確認

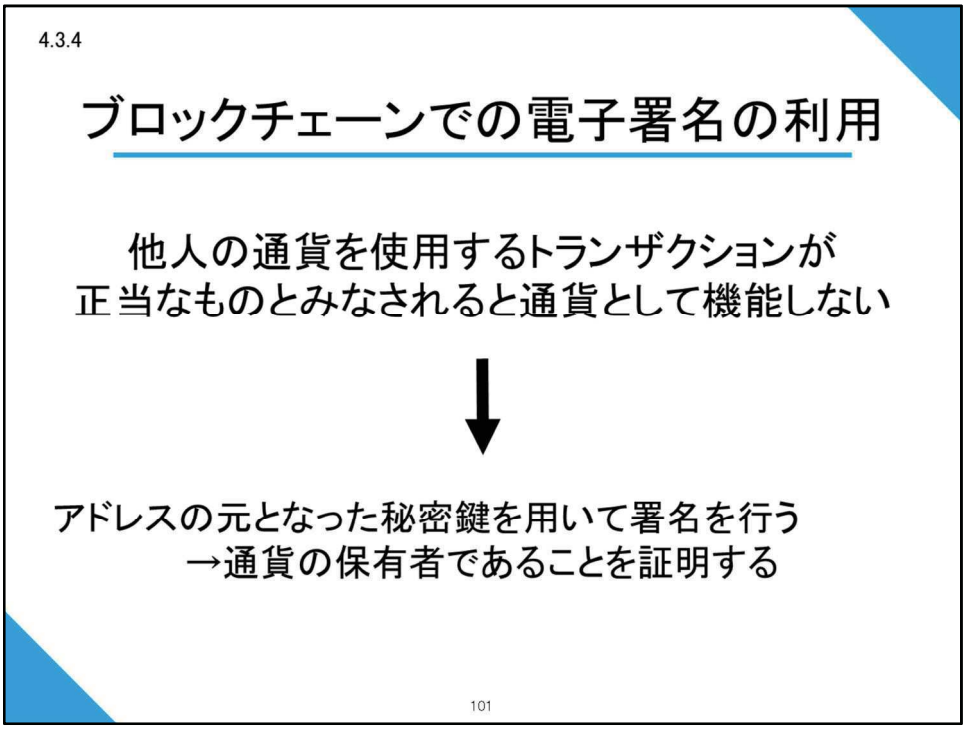
送られてきたハッシュ値がAさんの公開鍵で復号できたと言うことは、送信相手はAさんの秘密鍵を持っていると確認できる。なりすましや鍵の流出などの可能性を除くと、送信相手はAさんであることがわかる。



- 認証局は公開鍵と持ち主を紐づけたデジタル署名を発行する。これにより、なりすましを防ぐことができる。



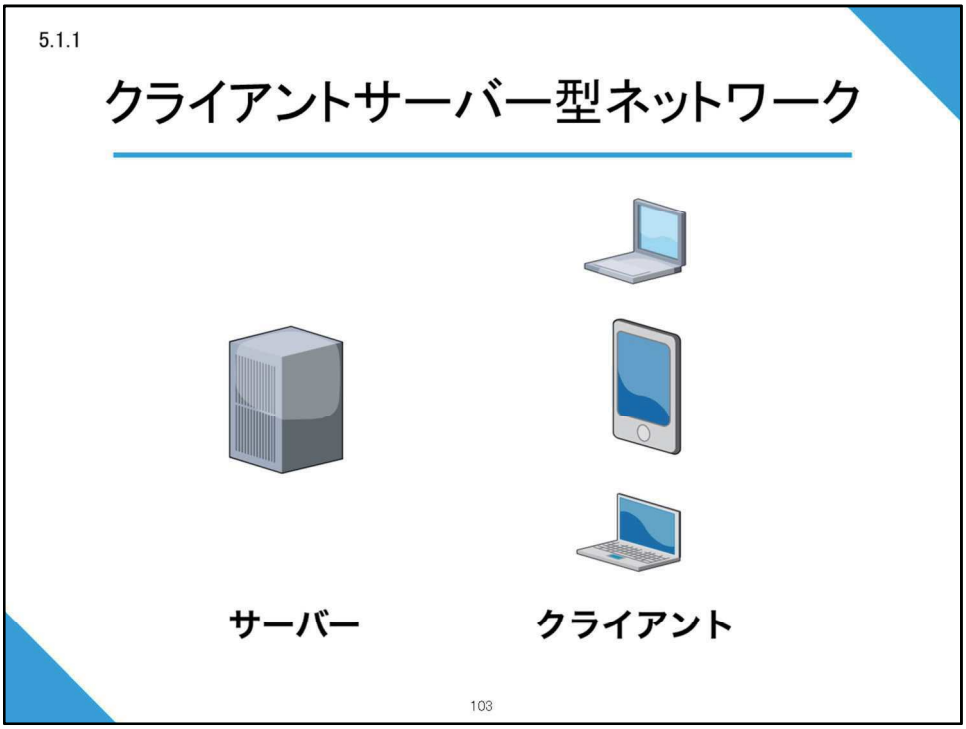
- 電子署名は特別な技術ではなく、私たちが普段から気にすることなく利用している技術の一つである。



- トランザクションは誰でも発行することができ、中身も自由に書くことができる。つまり、他人の通貨を利用するトランザクションも発行することはできる。
- トランザクションに電子署名をすることで、そのアドレスの正当な保有者であることを証明することができ、他人に通貨を使われることを防ぐことができる。

5. P2Pネットワーク

102



P2Pネットワークの説明を始める前に、現在多くのシステムで利用されているクライアントサーバー型ネットワークについて説明する。

クライアントサーバー型ネットワークでは、2種類のコンピュータが存在する。

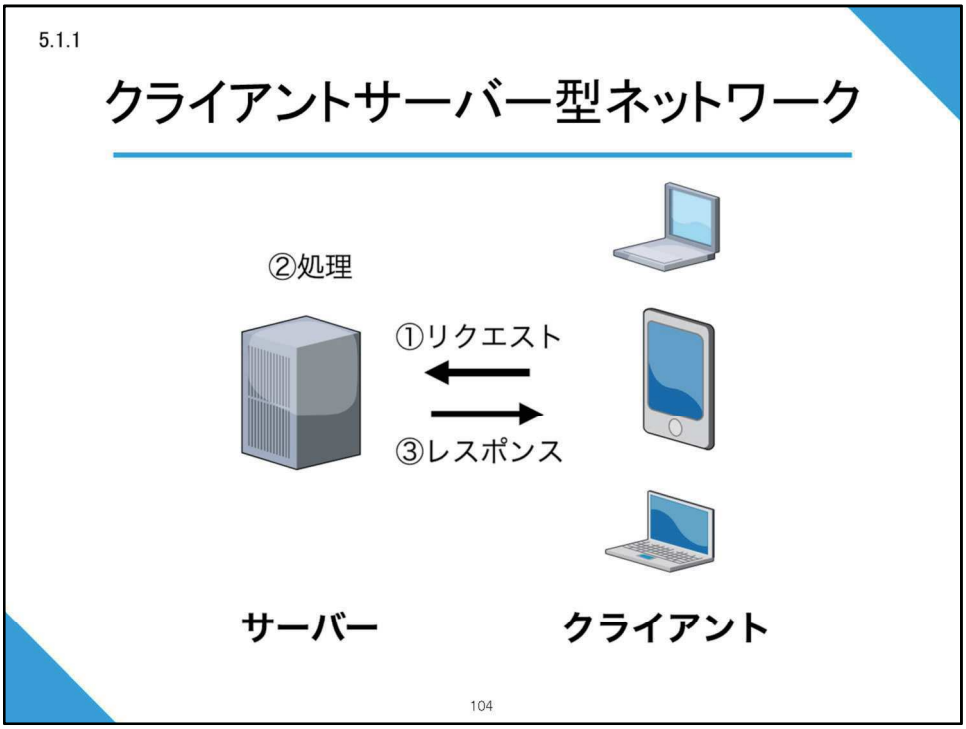
- クライアント

一般的に私たちが、webサイトを閲覧したり、オンラインでアプリケーションを利用している際には、私たちが利用しているPCやスマートフォンなどはクライアントの立場に立っている。

- サーバー

クライアントに対して、webサイトやアプリケーションのデータを保有し、クライアントから要求があった際に、それらを提供するのがサーバーである。サーバーはその役割によってメールサーバーや、Webサーバーなどに分類する事ができる。一般的にサーバーはサービスを提供する企業内や、データセンターで管理されており、日常生活で目にすることはほとんどない。

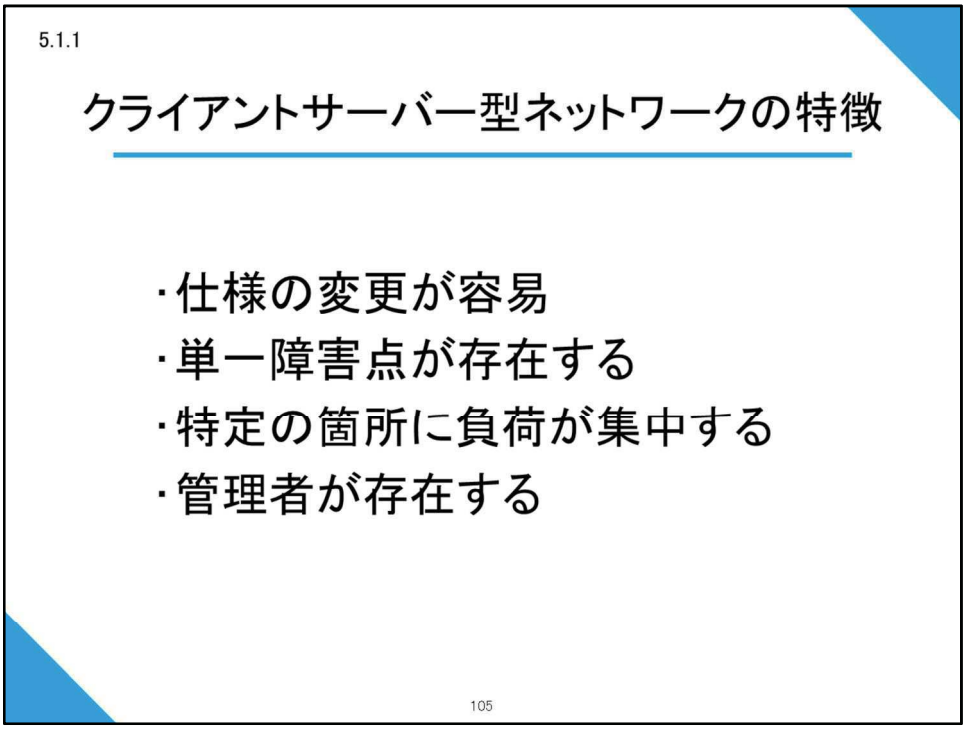
一般的に私たちが利用しているサービスの大半は、クライアントサーバー型のネットワークである。



- クライアントとサーバーが相互に通信し合うことにより成り立っている。

クライアントサーバー型ネットワークでの処理の流れを以下に示す。

- クライアントがサーバーにリクエストを送る。
- サーバーが受け取ったリクエストを処理する。
- サーバーがクライアントにレスポンスを返す。



- 仕様の変更が容易

サーバーが保持しているデータやプログラムに修正を行うだけでよい。

- 単一障害点が存在する

特定の箇所が機能不全に至るとシステム全体が機能しなくなる箇所を単一障害点と呼ぶ。クライアントサーバー型ネットワークでは通信は全てサーバーを経由するため、サーバーが単一障害点となり、サーバーが機能しなくなるとネットワーク全体が機能不全に陥る。

- 特定の箇所に負荷が集中する

すべての通信がサーバーを経由するため、クライアント数の増加や、一時的な通信量の増加に伴って、サーバーに大きな負荷がかかる。これにより、処理速度の低下や、最悪の場合には、サーバーが停止する可能性もある。

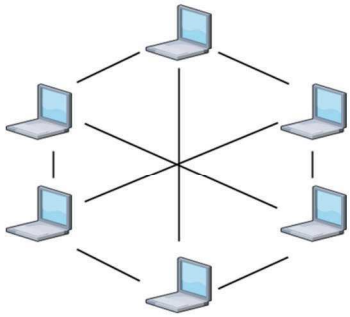
- 管理者が存在する

管理者が存在することにより、システムの管理が容易になるという利点はあるが、管理者の権限が悪用されることや、管理者権限が奪われることによる不正が行われる可能性もある。

5.2.1

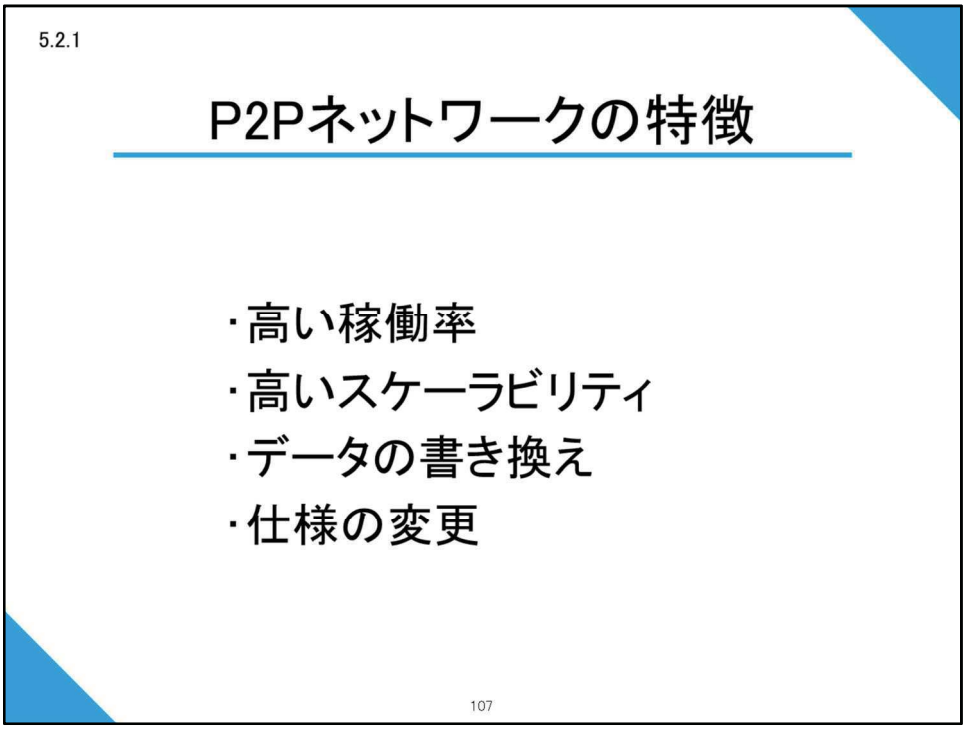
P2Pネットワーク

コンピュータが互いに情報を
伝達し合うことにより、通信が行われる



106

- コンピュータが互いに情報を伝達し合うことにより、通信が行われる。
- P2Pネットワークを構成するそれぞれのコンピュータは「ノード」と呼ばれる。



- 高い稼働率

特定のノードに依存していないため、複数のノードが機能しなくなった場合にも、システム全体が機能しなくなることは少ない。

- 高いスケーラビリティ

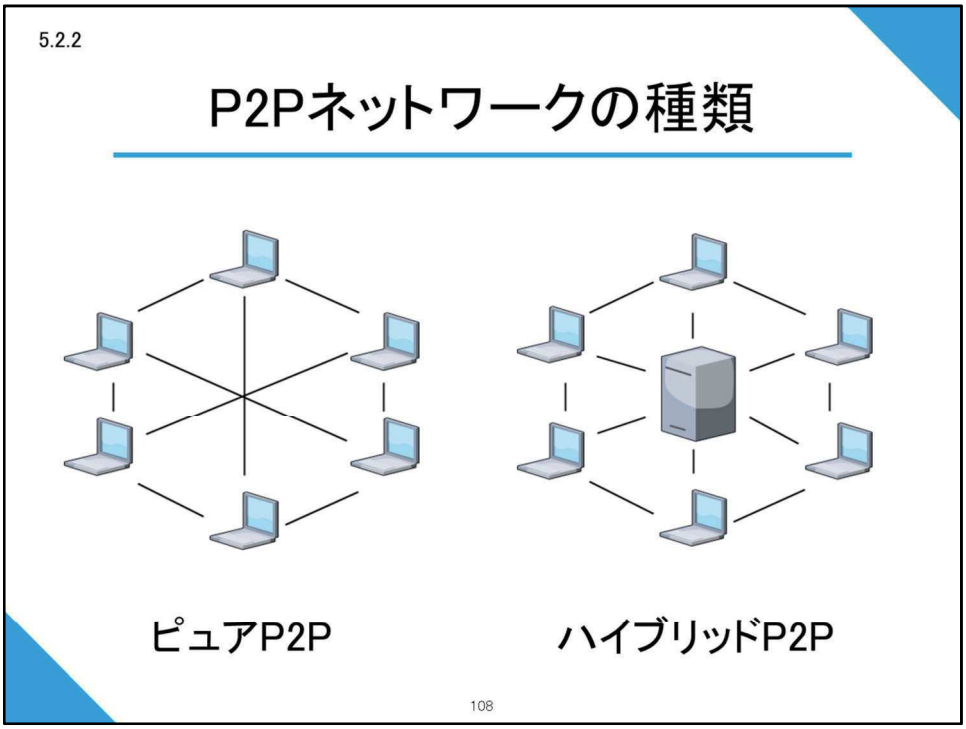
クライアントサーバー型のネットワークでは、すべての通信がサーバーを経由していたのに対して、P2Pネットワークでは特定のノードを経由することはなく、特定の回線に負荷がかかることはない。

- データの書き換え

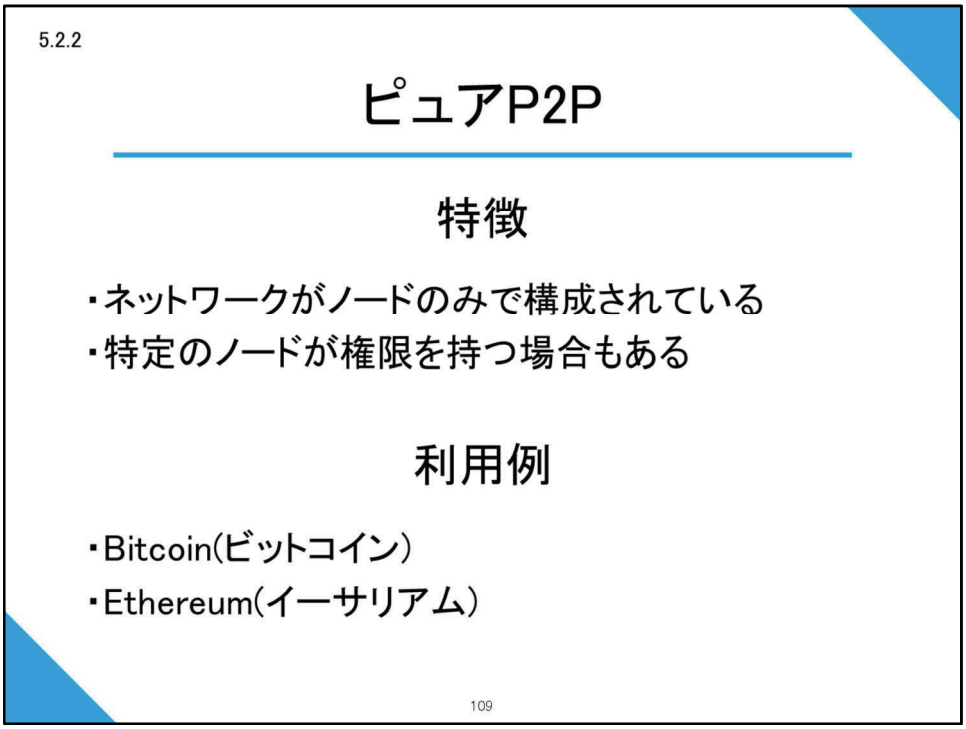
複数のノードを中継しデータを受け取る際には、中継したノードによりデータが書き換えられるリスクがある。

- 仕様の変更

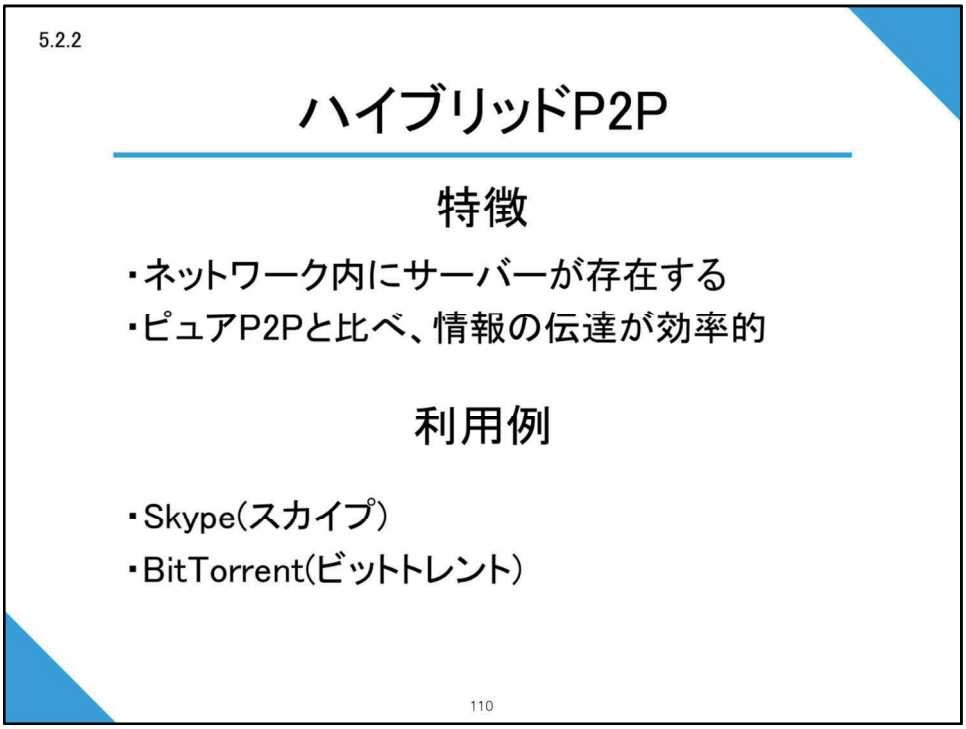
クライアントサーバー型の仕様変更と比べて、それぞれのノードでの作業が必要になるためソフトの配布などにコストがかかる。



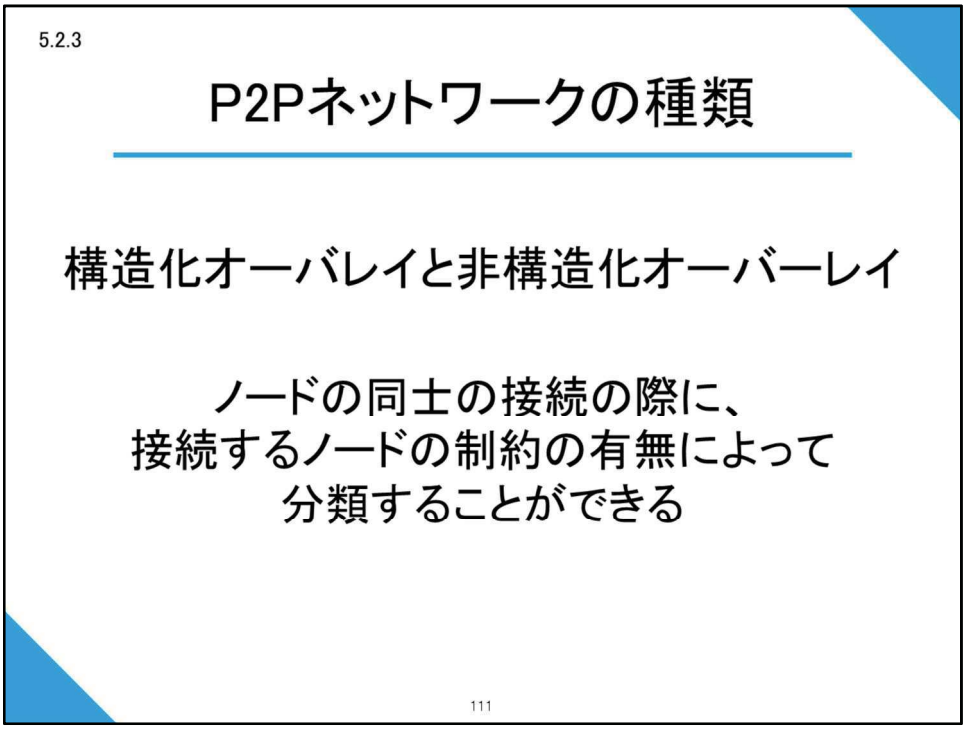
- P2Pネットワークは大きく「ピュアP2P」と「ハイブリッドP2P」の2種類に分けることができる。



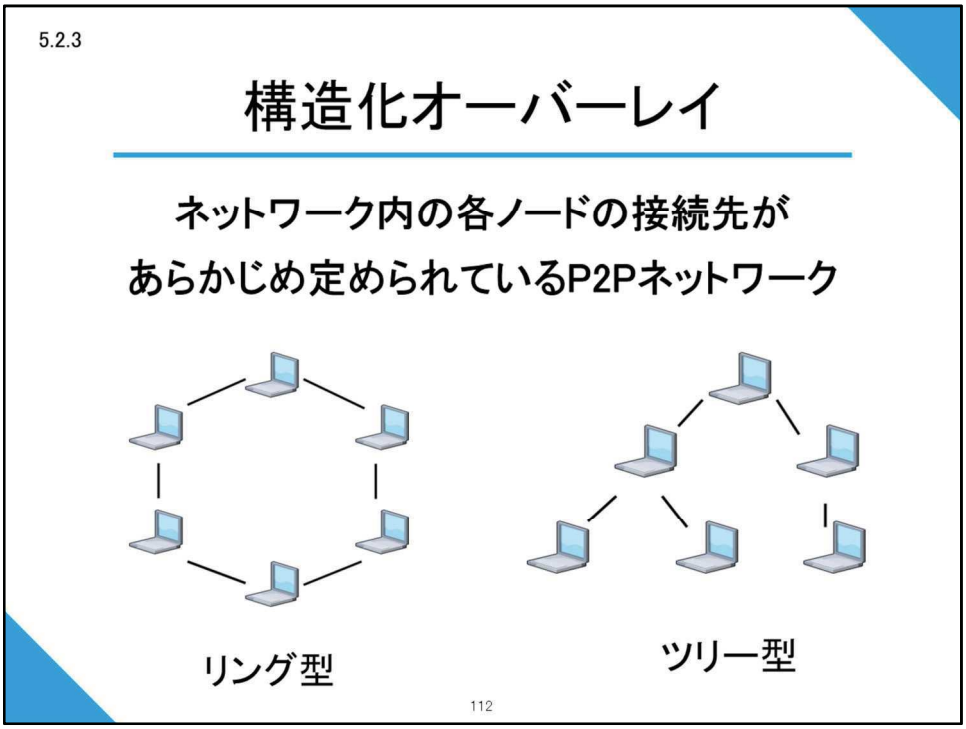
- ネットワークがノードのみで構成されているP2Pネットワーク
- ピュアP2Pの中にも、ノード間に権限の差があるものもある。
- 利用例にBitcoinやEthereumなどがある。



- ネットワークがノードだけでなく、ネットワーク内にサーバーが存在する。
- ハイブリッドP2Pのネットワーク内に存在するサーバーの役割は、目的により異なり、ネットワーク内のノードの位置を把握しておくことで、ピュアP2Pに比べて情報の伝達を効率的に行うことができるなどがある。
- 利用例には、ネット通話を行うことのできるSkypeやファイルの共有サービスであるBitTorrentなどがある。



- P2Pネットワークはノード同士の接続の際に、接続するノードの制約の有無により「非構造化オーバーレイ」と「構造化オーバーレイ」の2種類に分類する事ができる。

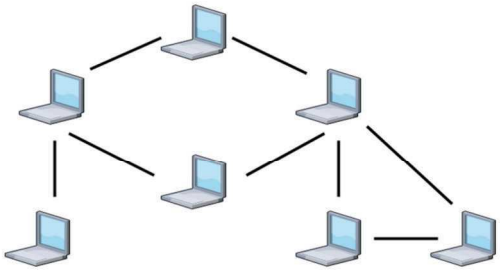


- 構造化オーバーレイとは、ネットワーク内の各ノードが接続するノードがあらかじめ定められているP2Pネットワークの方式である。
- 各ノードにIDが割り振られ、そのIDに従って接続相手が決定される。
- これにより、リング型やツリー型のオーバーレイネットワークが構築される。
- メッセージの転送効率が良い。
- 高いスケーラビリティを持つ。

5.2.3

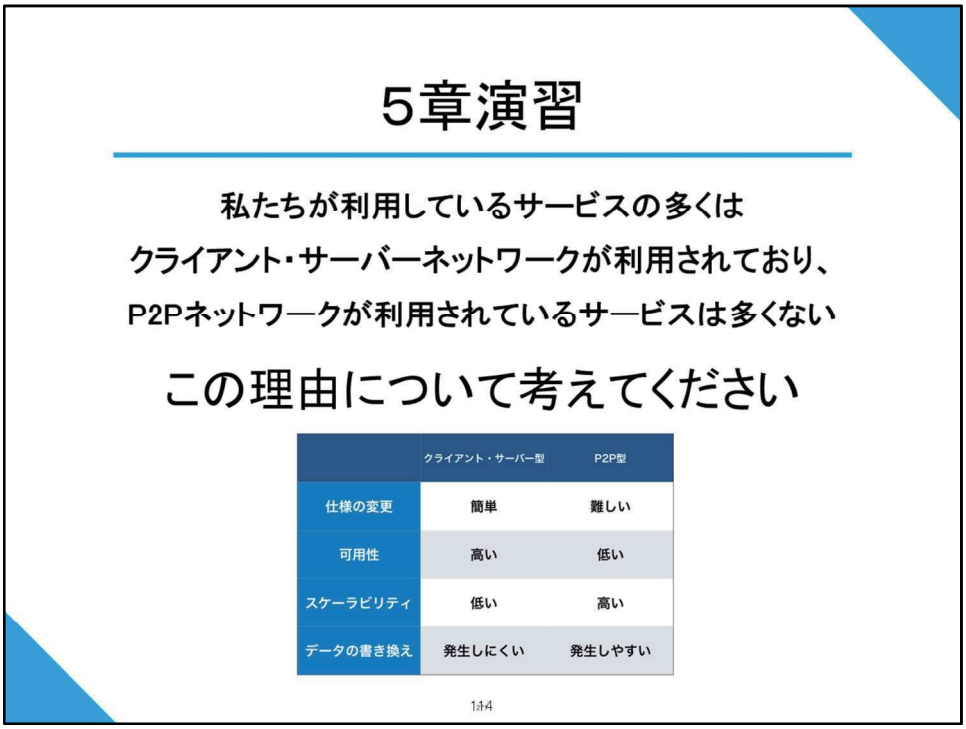
非構造化オーバーレイ

ネットワーク内の各ノードが他のノードと接続する際に、
ノードの選択に制約のないP2Pネットワーク



113

- 各ノードがネットワーク内の他のノードと接続する際に、ノードの選択に制約のない設計のオーバーレイネットワーク
- 隣接するノードを選択する際に制約がない。
- 送信相手へのメッセージの到達は保障されない。
- スケーラビリティに問題がある。



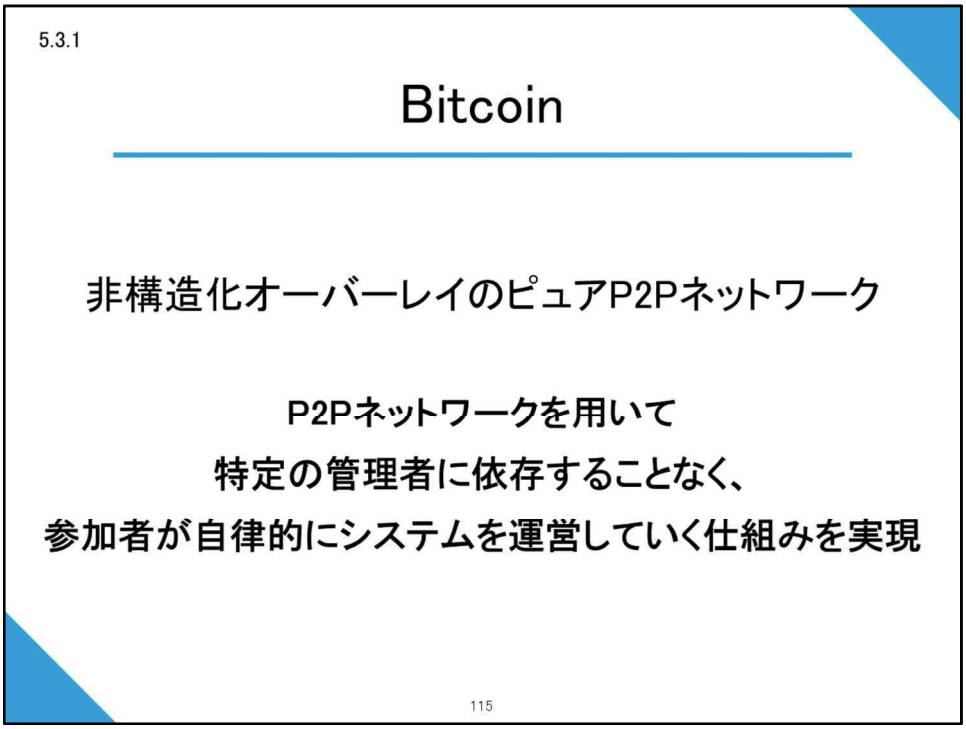
- 4～5人のグループで10分程度考え、その結果を代表者に発表してもらう。

発表の形式

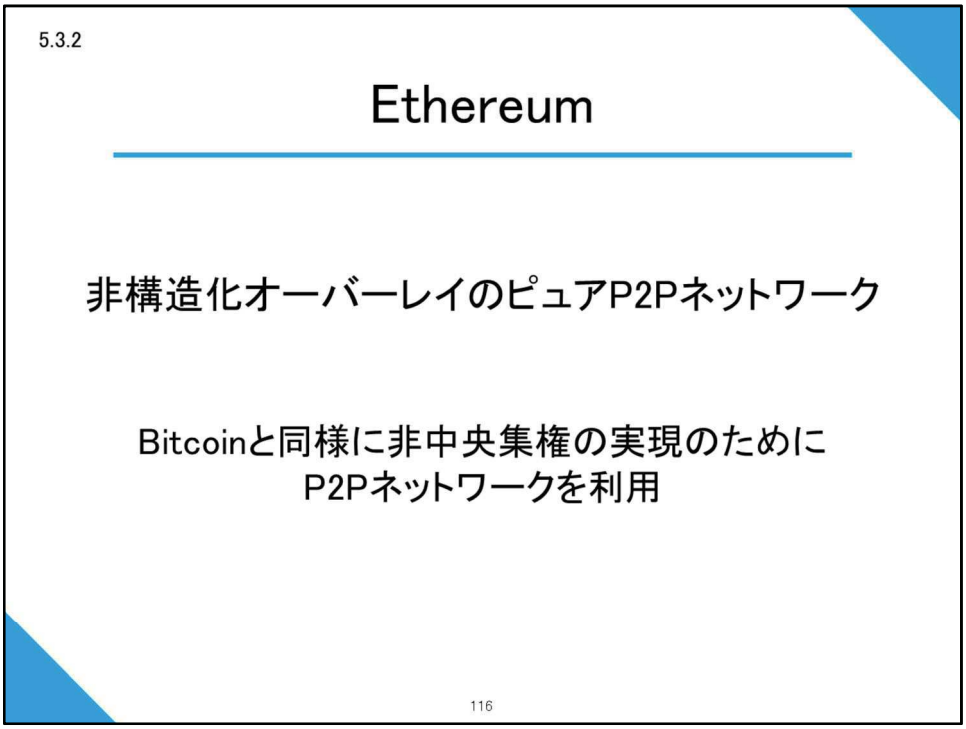
- クライアントサーバー型ネットワークに比べて、P2Pネットワークは～～～なため利用が難しいのではないか？
- P2Pネットワークの～～～の特徴が利用が難しい最大の要因ではないか？

正答例

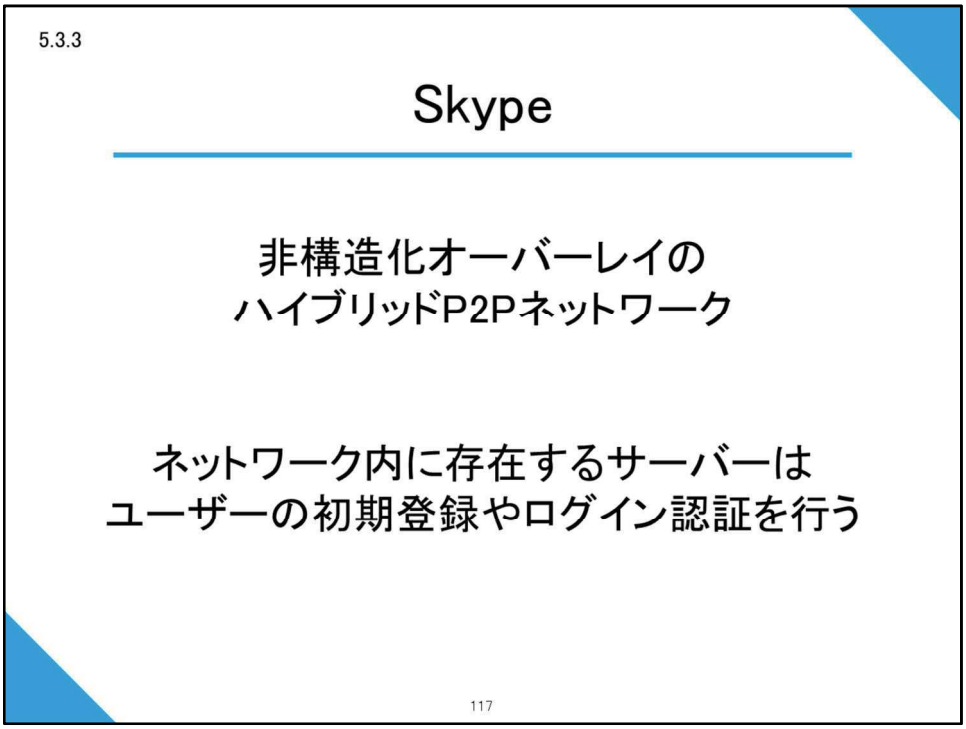
- クライアントサーバー型のネットワークに比べて、P2Pネットワークは一般のユーザーがシステムを利用するために行わねければならない作業が多い。
- P2Pネットワークに比べて、クライアントサーバー型のネットワークの方がサーバーが責任を持って管理されていることから、安定して運用される。単一障害点などの問題もあるが、ほとんど問題なく利用することができる。
- 一般の人はネットワークの仕組みに詳しくないことが大半であり、できるだけないにも考えずに使ってもらうためにはクライアント・サーバー型のほうが良い。



- 非構造化オーバーレイのピュアP2Pネットワークを利用している。
- 特定の管理者に依存することなく、参加者が自律的にシステムを運営していく仕組みを実現するために利用している。
- ネットワークに参加するためには、クラアントソフトを利用する。
- クラアントソフトには現在Bitcoinネットワークに参加しているノードのIPアドレスを提供してくれる機能がある。これによりネットワークに参加することができる。



- Bitcoinと同様にEthereumも専用のクライアントソフトを利用することで、ネットワークに参加することができる。
- Ethereumのクライアントソフトで最も利用割合が高いものは「Geth(Go-Ethereum)」である。



- 非構造化オーバーレイのハイブリッドP2Pネットワークを採用している。

- **Skypeサーバー**

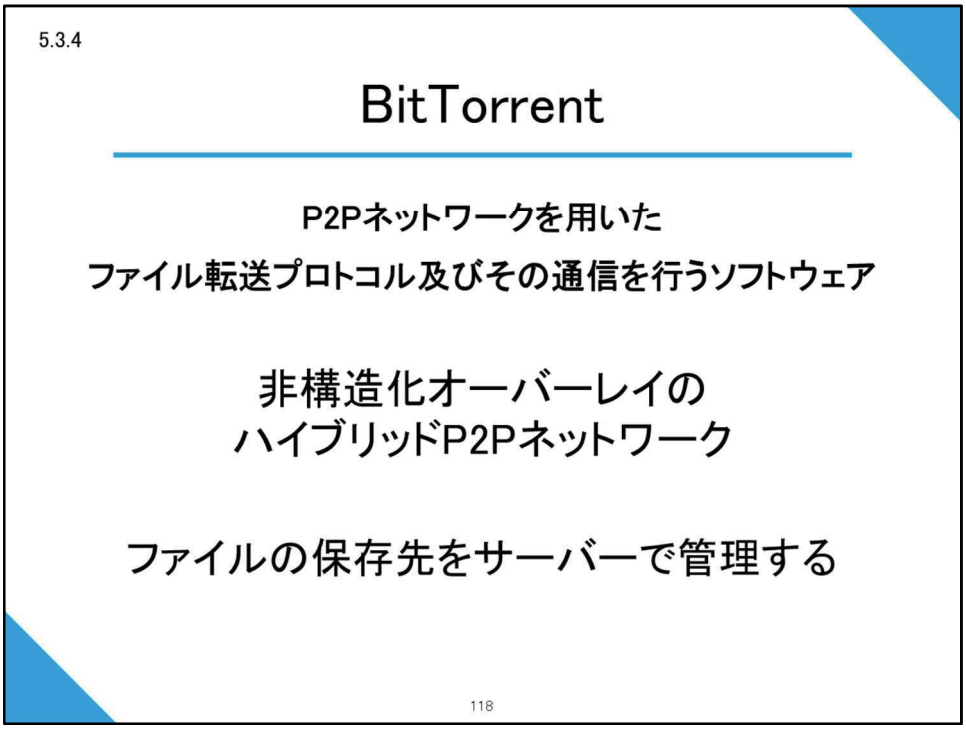
ユーザーの初期登録やログイン認証、セキュリティ上、一元管理が必要なものや、技術的に分散処理が向いていない機能を提供する。

- **通常ノード**

Skypeアプリケーションを起動すると通常ノードとしてSkypeネットワークに参加することになる。

- **スーパーノード**

Skypeに参加しているノードの情報を記録したり、探索したりする機能も担当する特殊なノードである。Skypeユーザー名やIPアドレス、ポート番号、ログイン状態などを管理する。



- P2Pネットワークを用いたファイル転送プロトコル及びその通信を行うソフトウェア

BitTorrentのネットワーク上に分散して保存されたファイルをダウンロードする際には、BitTorrentのプロトコルを実装したクライアントソフトウェアを利用する。

非構造化オーバーレイのハイブリッドP2Pネットワークを採用している。

- **トラッカー**

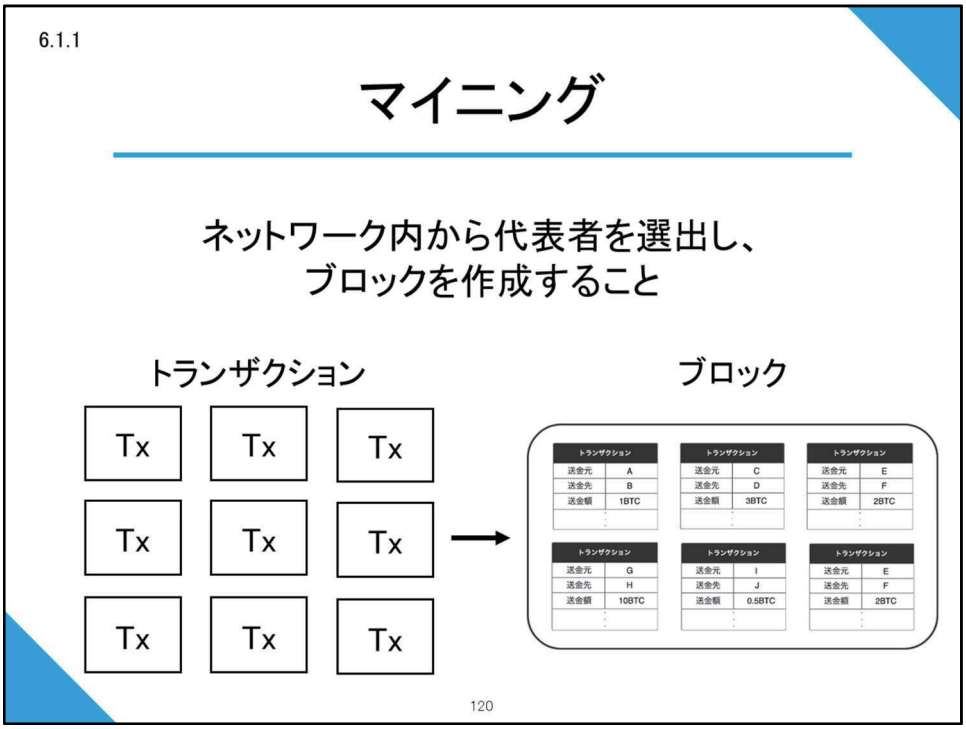
トラッカーとはファイルを保存しているノードの情報を持っているサーバーのことである。

- **トレントファイル**

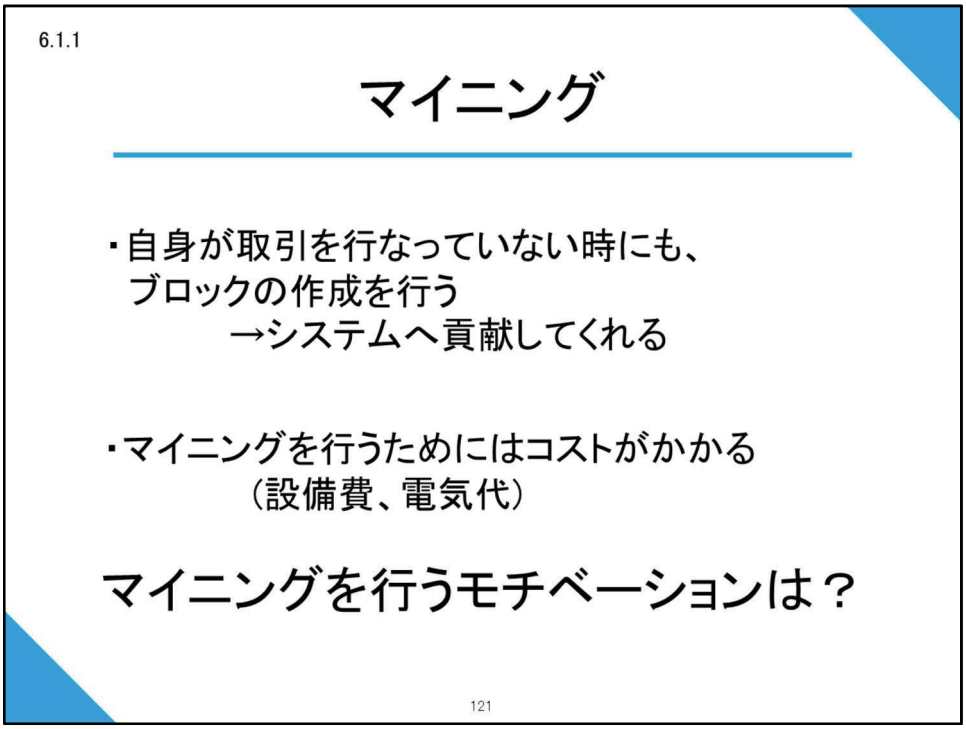
ネットワーク上にアップロードされているファイルをダウンロードする際に必要な情報が記録されているファイルである。トレントファイルは自体は、BitTorrentのネットワーク内に保存されるのではなく、BitTorrentのサービスからは独立したWebサーバー上に保存される。

6. マイニングとコンセンサスアルゴリズム

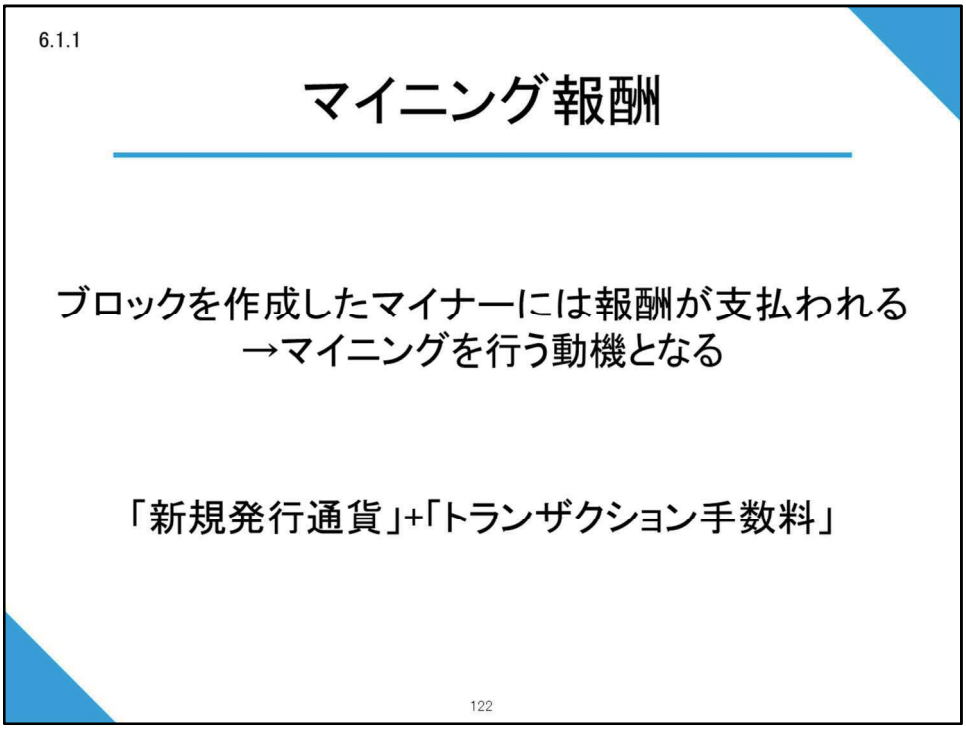
119



- マイニングとはネットワーク内から代表者を選出し、ブロックを作成することを言う。
- マイニングを行なっているノード、人のことをマイナーと言う。



- マイナーは自身が取引を行なっていないときにも、トランザクションをまとめてブロックを作ろうとしている。
- マイニングをするためには、クライアントソフトを立ち上げ、常にネットワーク内で発行されたトランザクションを受け取ることのできる状態にしておく必要がある。これには設備費や電気代などのコスト(お金)がかかる。
- なぜマイナーはコストを投じてまで、わざわざブロックを作ろうとしてくれるのか？

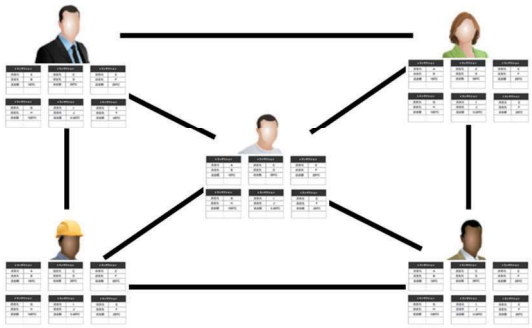


- マイナーは代表者に選ばれブロックを作成すると、報酬をもらうことができる。この報酬をマイニング報酬と呼ぶ。
- 報酬はマイニングに参加しているブロックチェーンの内部通貨で支払われる。
- マイニング報酬は「新規発行通貨」と「トランザクション手数料」の合計である。

6.1.1

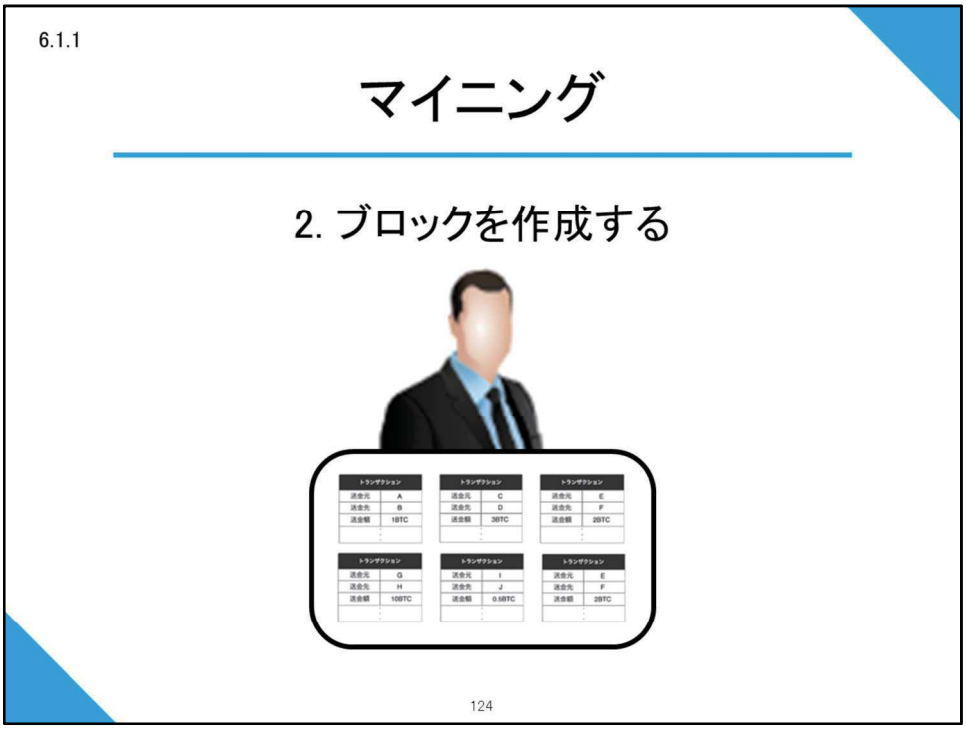
マイニング

1.ネットワークに参加し、トランザクションを集める



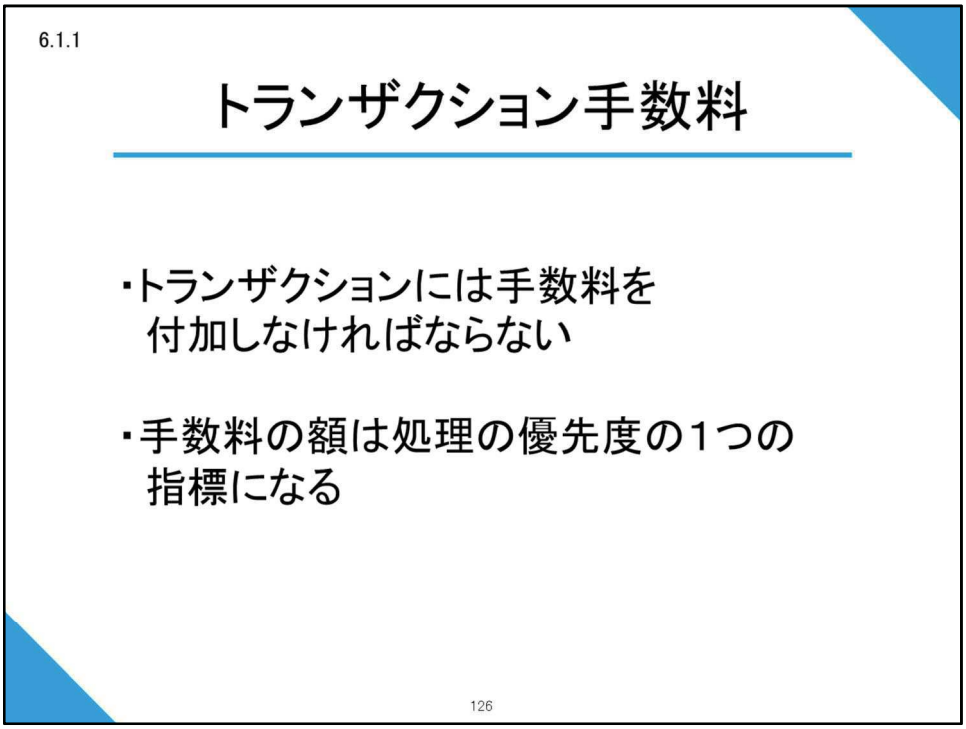
123

- スライドの図のネットワークを構成する5つのノードがマイナー
- マイナーはブロックチェーンのネットワークに参加して、トランザクションを手元に集める。
- 左上のノードがブロックを作成する代表者に選出されたとする。



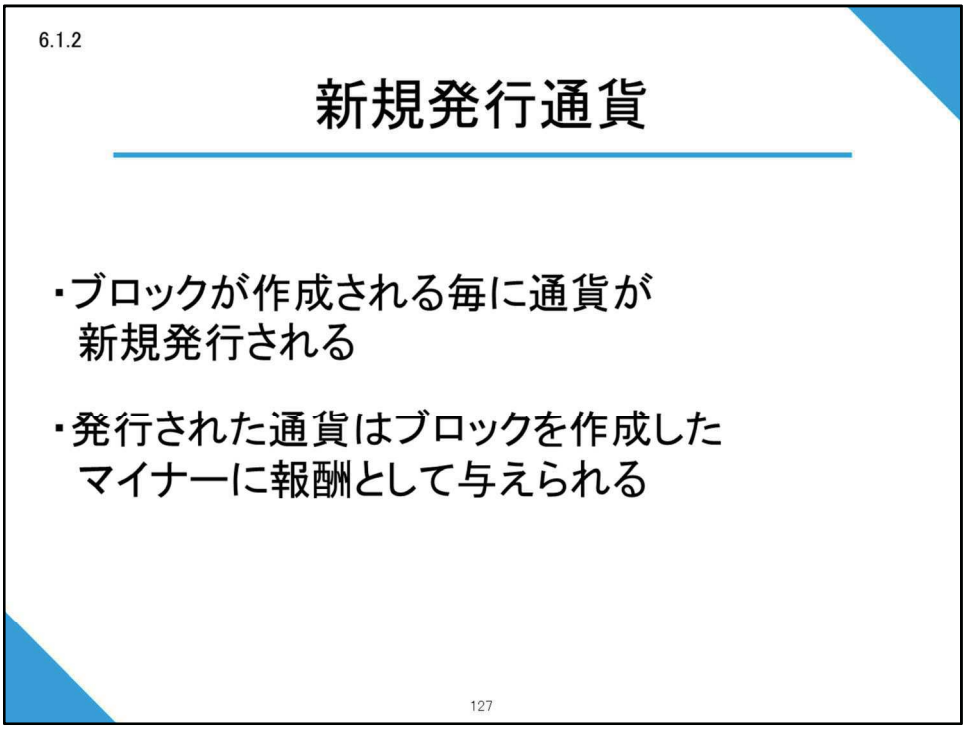
- 複数のトランザクションをまとめて、ブロックを作成する。

- ブロックを作成した報酬がもらえる

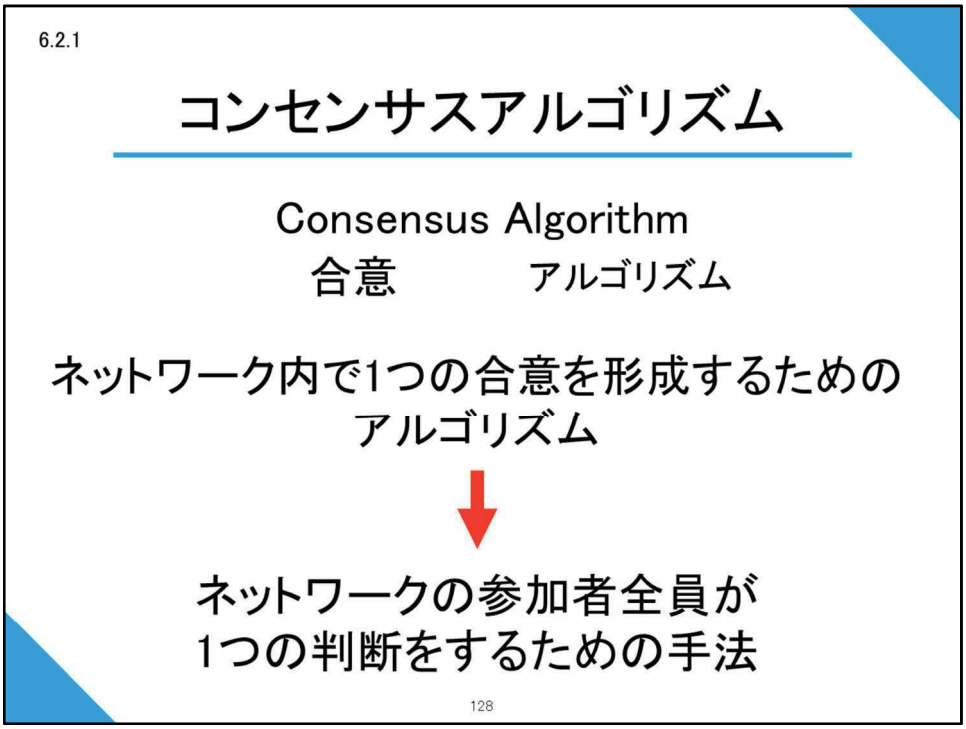


- 多くのパブリックブロックチェーンではトランザクションを発行する際に、手数料を付加しなければならない。これがトランザクション手数料と呼ばれる。
- トランザクション手数料は一定額ではなく、トランザクションの発行者が自由に定めることができる。
- 高いマイニング手数料をつけると、マイナーが優先的に処理を行なってくれる。
- マイナーは自身が作ったブロックに含まれるトランザクションにつけられた手数料を自身の報酬にすることができる。

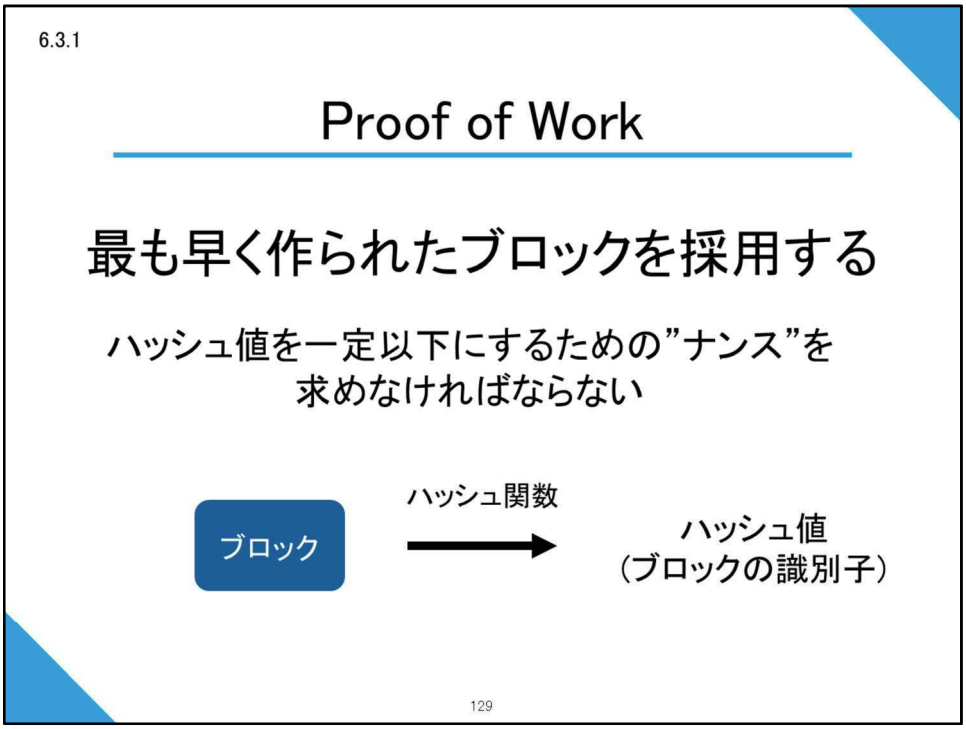
- Bitcoinのトランザクション手数料については次のサイトで確認することができる。
(https://www.blockchain.com/ja/charts/cost-per-transaction)



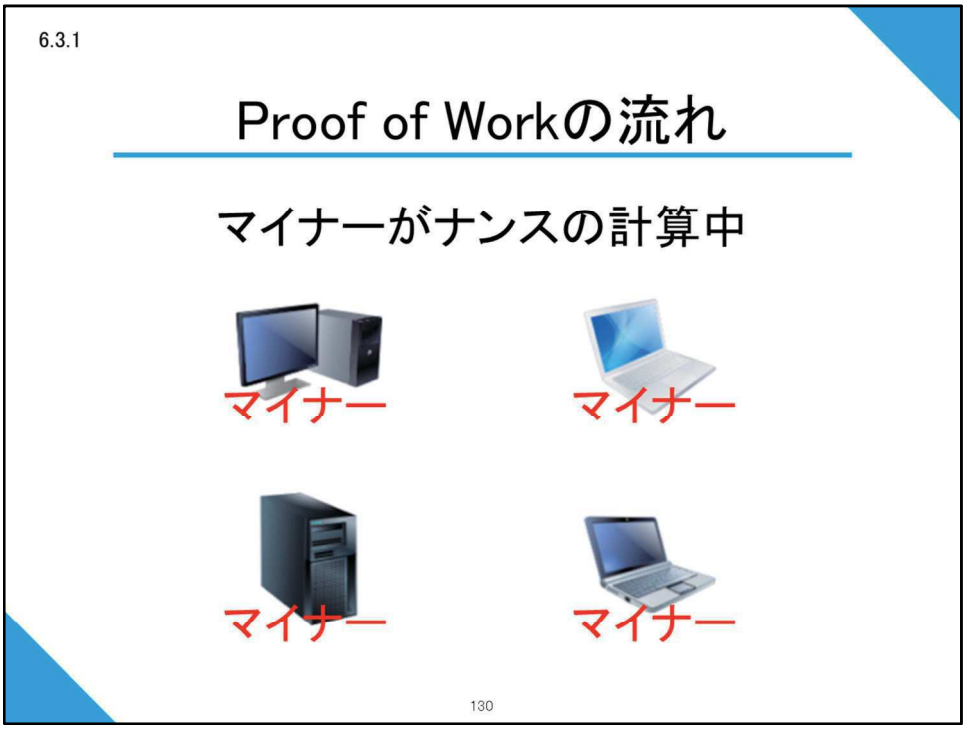
- 仮想通貨の新規発行は、ブロックが作成されるタイミングで行われる。
- 発行された通貨はブロックを作成したマイナーへの報酬となる。
- ブロックが作成される際に、何もないところから新たに通貨が発行されることが、金の採掘(mine)と似ていることから、マイニング(mining)と呼ばれる。



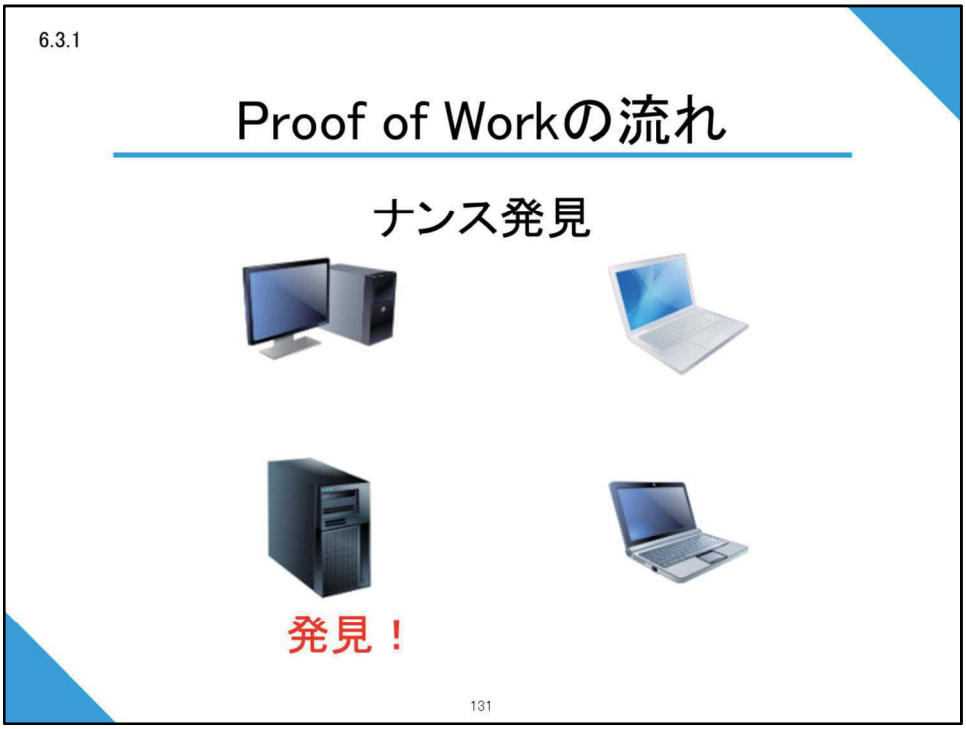
- ブロックチェーンネットワーク内で1つの合意を形成するためのアルゴリズムである。
- さらに言い換えると、正しい記録のみをブロックチェーンに書き込むための方法である。
- このコンセンサスアルゴリズムの発明がブロックチェーンの最大の技術革新と言える。



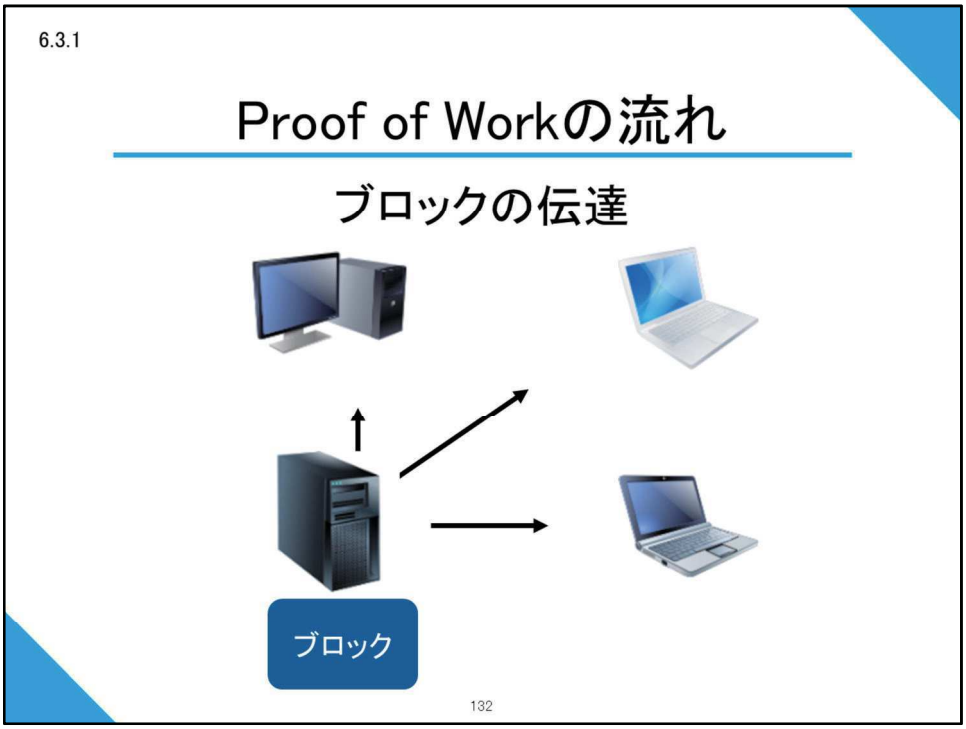
- コンセンサスアルゴリズムの1つである。
- 2008年に「Satoshi Nakamoto」により考案された。
- Proof of Workは初めて実用的に使用することのできるコンセンサスアルゴリズムである。
- Bitcoinで利用されている。
- Proof of Workでは、最も早く作られたブロックが採用される。
- ブロックを作る際には、トランザクションをまとめるだけでなく、ブロックの中身をハッシュ関数にかけて、そのハッシュ値が一定以下にならなければ、正しいブロックとしては認められない仕組みになっている。
- ブロックのハッシュ値を操作するためには、ブロックの項目の1つである、ナンスを操作する必要がある。
- ハッシュ関数の特性から狙ったハッシュ値を出力することはできないため、何度も繰り返し試行することが必要になる。



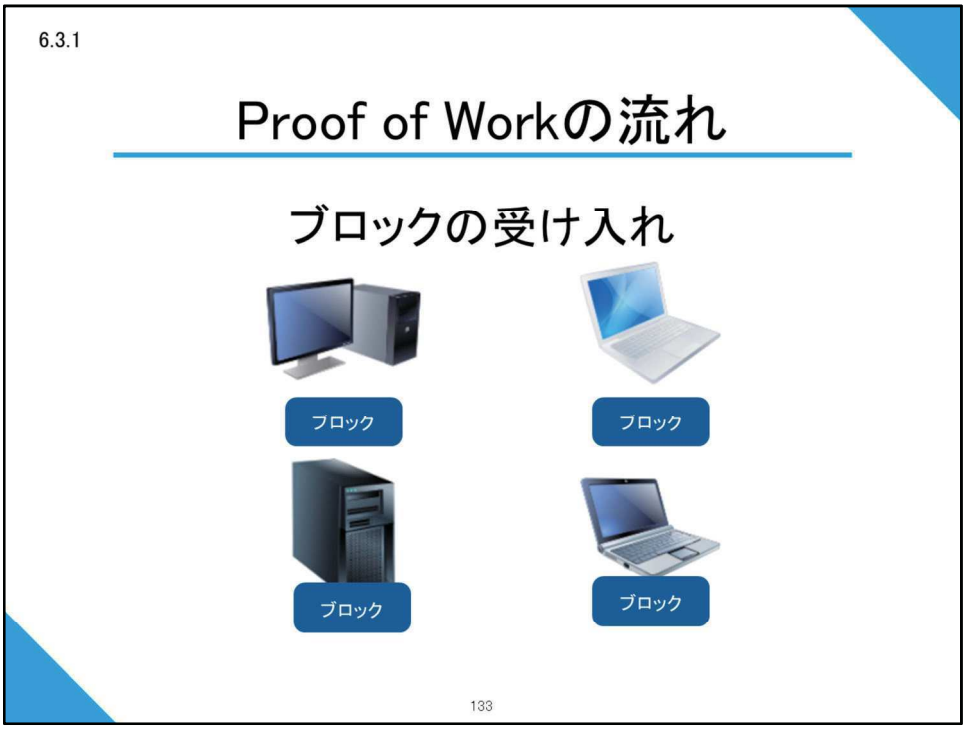
- マイナーがナンスを変更してはハッシュ値を求め、ブロック作成の条件を満たすナンスを探している。



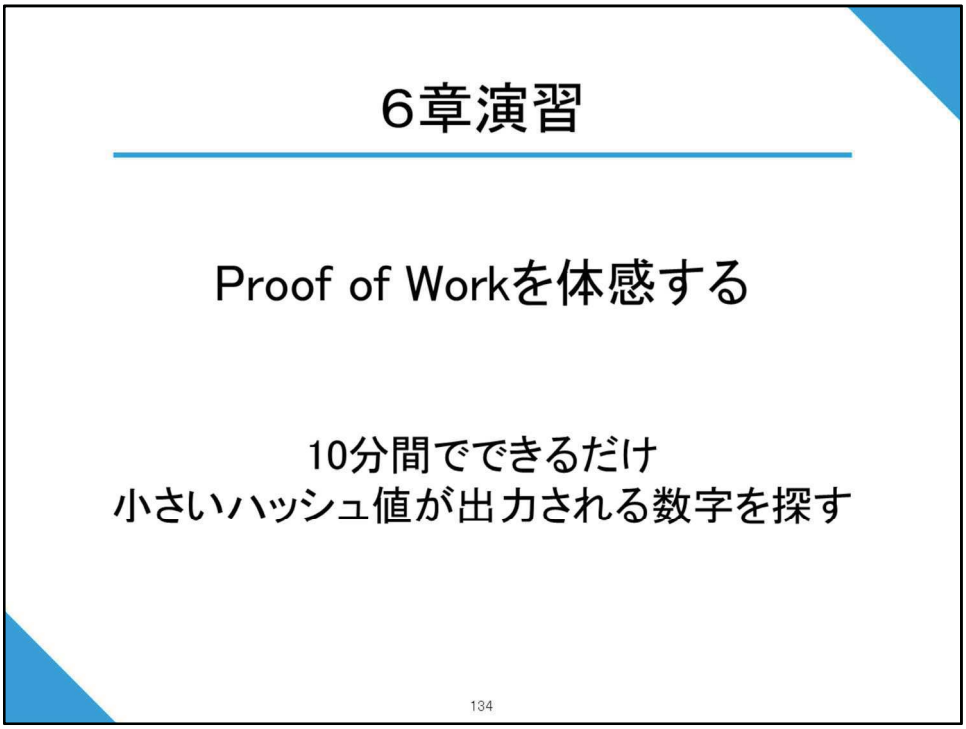
- 1人のマイナーがいち早くハッシュ値を一定以下にするナンスを発見する。



- 適切なハッシュ値となるナンスを見つけると、正しいナンスを含んだブロックを作成しネットワークに伝達する。



- 他のマイナーから新たなブロックが届くと、検証作業を行う。
- 正しいブロックであると判断すると、このブロックに対するナンスの計算競争が終了し、このブロックを親として持つ次のブロック作成の競争に移る。



準備

- 1人1台PCを利用する
- 巻頭で準備した仮想マシンを立ち上げる
- 仮想マシン上でターミナルを開く
- ターミナルで irb と入力する
- require ‘digest’ と入力すると、ハッシュ関数が利用できるようになる

Proof of Workの体験

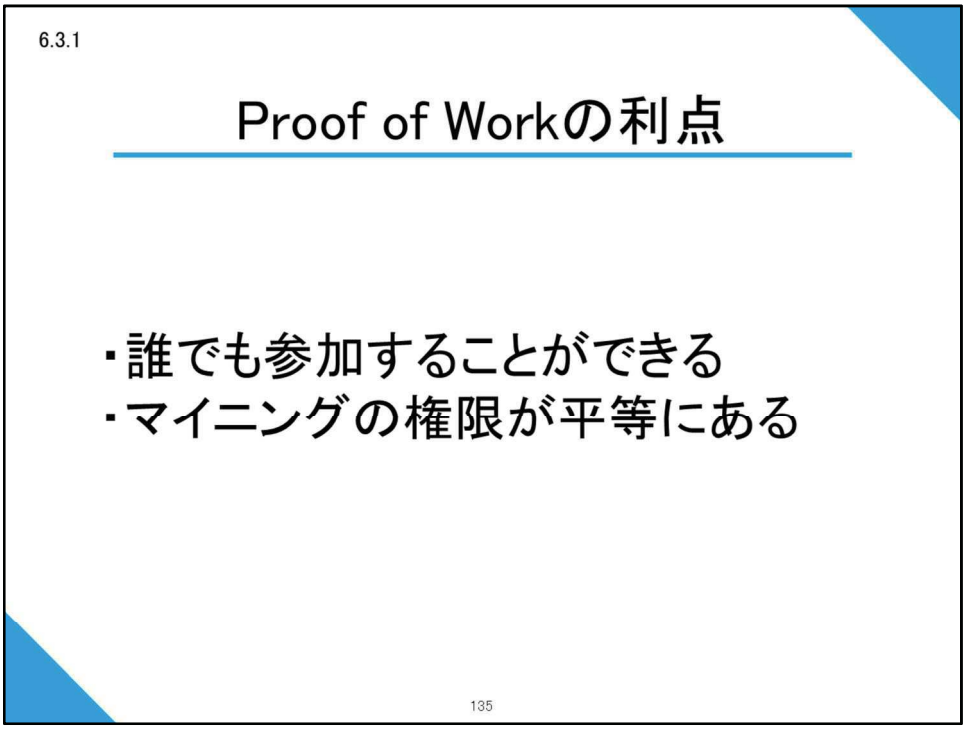
- SHA-256に数字を入力し、できるだけ小さいハッシュ値を求める。
- 制限時間は10分(Bitcoinでは平均して10分に1回ブロックが作られる)で”00”から始まるハッシュ値が出力された場合には、入力値をメモしておく。

BitcoinのProof of Workの確認

- Bitcoinのブロックチェーンエクスプローラーを開き、実際のブロックのハッシュ値を確認する。
  (https://www.blockchain.com/ja/explorer)

ハッシュを繰り返し求めるためのプログラム(Ruby)

```
require "digest"
end_number = 1000
number = 0
while number <= end_number
    hash = Digest::SHA256.hexdigest(number.to_s)
    puts hash,number if hash.start_with?("00")
    number += 1
end
```

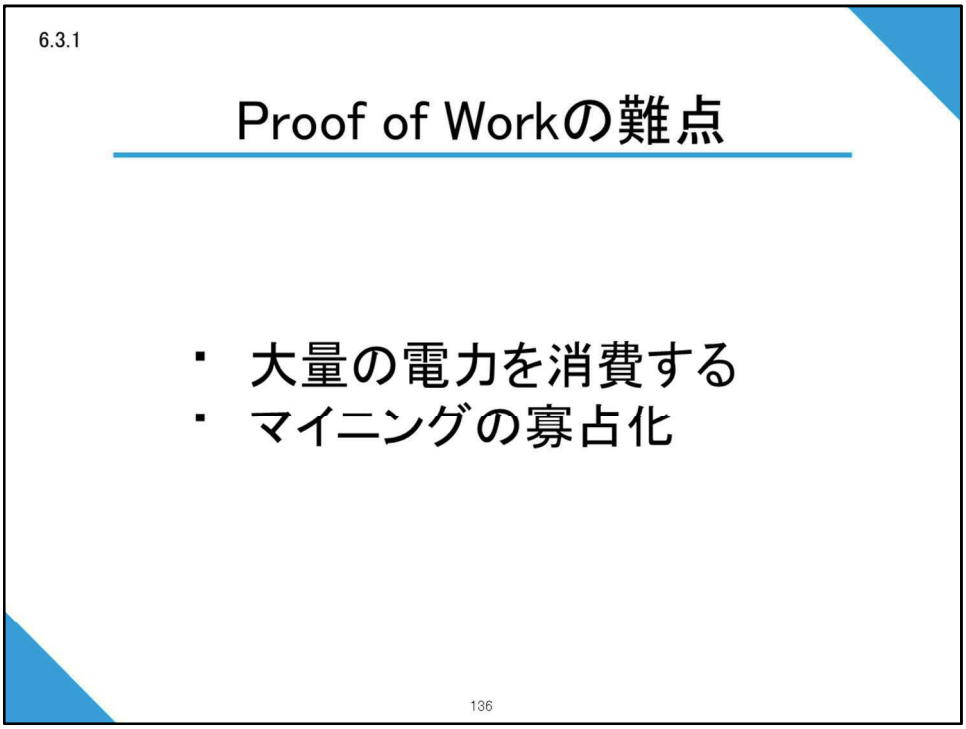


- 誰でも参加することができる

マイニングにはWebサイトからソフトウェアさえ入手すれば誰でも参加することができる。

- 権限が平等にある

マイニングに参加する段階では、マイニングの権限は参加者全員に平等にある。ハッシュの計算を速く行うために投資することにより、マイニングの成功率が高まる。



- **大量の電力を消費する**

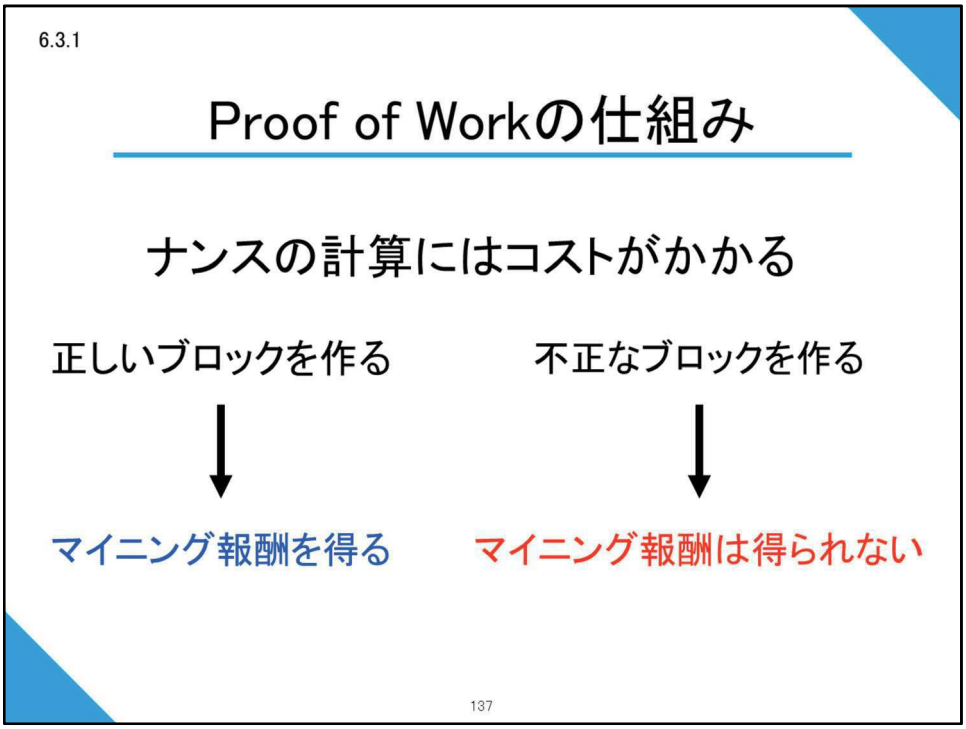
世界中のマイナーが大量の計算資源を投じて、マイニングを行うため、大量の電力をる。1年間でBitcoinのマイニングに投じられている電力は、国家の消費電力ランキング前後に相当する。

- **マイニングの寡占化**

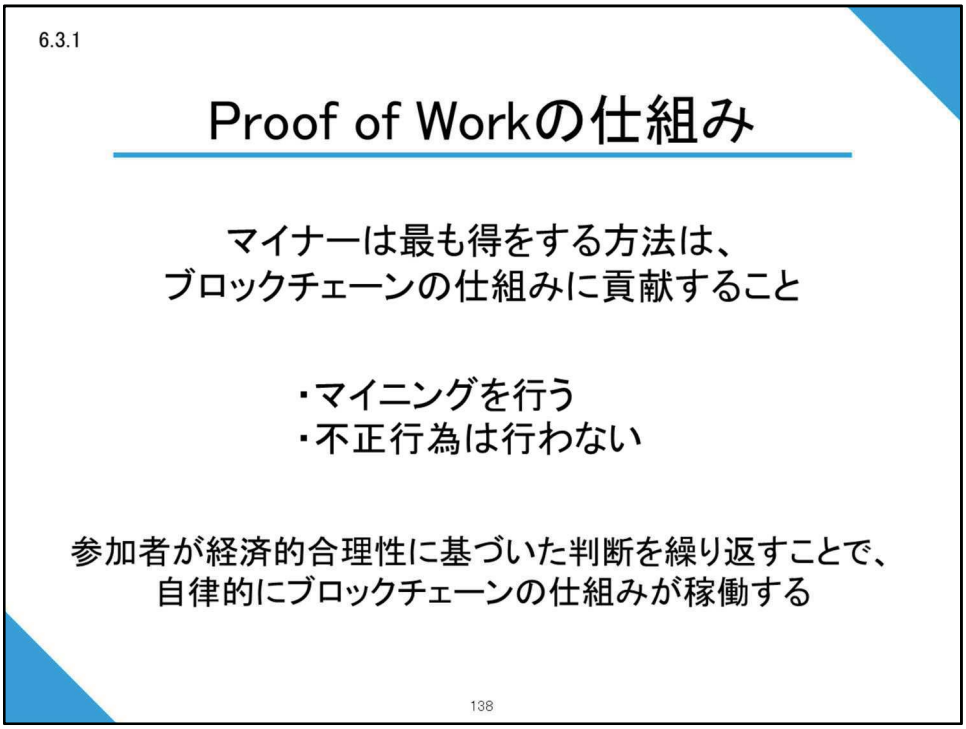
マイニングには誰でも参加することができるが、実際にブロックを作成することがで大量の計算資源を保有している一部のマイナーのみである。このような状態はブロッンの安全性が低下した状態であるといえる。詳細については、後に説明する。

Bitcoinのマイニングに関するデータを参照する

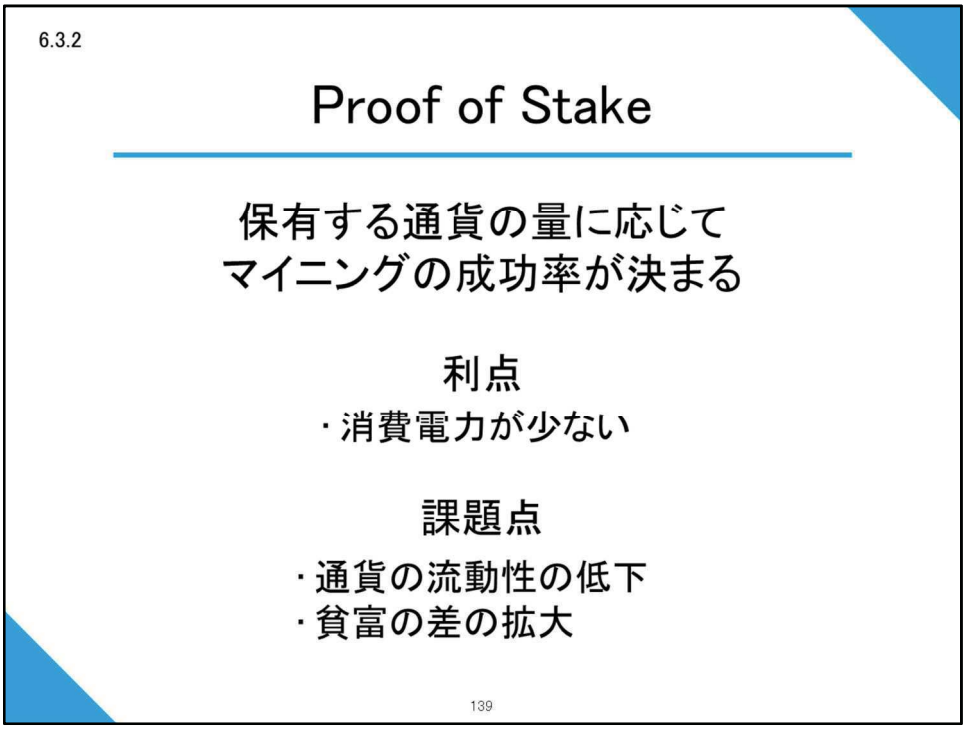
- HashRateについて: https://www.blockchain.com/ja/charts/hash-rate
- Difficultyについて: https://www.blockchain.com/ja/charts/difficulty
- HashRateの分布について: https://www.blockchain.com/ja/pools



- Proof of Workではナンスの計算にコンピュータなどの初期投資や電気代などのコストがかかる。
- 正しいブロックを作成するとマイニング報酬を得ることができ、採算が取れる。
- 不正な取引を含んだブロックを作成することや、条件を満たさないナンスを含んだブロックを作成すると、他のマイナーの検証で弾かれてしまい、報酬を得ることはできず、ナンスの計算にかかった費用は無駄になる。



- Proof of Workに参加してマイナーが最も得をするための方法は、マイニングを行うことや、不正行為を行わないこと。つまり、ブロックチェーンの仕組みに貢献することである。
- マイナーが自身にとって得になる行動(経済的合理性に基づいた判断)を繰り返すことで、ブロックチェーンの仕組みは管理者を必要とせずに自律的に稼働することができる。



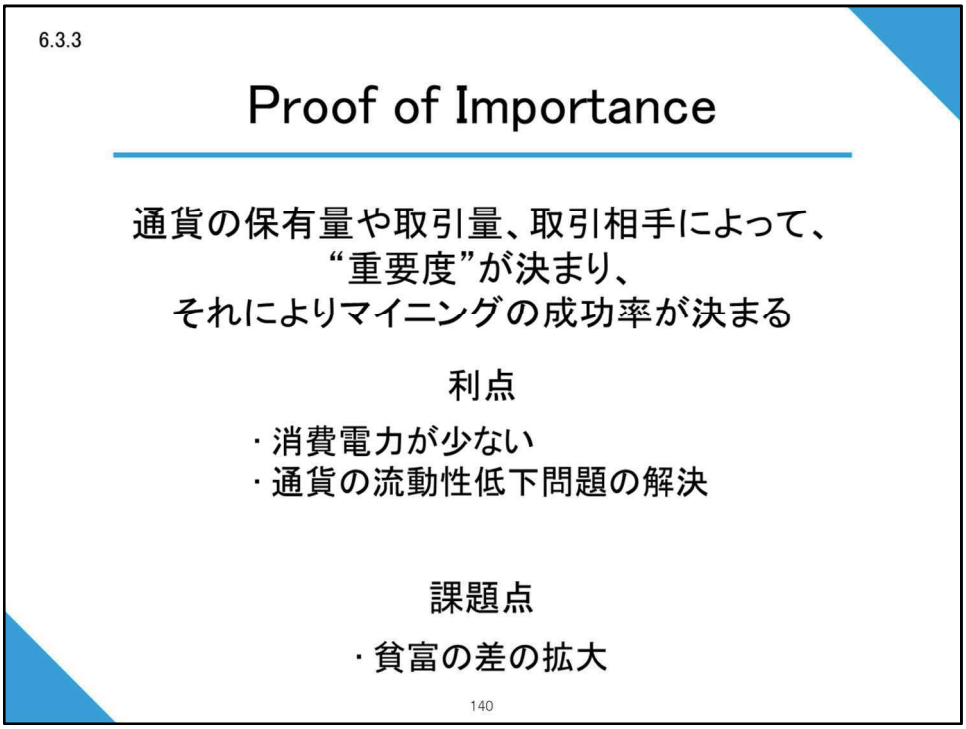
- 保有する通貨の量に応じて、マイニングの成功率が決まるコンセンサスアルゴリズムである。
- Ethereumは現在、Proof of Workを採用しているが、今後Proof of Stakeに移行される予定になっている。

利点

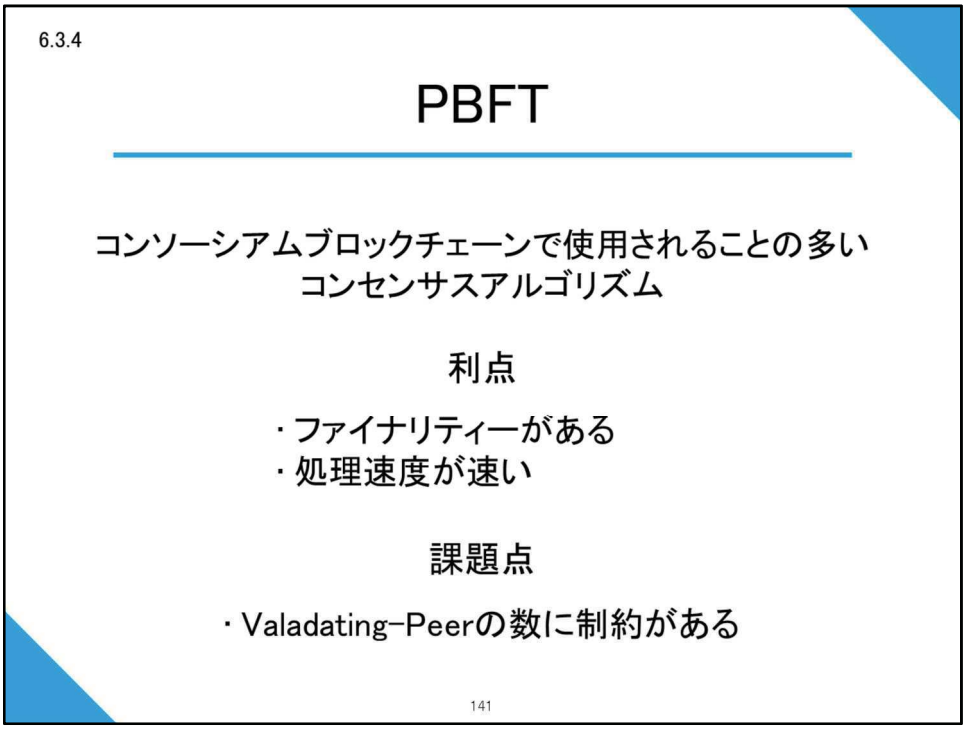
- Proof of Workと異なり、計算資源をベースとした競争は行われないので、消費電量が少ない。

課題点

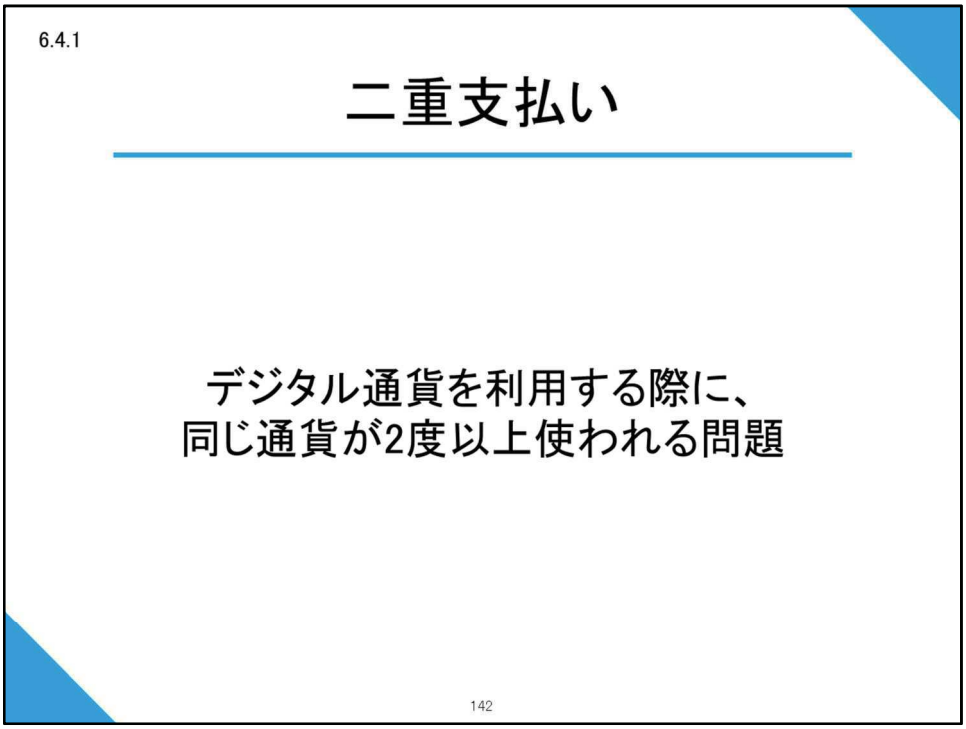
- 保有する通貨の量が多ければ多いほど、マイニングの成功確率が高くなるので、通貨の抱え込みが増え、流動性が低下するという問題がある。
- また、通貨を多く持っている人のところに、さらに通貨が集まる仕組みとなっているので、貧富の差が拡大するという問題もある。



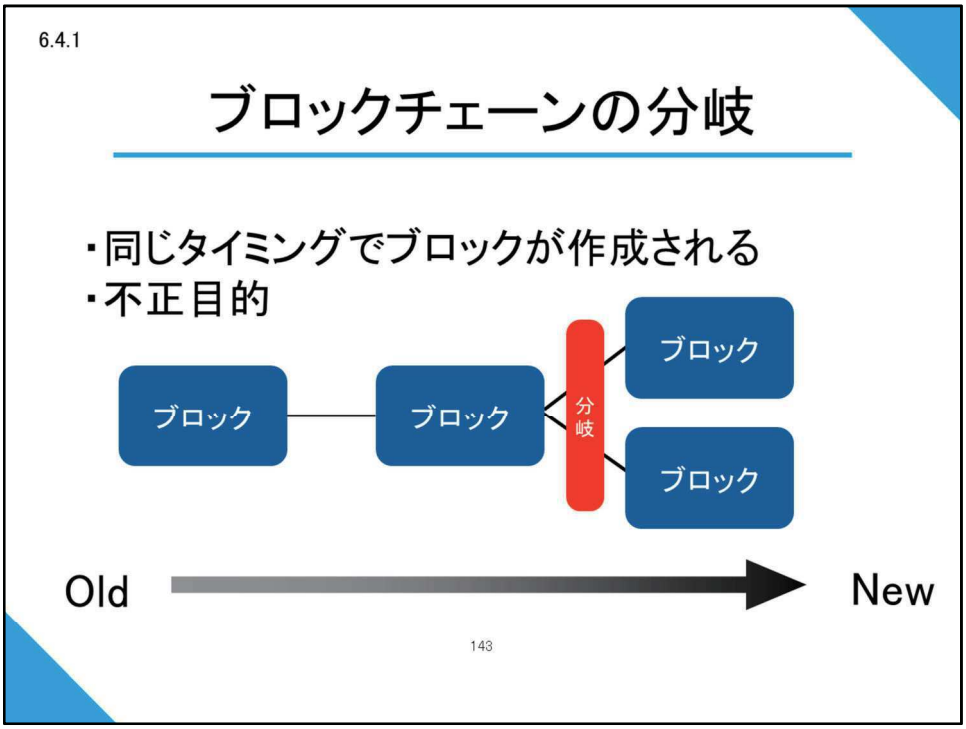
- Proof of Stakeに手を加えたコンセンサスアルゴリズムである。
- Proof of Stakeでは通貨の保有量のみが指標になっていたものを、通貨の取引量、取引相手なども考慮され、重要度という指標が決められた。これの指標によってマイニングの成功確率が決まる。
- Proof of Stakeでは通貨の取引量を指標に組み込むことで、通貨の流動性の低下を抑えることができる。
- ・貧富の差に関しては、通貨を多く持っている人の取引量が必然的に多くなるため、解決されたとは言えない。



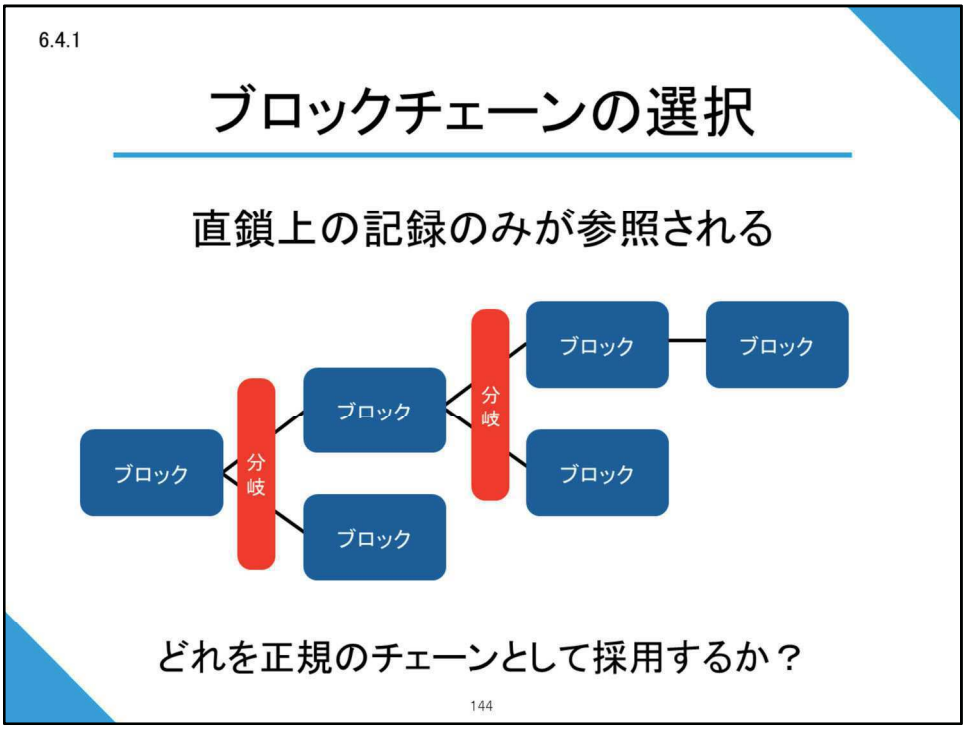
- コンソーシアムブロックチェーンで使用されることの多いコンセンサスアルゴリズムである。
- 今回紹介した3つのアルゴリズムと大きく異なるのは、ブロックの作成を誰もが行うことができるのではなく、ネットワーク内の代表者のみが行うことができる点である。
- Validating-peerの合意によってのみブロックが作成されるため、取引終了のタイミングがわかりやすい。
- Proof of Workなどのように適切なハッシュ値を求めるための計算を必要としないため、処理速度が速い。
- Validating-Peerが一定数以下になるとPBFTが機能しなくなる可能性がある。
- ノード数が増加すると飛躍的に通信量が増加し、それに伴い処理に時間がかかるようになる。



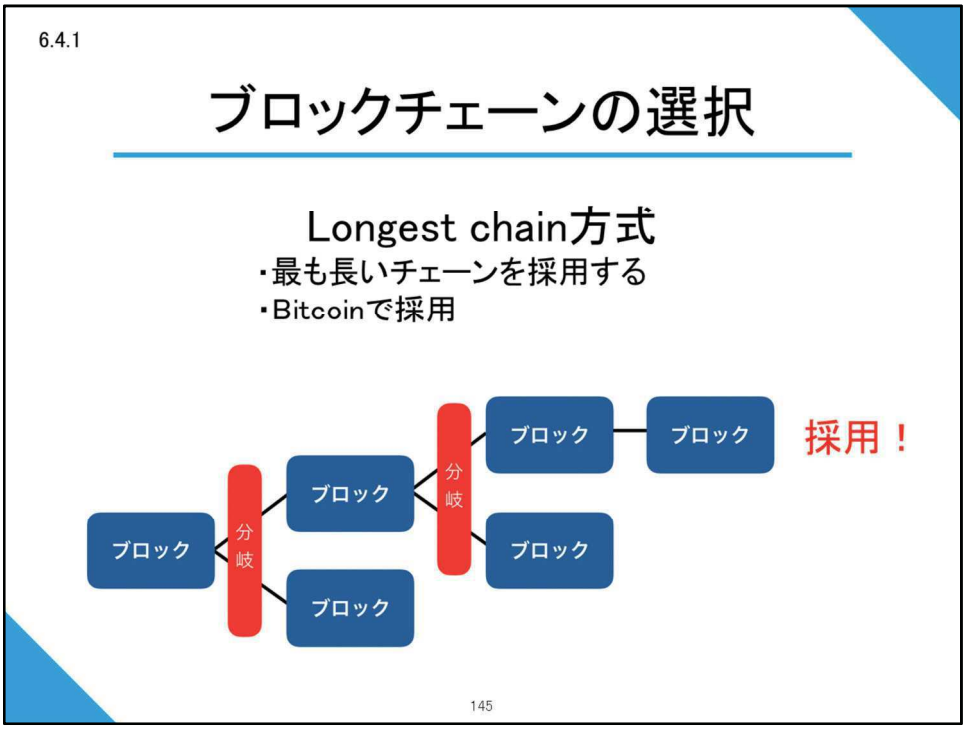
- 仮想通貨をはじめとした、デジタル通貨には「二重支払い」と呼ばれる、同じ通貨が2度以上使われる問題がある。



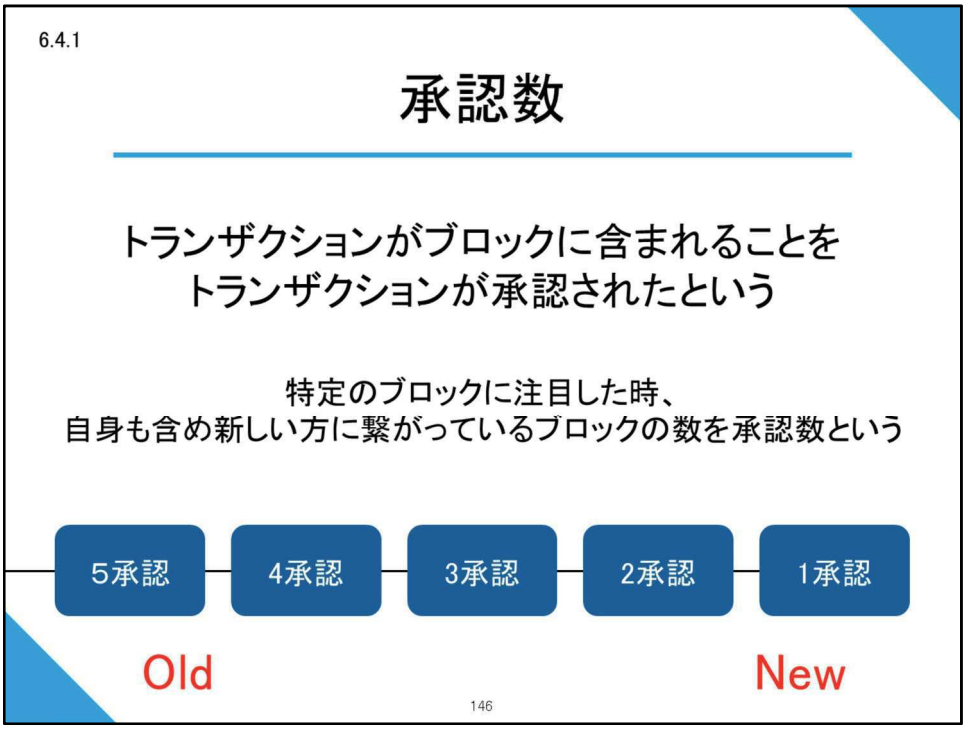
- 基本的にブロックチェーンは1つのブロックに対して、1つのブロックが繋がっている。
- 時々、1つのブロックに2つ以上のブロックが繋がり、ブロックの分岐が発生することがある。この原因としては、「同じタイミングでブロックが作成される場合」と、「不正目的」が考えられる。



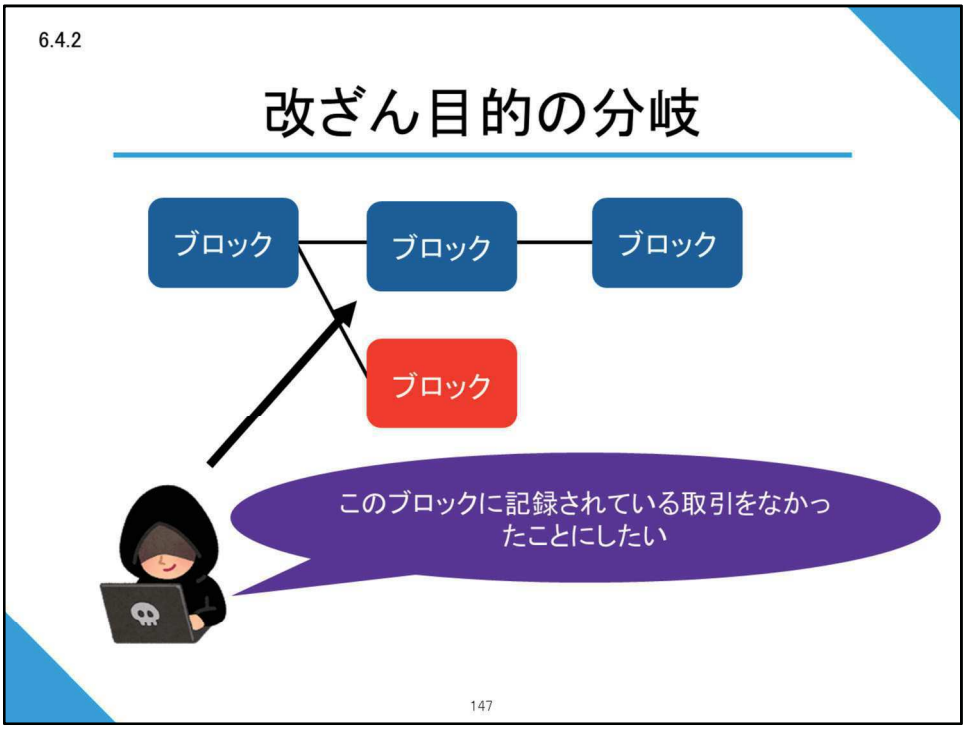
- ブロックチェーンでは、直鎖上のブロックに含まれている記録しか参照しない。
- スライドのような場合において、どのブロックチェーンを正規のブロックチェーンとするか決めなければならない。(3つのチェーンが存在している状態)



- ブロックチェーンは分岐が発生した際に1つのチェーンに収束させる仕組みが作られている。
- 多くのブロックチェーンでは最も信頼のおけるチェーンを正規のチェーンとして採用する。
- 信頼の置けるチェーンを決めるための方法はいくつかあり、ブロックチェーンによって採用している方式は異なる。
- Bitcoinに採用されている方式はLongest Chain方式と呼ばれる方式で、言葉の通り最も長いチェーンを正規のブロックチェーンとする。

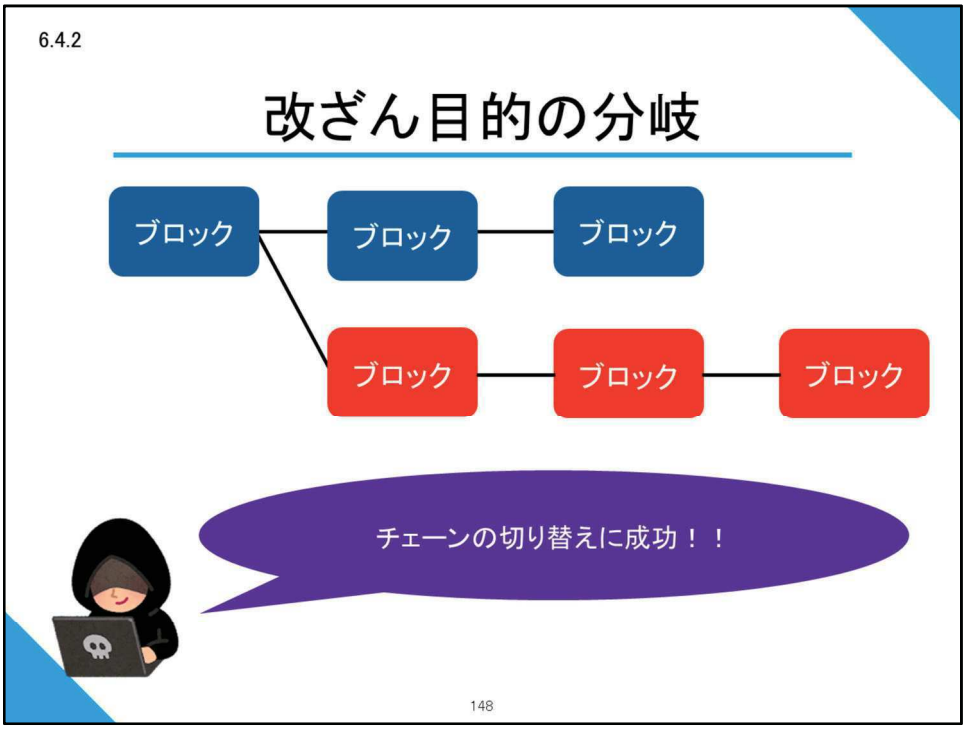


- トランザクションがブロックに含まれることをトランザクションが承認されたという。
- 特定のブロックに注目した時、自身も含め新しい方に繋がっているブロックの数を承認数という。
- 時間の経過に連れてブロックが作成されるため、承認数は増えていく。
- 承認数についての詳細は51%攻撃の部分で説明する。

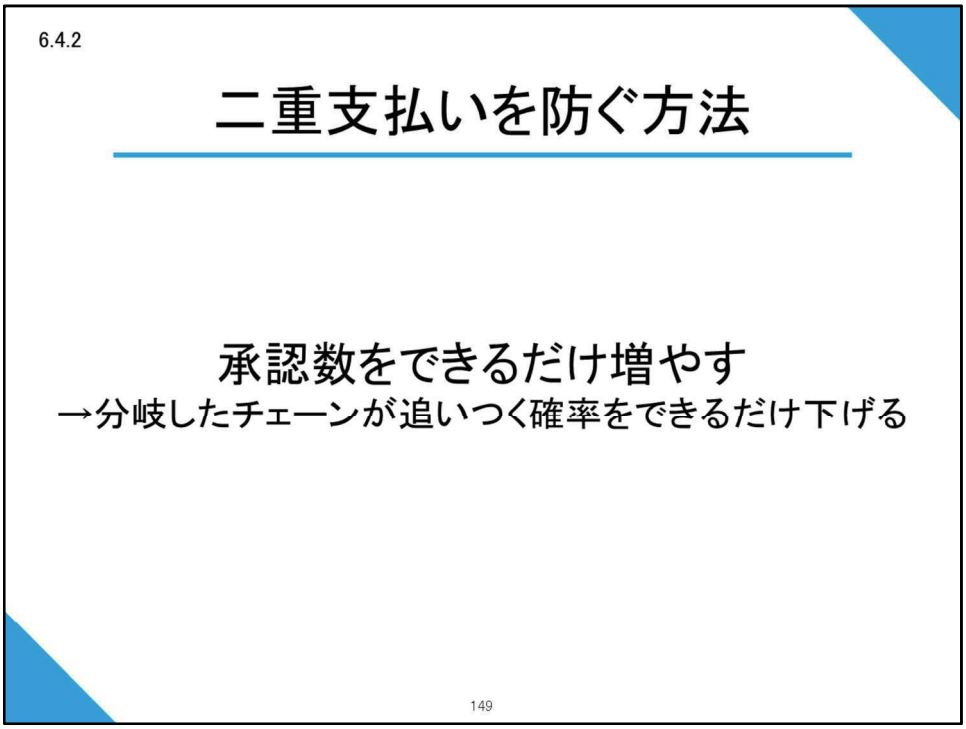


仮想通貨の二重支払いについて

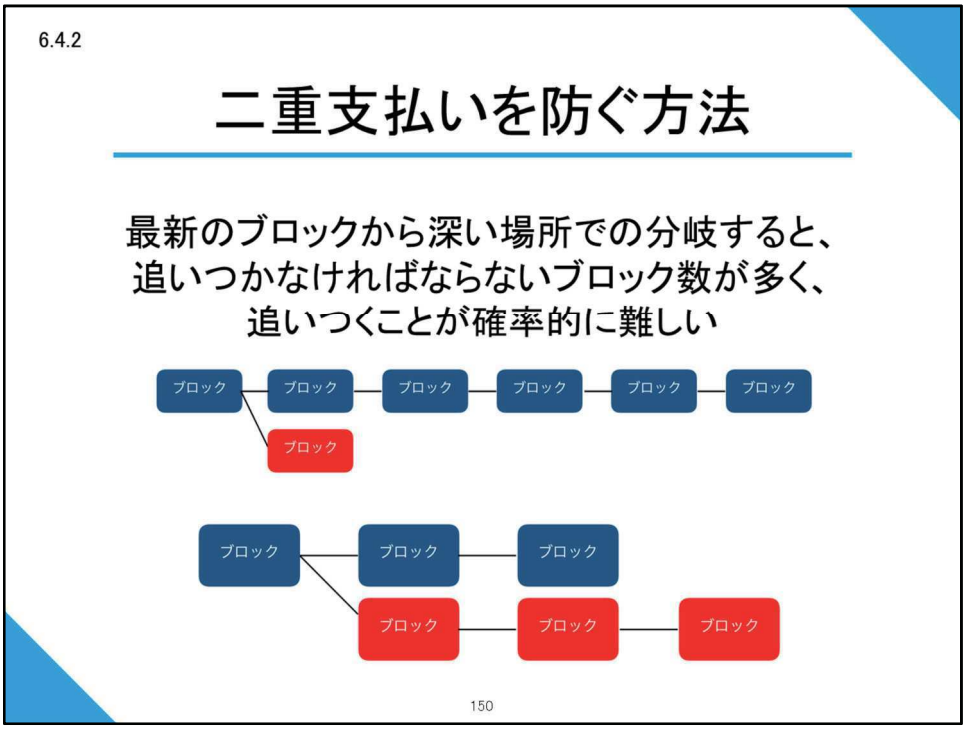
- あるブロックに含まれる取引をなかったことにしようと考える。(支払いに使った通返し、再度利用しようとする)
- 目的のブロックより前のブロックから分岐を発生させる。
- このままでは、分岐させて作ったブロックチェーンは正規のものより短く、このブまれる取引は正当なものであるとはみなされず、安全上の問題はない。



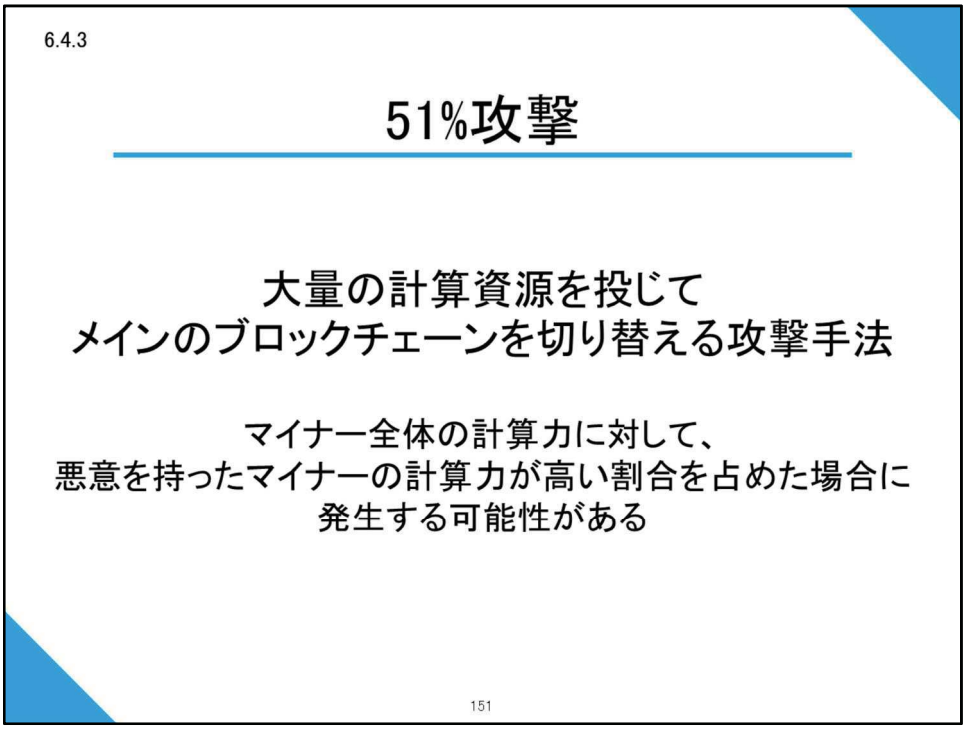
- 攻撃者は分岐させて作ったブロックチェーンを正規のブロックチェーンよりも長く伸ばす。
- これにより、メインのチェーンが切り替わりが発生する。
- 元のチェーンに含まれていた取引は取り消され、攻撃者は通貨を取り戻すことができる。



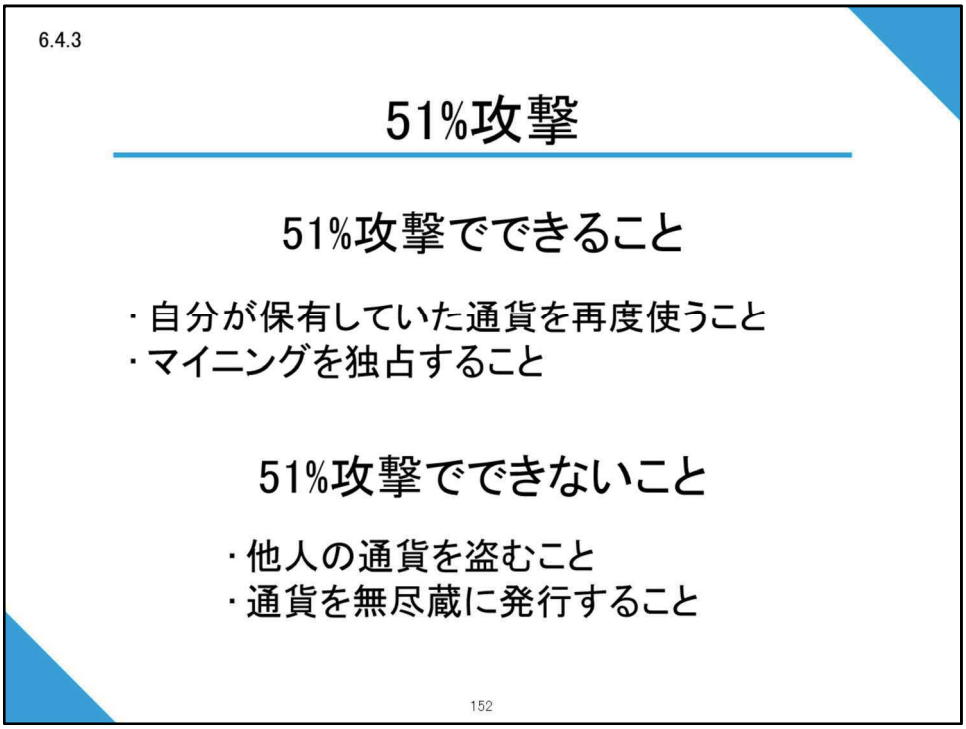
- 二重支払いを防ぐ唯一の方法は、発行したトランザクションが含まれるブロックの承認数が増えた状態で取引を完結させることである。



- ブロックの承認数が多いということは、最新のブロックから深いところにあり、分岐したブロックチェーンをメインのチェーンよりも長くするためには、作成しなければならないブロックが多く、これは確率的に難しい。
- これに対して、浅い場所で分岐が発生した場合には追いつくことに必要なブロックは少なくて良いため、比較的簡単にチェーンの切り替えが発生する。



- メインのブロックチェーンを切り替える攻撃方法は、51%攻撃と呼ばれる。
- メインのチェーンよりも早くブロックチェーンを伸ばすためには、マイナー全体が保有する計算資源の過半数を持っていれば良いため、このような名前が付いている。
- 51%のシェアがあると、確実に攻撃は成功するが、シェアが51%以下でも攻撃が成功する確率がある。



51%攻撃でできること

- 自分が保有していた通貨を再度使うこと(二重支払い)
- マイニングを独占すること

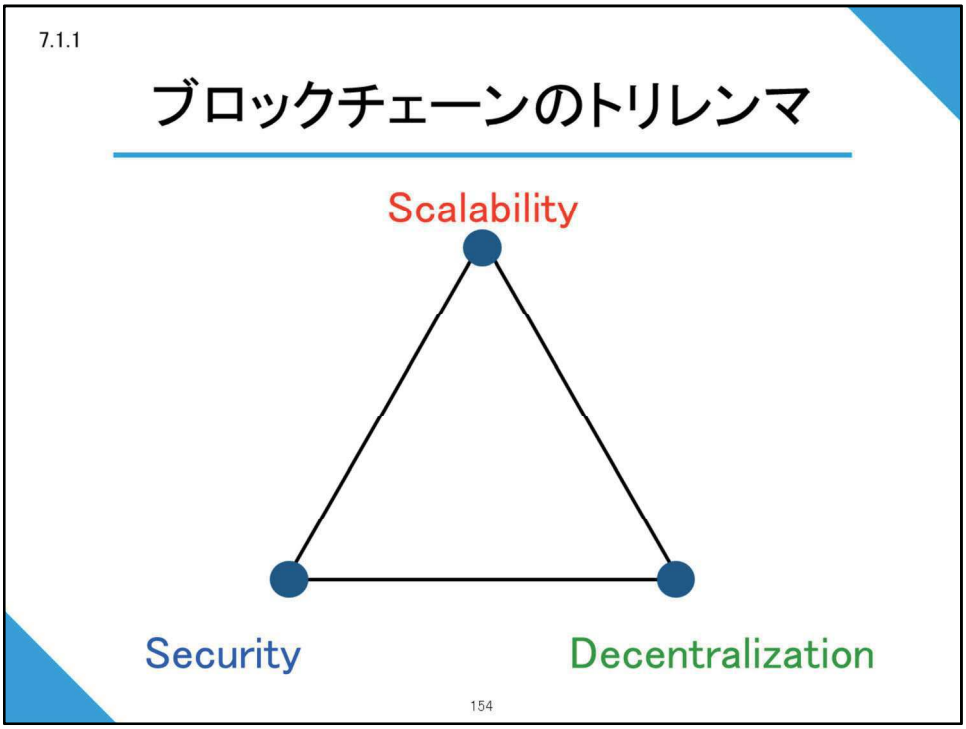
51%攻撃できないこと

- 他人の通貨を盗むこと(鍵を盗むしかない)
- 通貨を無尽蔵に発行すること(発行量はあらかじめ決まっている)

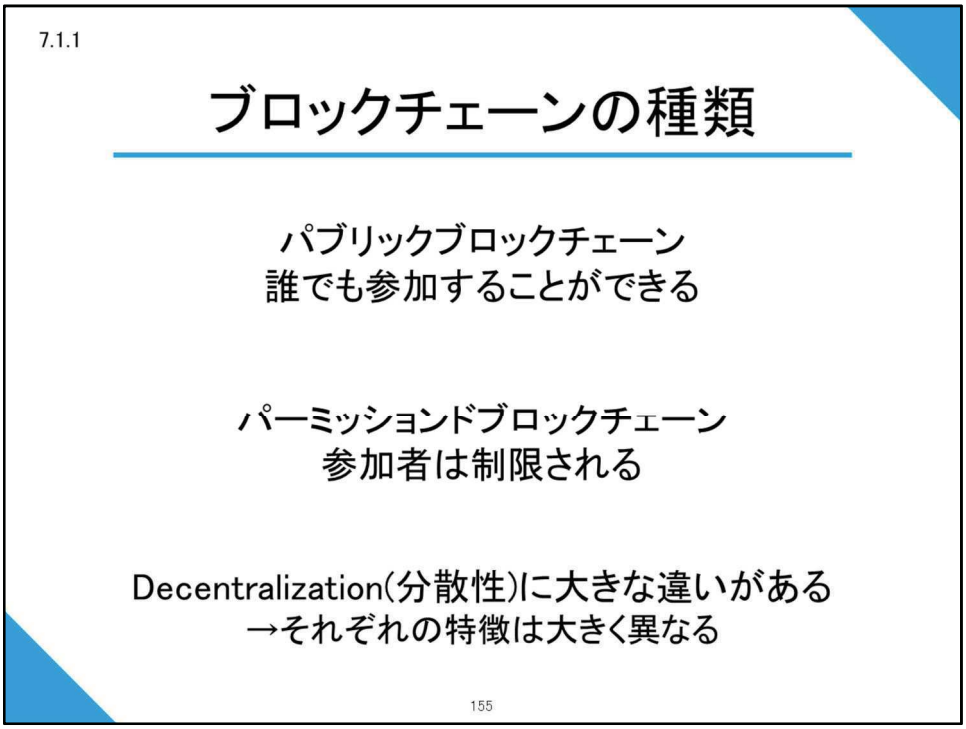
- 51%攻撃でできることは限られている。
- 51%を行うためには大量のコストがかかる。次のサイトにBitcoinに対して51%攻撃をにかかるコストがまとめられている。(https://gobitcoin.io/tools/cost-51-attack/)
- BitcoinやEthereumでは計算資源を投じて51%攻撃を行うよりも、マイニングを行っ益が大きい。
- マイニングの難易度と通貨価値のバランスによっては51%が容易に行われてしまうもある。

7. ブロックチェーンの課題

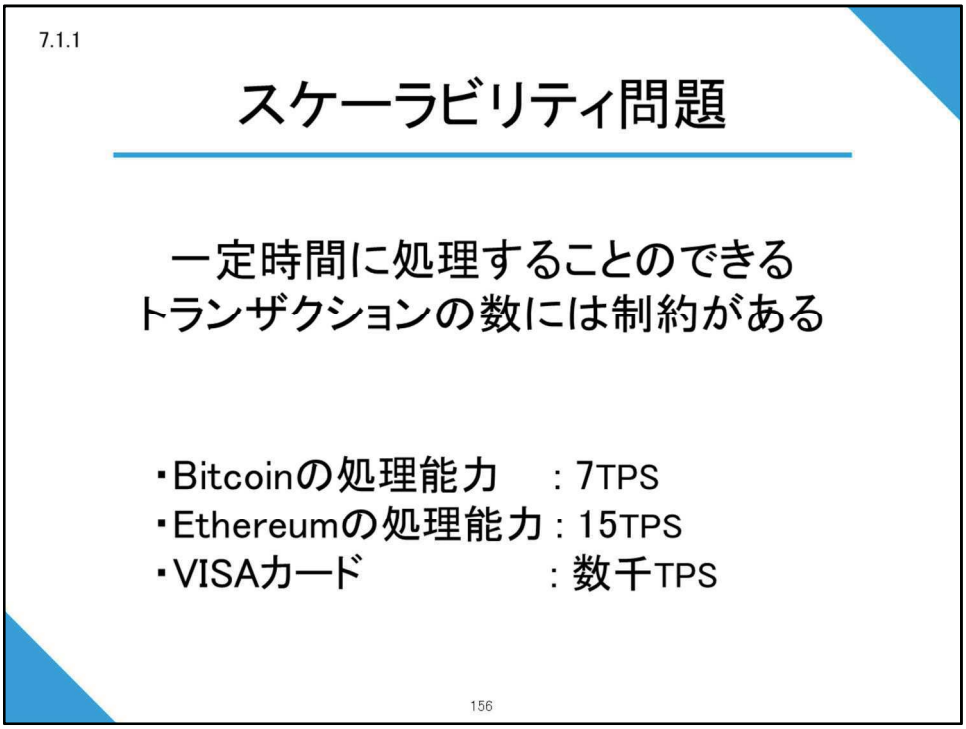
153



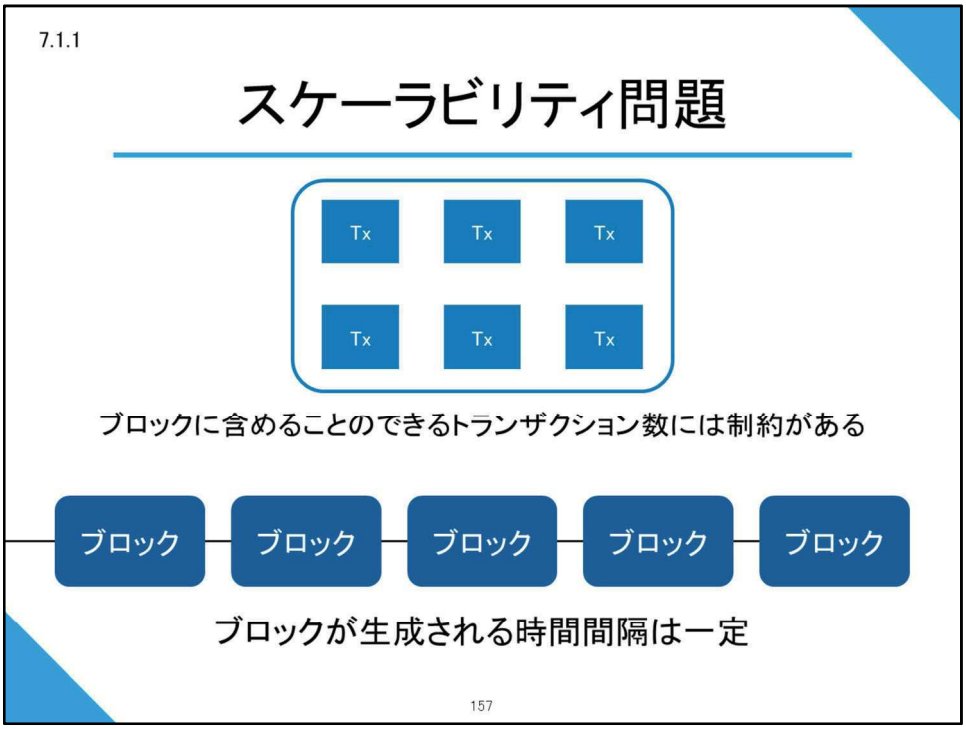
- ブロックチェーンでは、「Scalability(処理能力)」「Security(安全性)」「Decentralization(分散性)」の3つを同時に満たすことはできない。これをブロックチェーンのトリレンマと言う。



- ブロックチェーンの課題についての説明を始める前に、ブロックチェーンの種類についての復習を行う。
- ブロックチェーンはだれでも参加することのできるパブリック型と、参加には許可が必要なパーミッションド型のブロックチェーンがある。
- この2つのブロックチェーンには「分散性」に大きな違いがあり、これによりその他の特徴も大きく異なってくる。



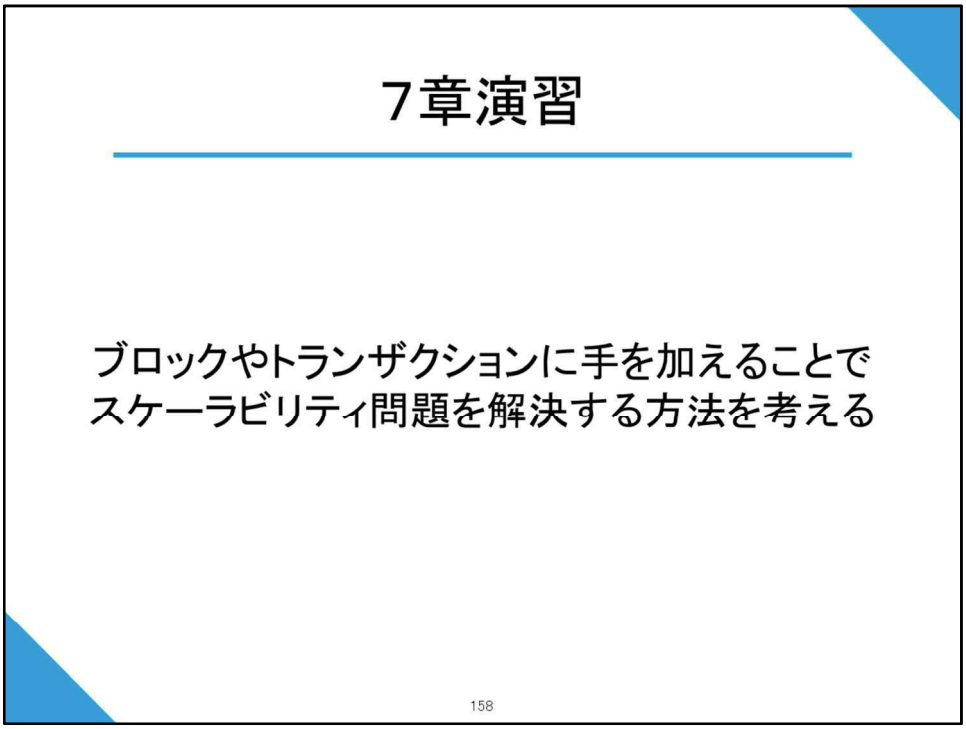
- スケーラビリティ問題とは、ブロックチェーンの仕様を作った時点から、一定時間に処理することのできるトランザクション数に制約が生まれており、その数が少なく実用化に難があるといった問題である。



トランザクションの処理能力があらかじめ決まっているという点について説明する。理由は2つある。

- 1つ目にブロックに含めることのできるトランザクション数には制約がある点。各ブロックには最大のデータサイズが定められており、当然トランザクションにもサイズがあることから、このような制約が生まれる。
- 2つ目にブロックが生成される時間間隔があらかじめ定められている点。これにより、一定時間に作られるブロックの数が固定される。

以上により、ブロックチェーンのスケーラビリティ問題が発生する。



準備

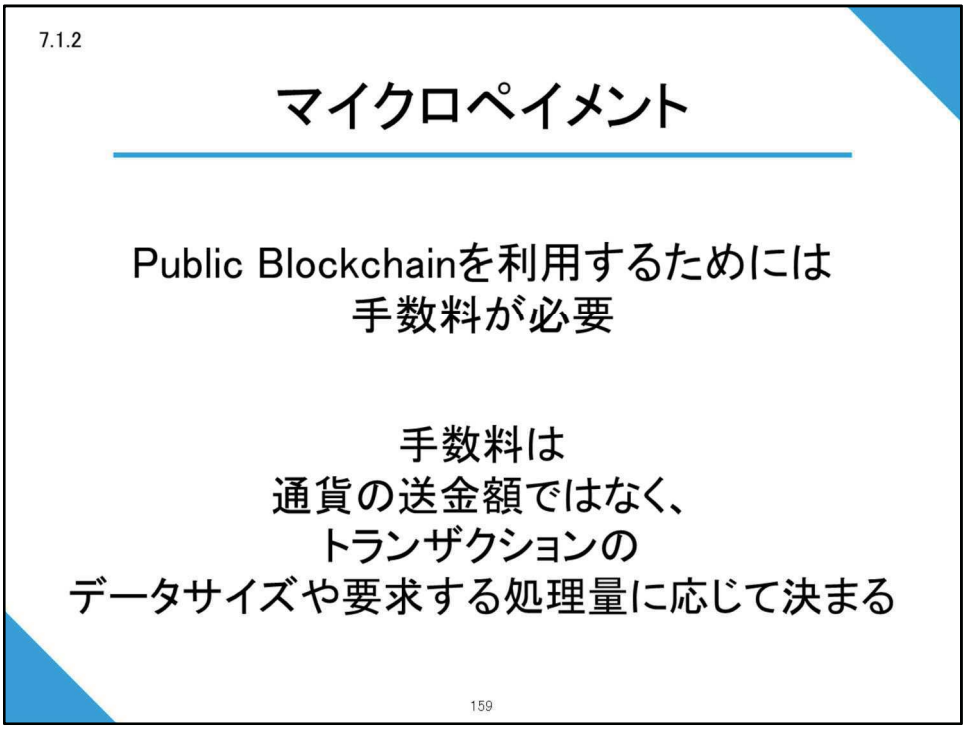
- 4～5人のグループを作成する

- 図7.1を参考にしながら、スケーラビリティ問題の解決法についてグループで10分話し合い、代表者が発表する。

正答例

- それぞれのブロックのデータサイズを大きくする
- ブロックの作成間隔を短くする
- トランザクションのデータサイズを小さくし、トランザクションが多くブロックに入るようにする

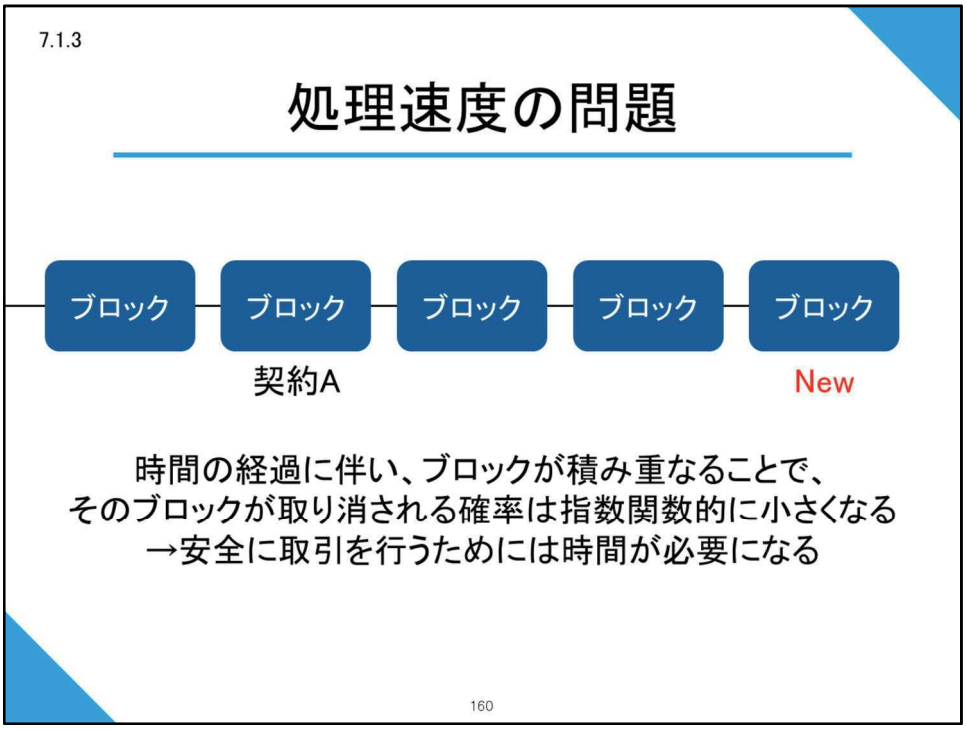
以上の3つの方法では簡単にスケーラビリティ問題を解決することができる。ただし、これらの方法はブロクチェーンの安全性を低下させてしまうことになるため、積極的に導入される方法ではない。



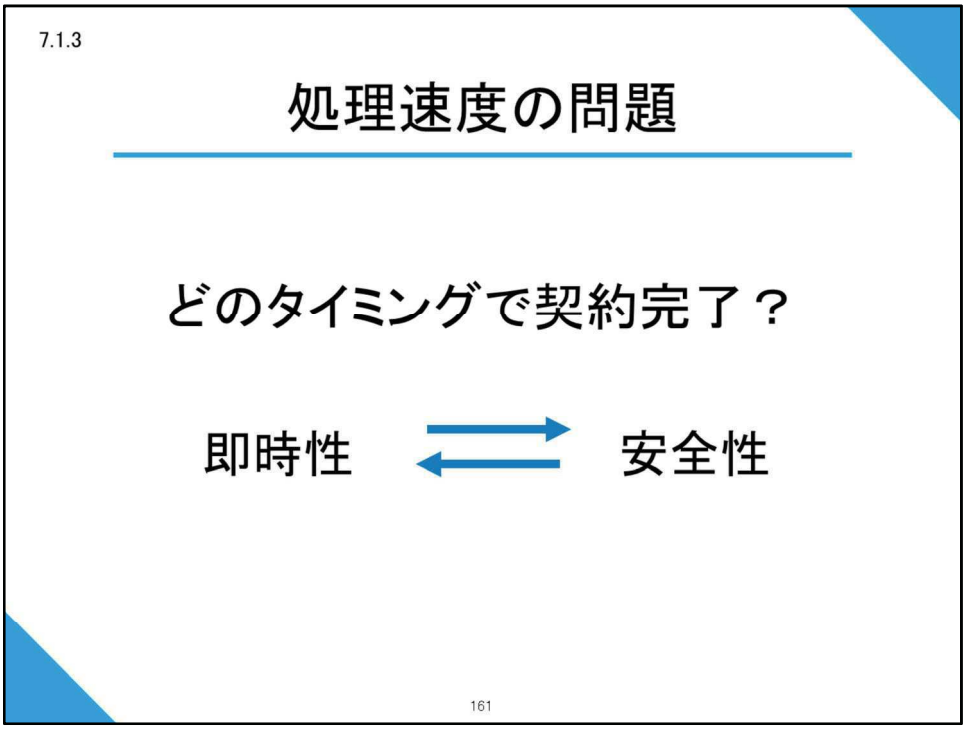
- パブリックブロックチェーンを利用する際には、手数料が必要になる。Bitcoinではトランザクション手数料と呼ばれる。
- この手数料は送金額に応じて決まるのではなく、トランザクションのデータサイズや要求する処理量に応じて決まる。つまり、高額の送金と少額の送金ではほとんで手数料が変わらないということである。これにより、少額の送金を行なった際には、送金額よりも手数料の方が大きくなるという問題が生じ、少額の送金が行われにくくなる。これがマイクロペイメント問題である。

- 人間同士の送金であれば、手数料はわずかなものかもしれないが、今後ブロックチェーンとの連携が期待されているIoT分野では、機械間での少額決済が頻繁に行われることが予測されており、手数料が大きな問題になると考えられている。
- 実際の手数料に関しては、以下のサイトで確認する。

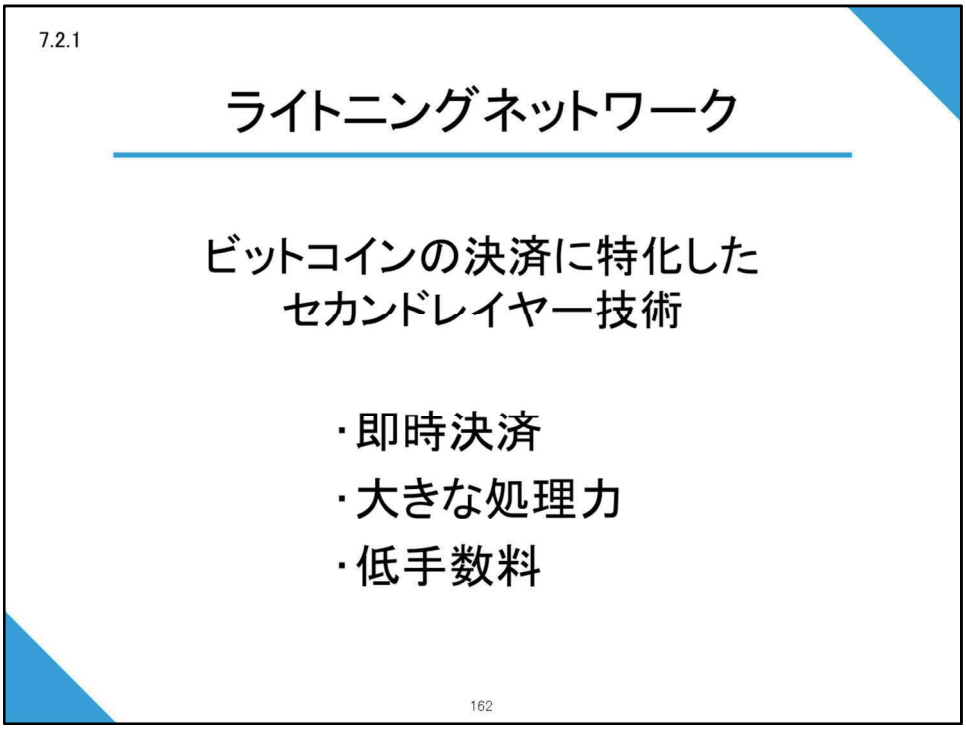
https://www.blockchain.com/ja/explorer



- ブロックチェーンでは決済の安全性は取引が行われてからの時間に強く依存する。
- 取引終了からの時間が経てば経つほど、その取引を行なったトランザクションが含まれるブロックに続くブロックが増えていく。
- ブロックが積まれれば積まれるほど、取引は安全なものになる。
- ブロックチェーンは「耐改ざん性が高い」特徴があるが、決済を行なった直後には決して安全であると言うことはできない。



- 安全な取引を行うためには、時間を必要とするため、ブロックチェーン上での取引は、即時性と安全性のトレードオフになる。
- 即時性を求めて、承認数0で取引確定としている場合もある。



- Bitcoinのセカンドレイヤー技術であり、決済に特化したレイヤーを作成し、高いスケーラビリティ、低手数料、即時決済を実現する。
- セカンドレイヤー技術とは、ブロックチェーンネットワークをファーストレイヤーとして、その上に新たな層を作成し、処理を行う技術である。
- ライトニングネットワークはセカンドレイヤーにはブロックチェーンを使わないオフチェーンと呼ばれる技術である。

- **即時決済**

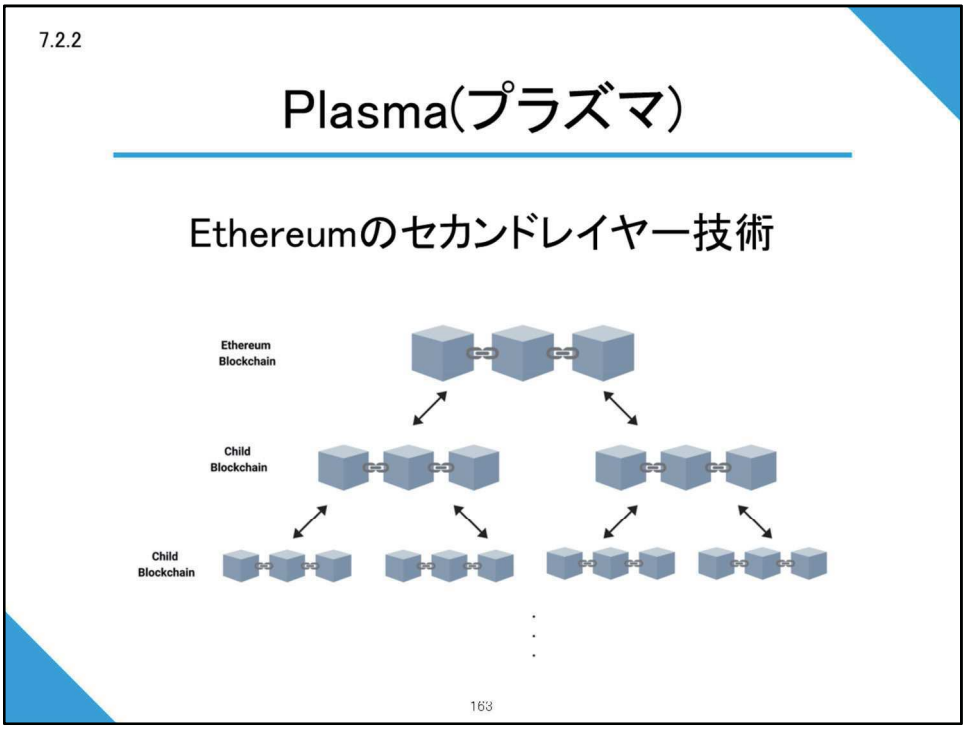
送金に使用されるネットワークが、Bitcoinのネットワークから独立している。これにより、安全な即時決済が可能になった。

- **大きな処理能力**

セカンドレイヤーではブロックチェーンを使用していないため、一定時間に処理することのできるトランザクション数はブロックのサイズや、ブロックの生成間隔などよる制限はされない。

- **低手数料**

ビットコインのネットワーク上で取引に比べて低い手数料で取引を行うことができる。



- Ethereumのセカンドレイヤー技術である。
- Ethereumのスケーラビリティ問題を解決する。
- セカンドレイヤー技術のうち、セカンドレイヤーにもブロックチェーンを使うサイドチェーンと呼ばれる技術である。

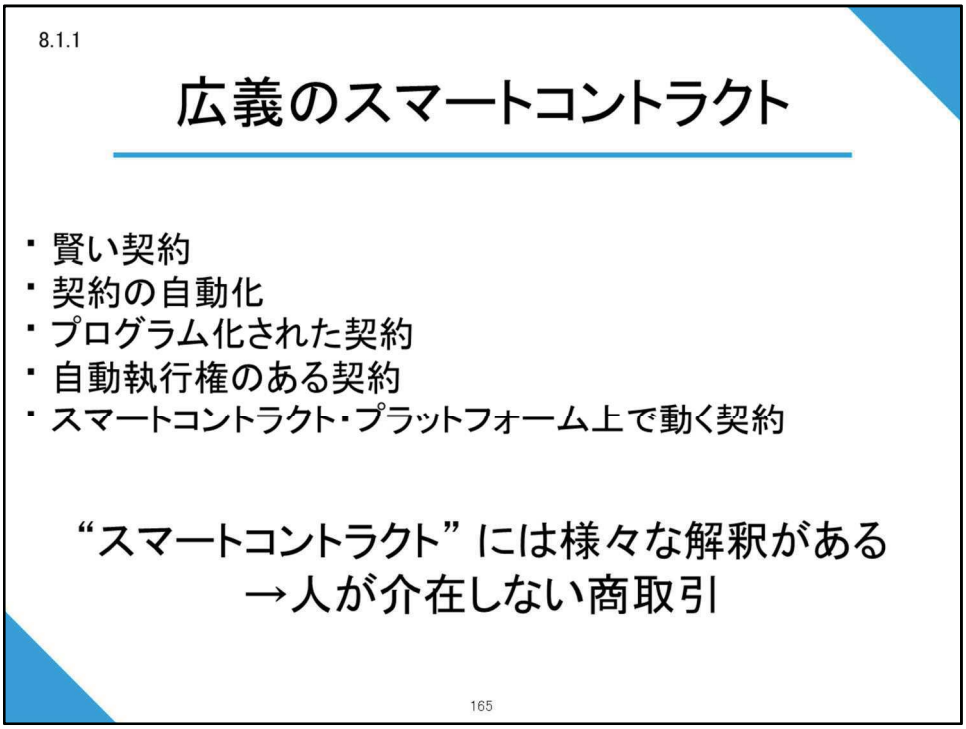
- **ブロックチェーンに記録されるトランザクション数の減少**

全てのトランザクションをEthereumのブロックチェーンに記録する必要がないため、Ethereumのブロックチェーンのネットワーク内で処理伝達されるトランザクション数を抑えることができる。

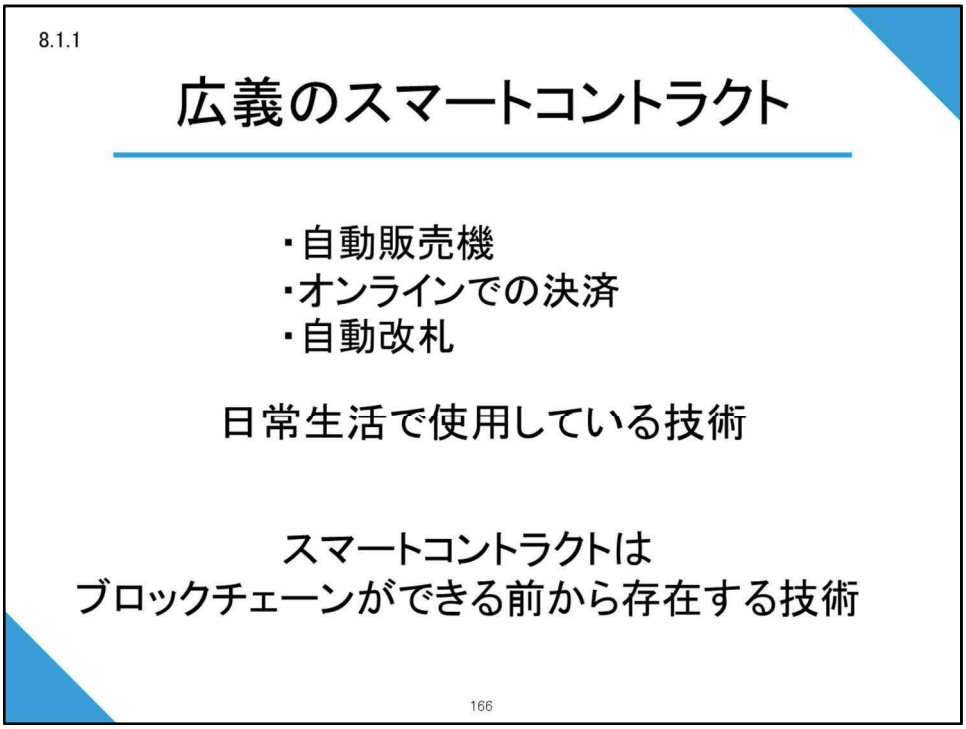
- **複雑なトランザクションもスムーズに実行することができる**

Ethereumのネットワーク内のコンピュータだけでなく、プラズマチェーンのネットワークに分割して処理を行うことで処理速度をあげることができる。

8. スマートコントラクトの概要



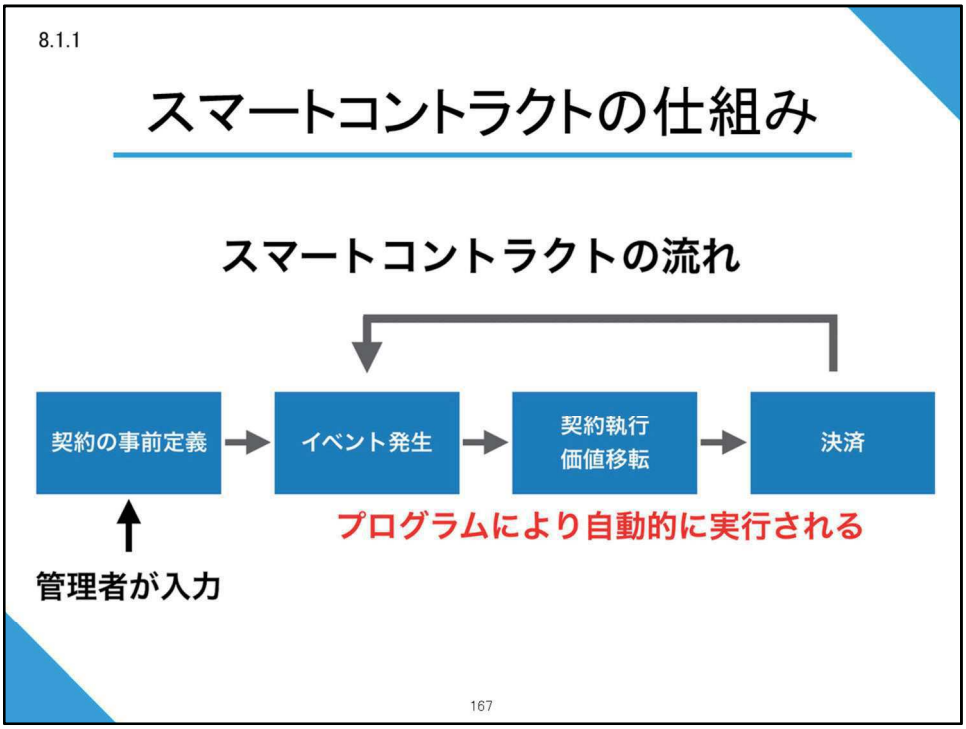
- スマートコントラクトには様々な解釈がある。
- ここでは人が介在しない商取引をスマートコントラクトとする。



スマートコントラクトの例

- 自動販売機
- オンラインでの決済
- 自動改札

- スマートコントラクトは日常で利用している技術であり、決して珍しい技術ではない。
- スマートコントラクトはブロックチェーンができる前から存在する技術である。



スマートコントラクトの処理の流れは4つのパートに分けることができる。
それぞれのパートを自動販売機を例にして説明する。

契約の事前定義

- 契約の内容を決定し、それをプログラムに記述する。
- 自動販売機を作成して、商品を入れて設置する。

イベント発生

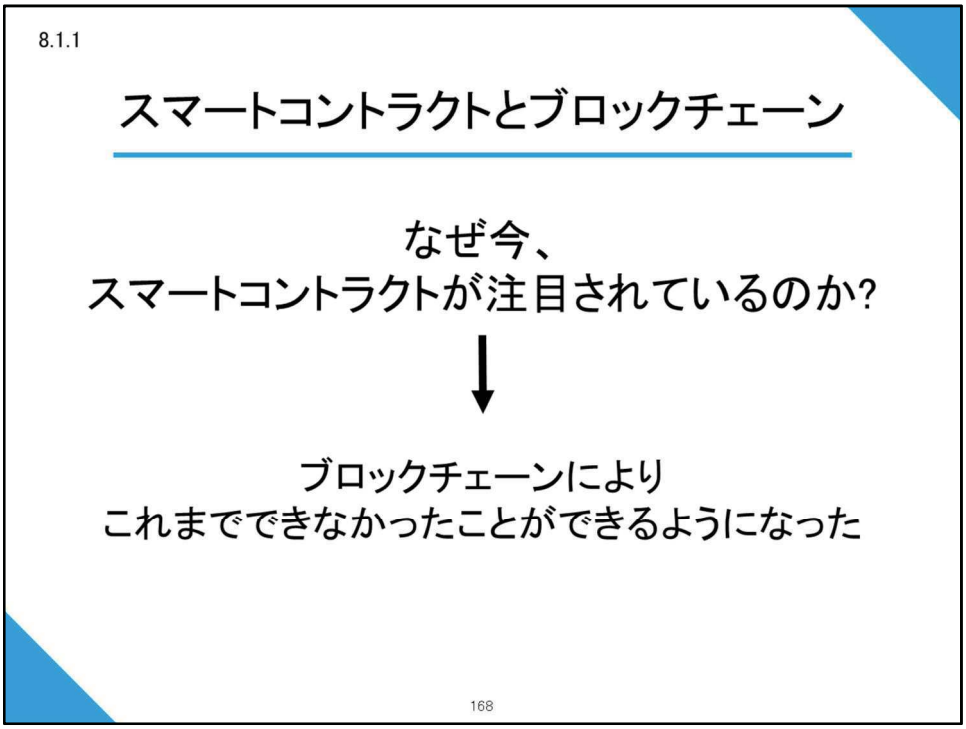
- 実行可能な状態になったスマートコントラクトは、発動のトリガーとなるイベントを待つ。
- お金が入れられ、ボタンが押される。

契約執行　価値移転

- あらかじめ定められたイベントが発動すると、定められたプログラムに従って契約を行うための処理が実行される。
- 押されたボタンと投じられた金額から自動販売機が商品を送り出す用意をする。

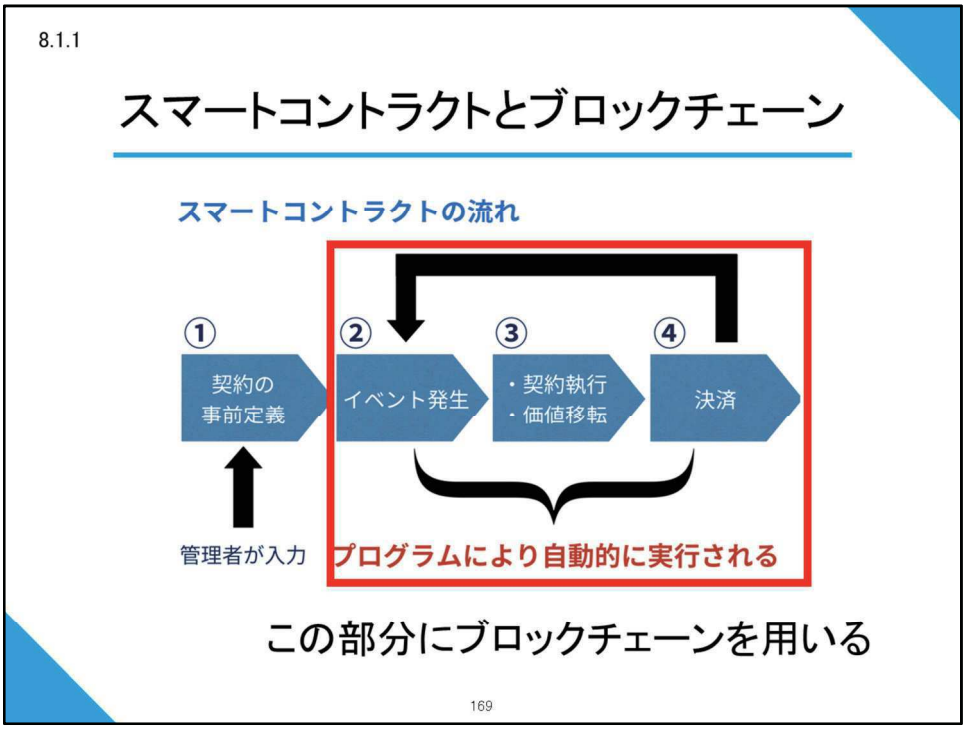
決済

- 契約内容に基づいて資産の移転が行われる。
- 商品が取り出し口に落ち、おつりがある場合は出てくる。

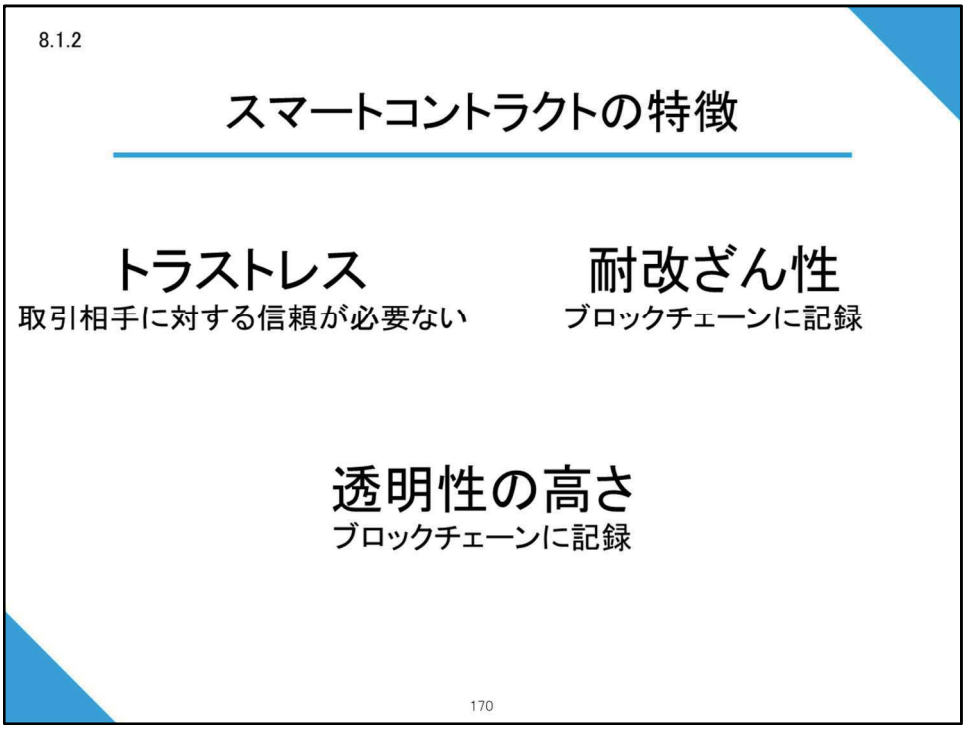


スマートコントラクトが注目されている理由

- ブロックチェーンを用いることで、管理者不在の取引を行うことができるようになったためである。



- これまでサービスの提供者が準備したサーバーで処理を行なっていた部分を、ブロックチェーン上で行う。



- ブロックチェーンを利用したスマートコントラクトの特徴はスライドの通りである。
- それぞれについて、後のスライドで説明を行う。

8.1.2

トラストレス

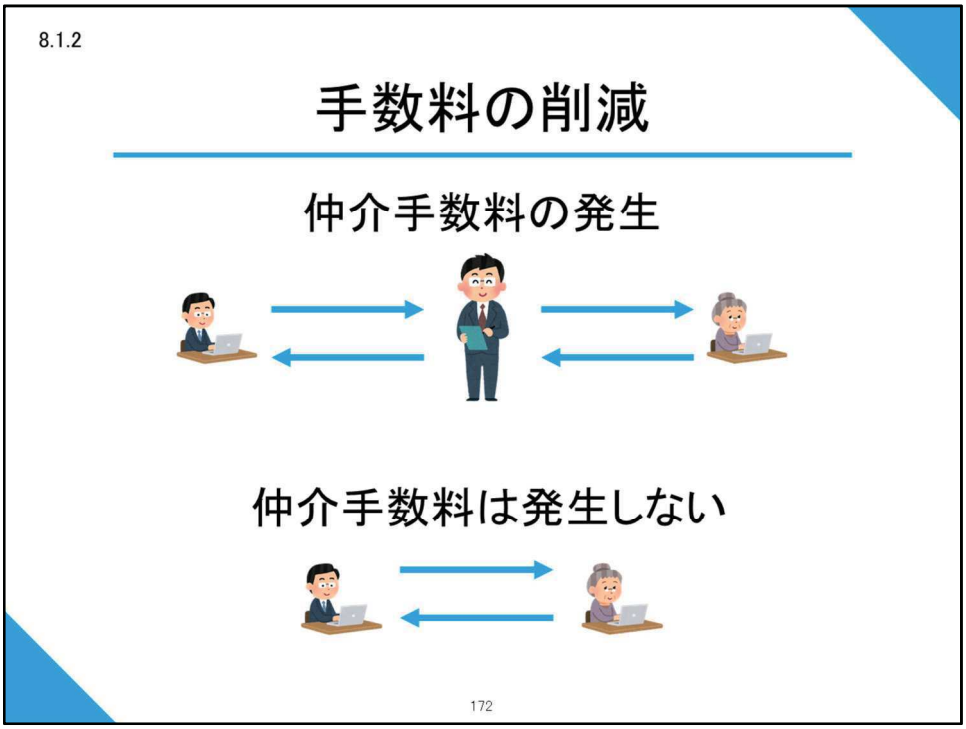
仲介者を介さずに安全な取引を行うことができる

従来のスマートコントラクト

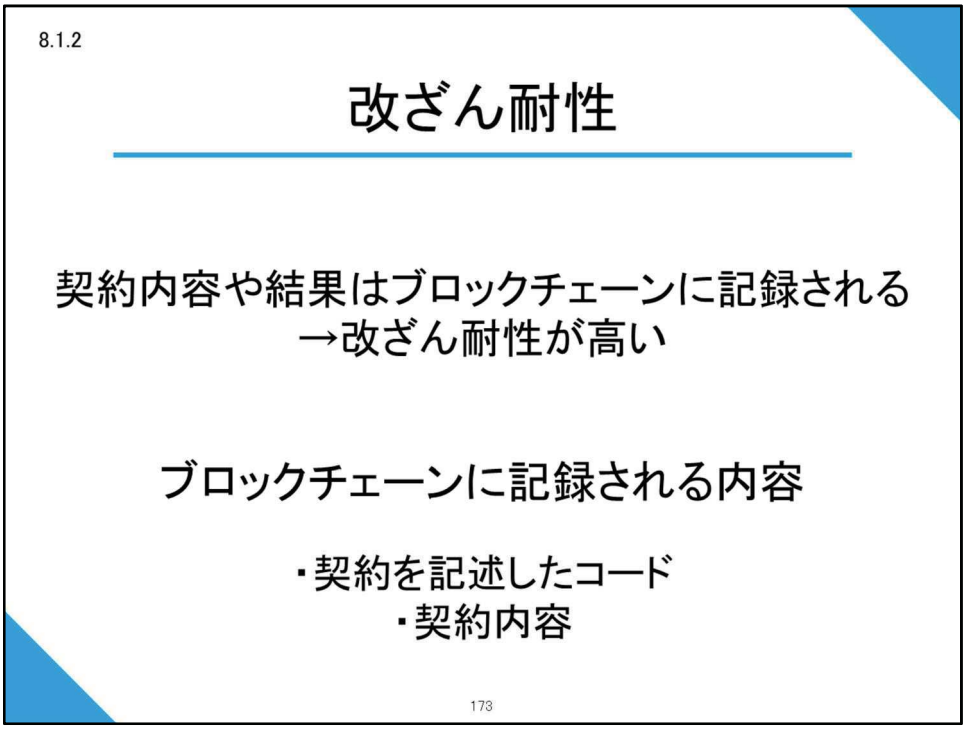
ブロックチェーンを用いたスマートコントラクト

171

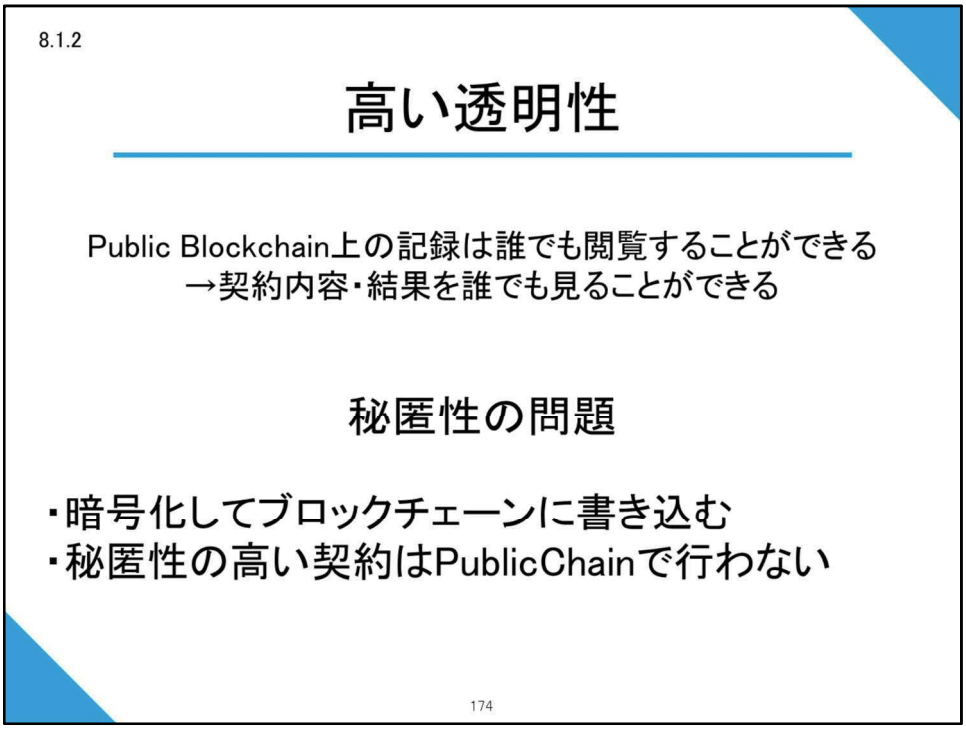
- 従来のスマートコントラクトは信頼点としての仲介者が必要だった。
- ブロックチェーンを用いることで、仲介者を必要とせずに安全に取引を行うことができる。



- 仲介者が必要なくなることで、取引にかかるコストを抑えることができる。
- パブリックブロックチェーンを利用する際には、トランザクション手数料が必要になる



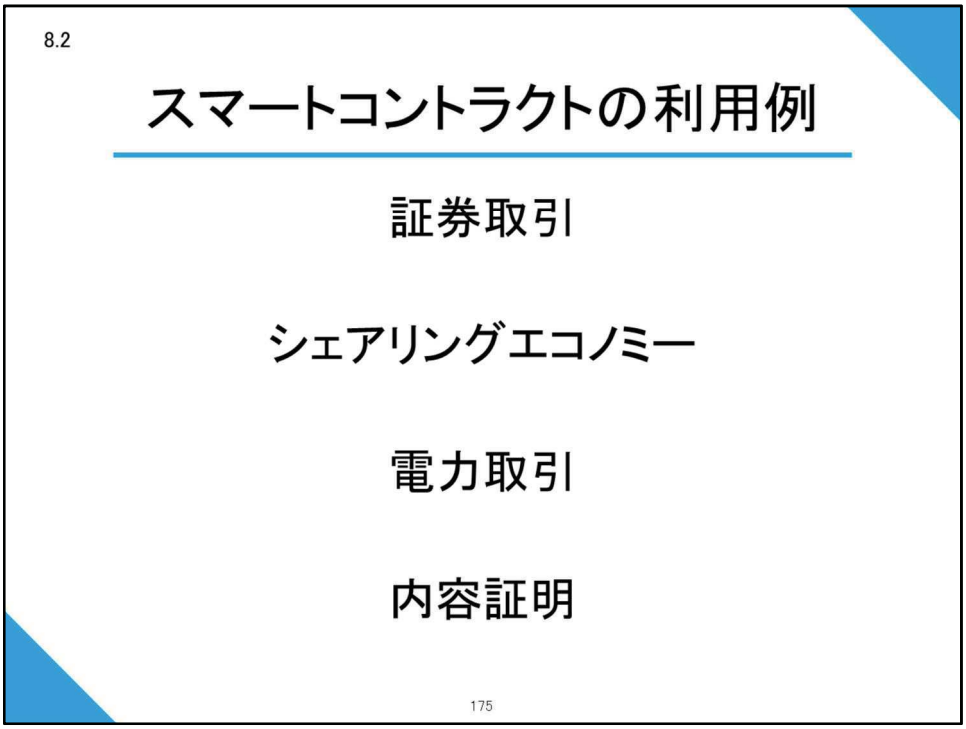
- スマートコントラクトの契約内容や、契約結果はブロックチェーンに記録される。
- これにより、ブロックチェーンの改ざん耐性を活かすことができる。



パブリックブロックチェーンに記録される取引は誰でも閲覧することができる。

秘匿性の問題

- 誰でも閲覧できるということは、秘匿性が問題になる。
- 暗号化してブロックチェーンに書き込むことで、だれでも結果を閲覧できる状態を防ぐ。
- 秘匿性の高い取引は、閲覧権限の制限されるパーミッションドブロックチェーンで行う。



証券取引

証券、株式、不動産などの取引には直接的に金銭が関与するため、法律により様々な契約方法が厳格に定められており、契約をプログラミングコードとして記述することが比較的容易であり、スマートコントラクトとの相性が良いとされる。

シェリングエコノミー

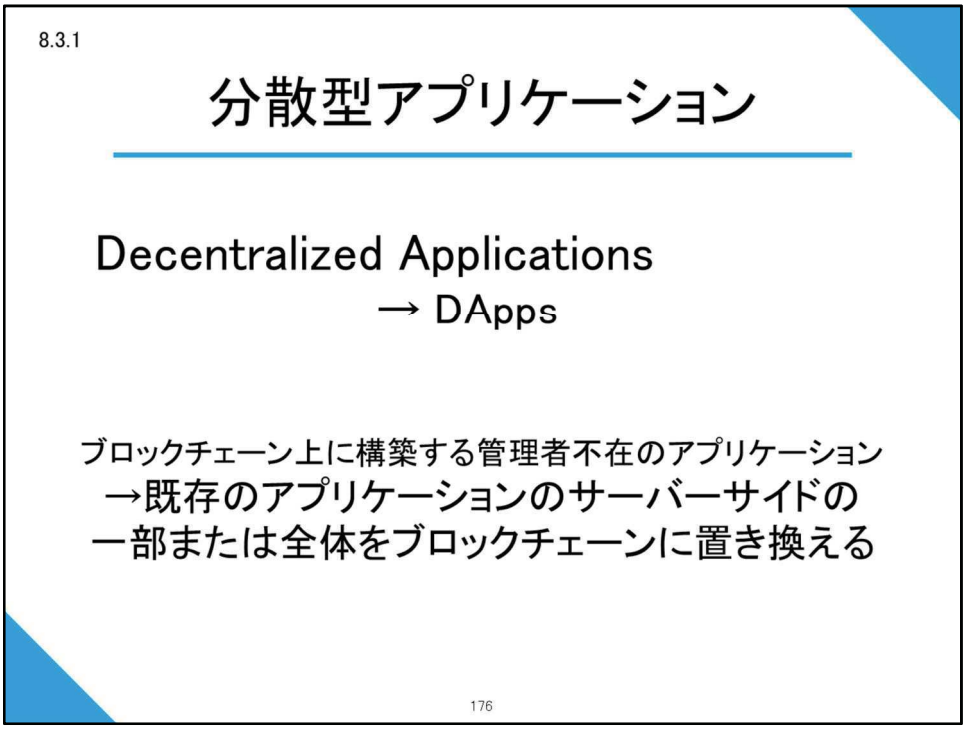
シェアリングエコノミーを仲介者を必要とせずに、個人間で実現するためには、取引を行う相手がどのような人物であり、信頼することができるのか知る必要がある。
このような情報をブロックチェーンを用いて管理することにより、契約を結ぶ前に取引相手が信頼のできる人物であるかを確かめることができる。

電力取引

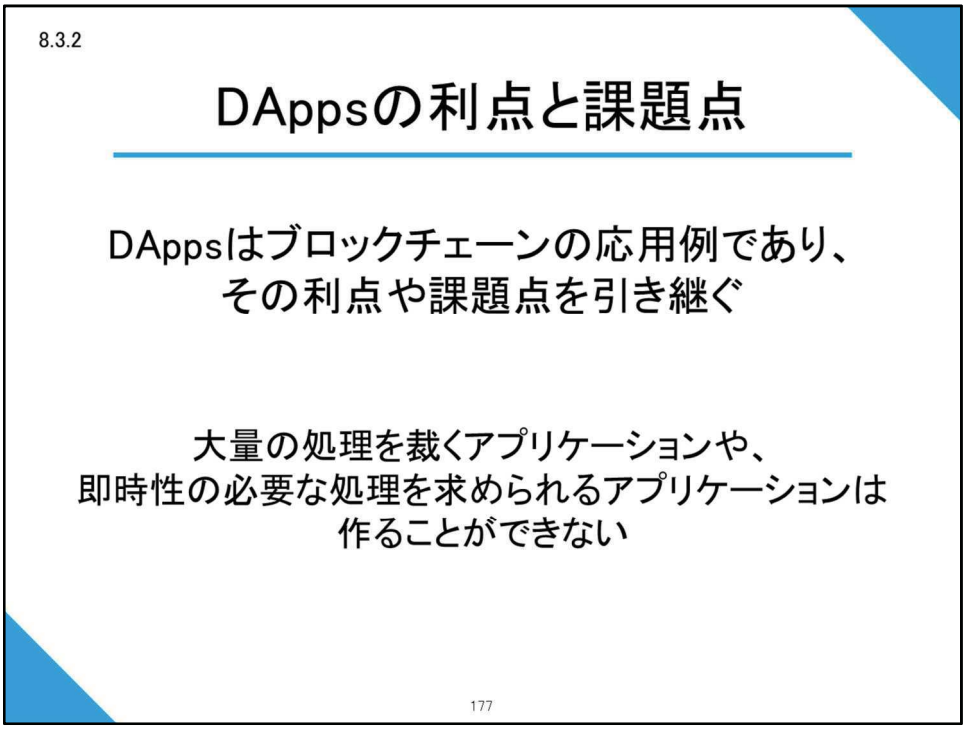
個人宅で作られた電力を電力会社を介することなく、個人間で取引を行う仕組みがスマートコントラクトにより実現されようとしている。スマートコントラクトを用いることで、これまでの中央集権的な電力システムから脱却し、自律的に電力を受給できるようになる。

内容証明

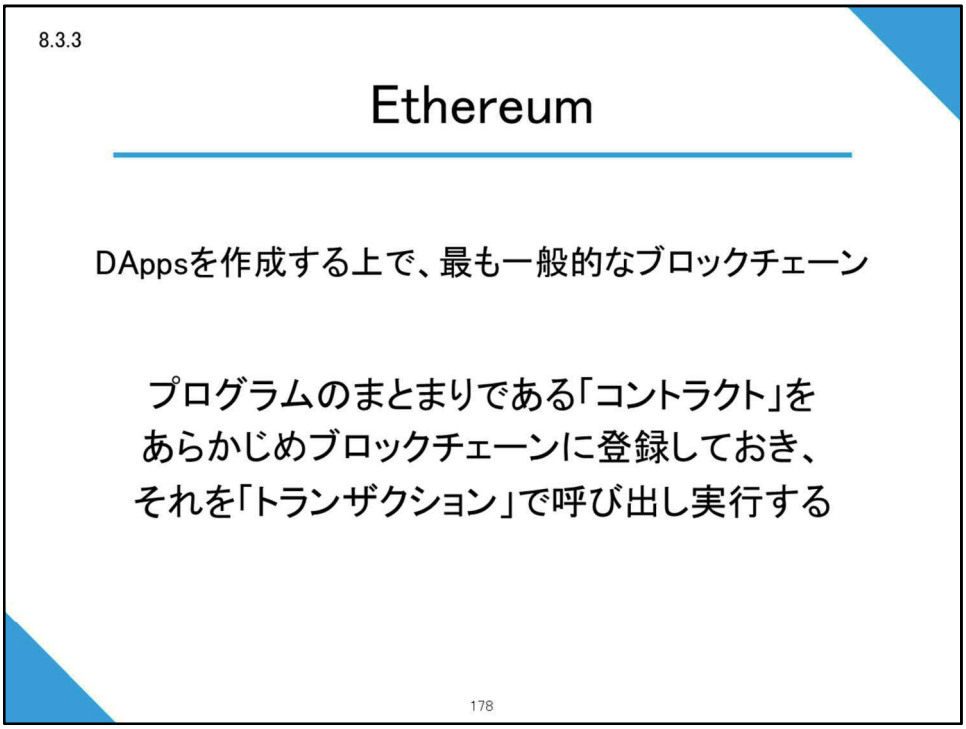
「Proof of Existence」と呼ばれる契約書や所有権の書類の存在証明。データのハッシュ値をブロックチェーンに記録することで、その時刻に、そのデータが存在していたことを永久に証明することができる。



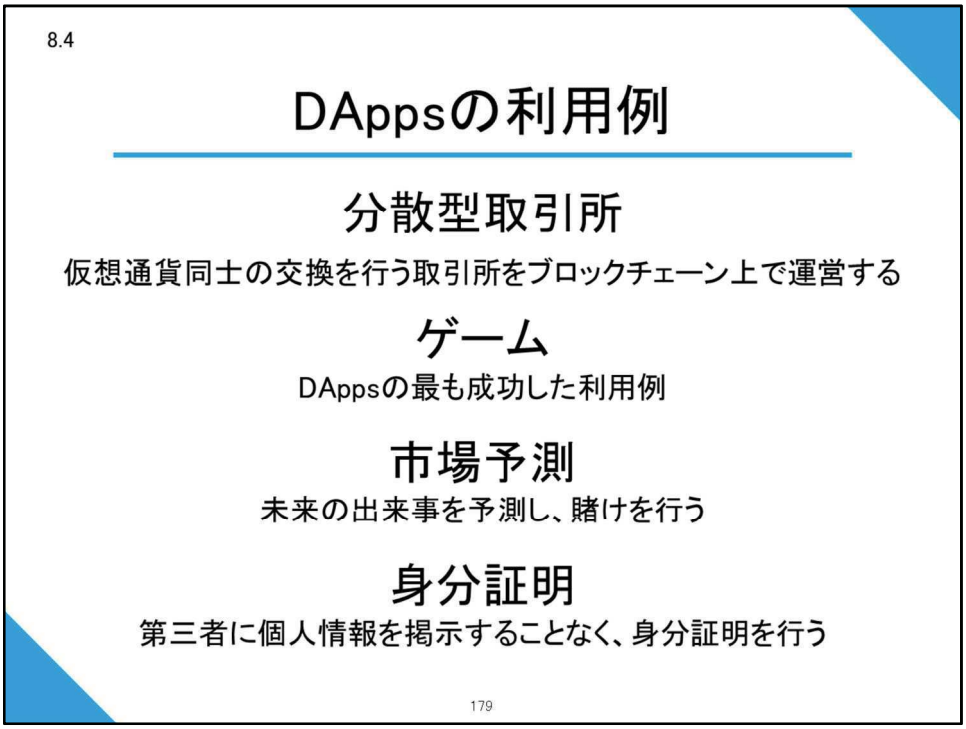
- ブロックチェーン上に構築する管理者不在のアプリケーションである。
- 既存のアプリケーションのサーバーサイドの一部または全体をブロックチェーンに置き換える。



- DAppsはブロックチェーンの応用例であり、その利点や課題点はそれぞれの性質を引き継ぐ。
- ブロックチェーンのスケーラビリティ問題により、大量の処理を裁くことはできない。
- 安全な取引には時間が必要であり、即時性の求められる処理には向いていない。
- ブロックチェーンの特徴を踏まえて、アプリケーションを作らなければならない。



- Ethereumは現在DAppsを作成する上で、最も一般的なブロックチェーンである。
- 他のプラットフォームに比べて、情報も多いので取り組みやすい。
- 「コントラクト」と呼ばれるプログラムのまとまりをブロックチェーンに登録し、それをトランザクションで呼び出すことで実行する。
- Ethereum以外にも、NEOやEOSといったブロックチェーンがDAppsのプラットフォームとして機能する。



分散型取引所

- 分散型取引所はブロックチェーン上で構築される非中央集権的な取引所
- 一般的な仮想通貨取引所では、ユーザーは通貨を使用するための秘密鍵を取引所に預ける必要があり、サイバー攻撃などにより取引所から秘密鍵が盗まれ、それにより通貨が流出する危険性が高い。分散型取引所では秘密鍵は取引所に預けるのではなく、自身で管理する。

ゲーム

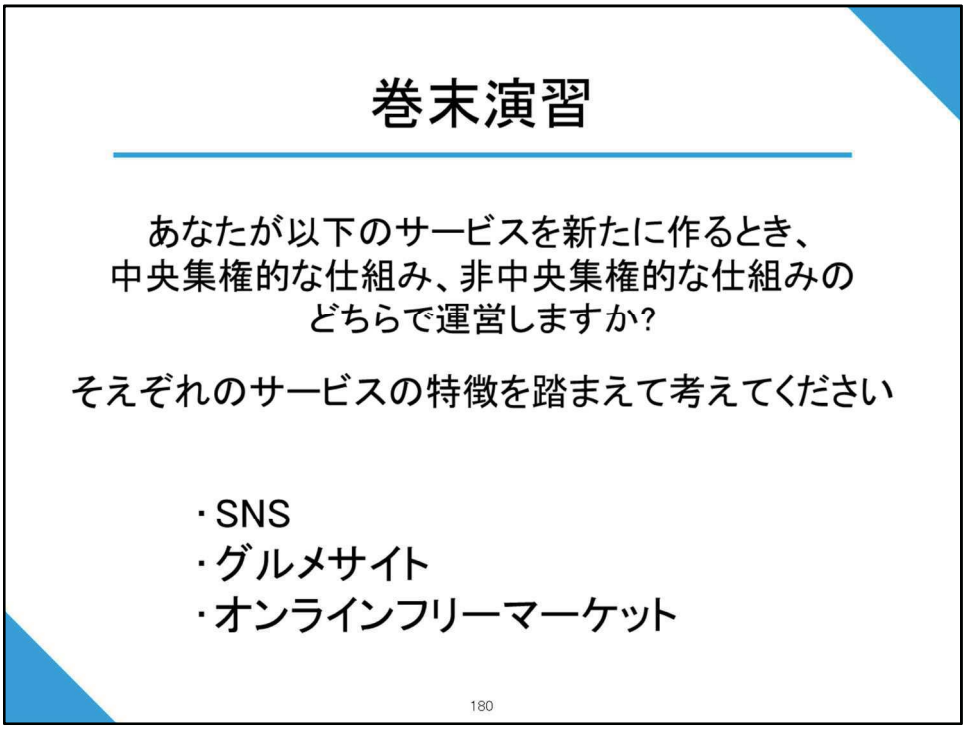
- 改ざんが難しく、透明性が高い性質を利用して、ゲームの結果が意図的に操作させていないことをユーザーが確認することができる。現在は、トークンを使ったギャンブルのようなゲームが主流である。

市場予測

- 株価や、サッカーの試合結果などの未来の出来事を管理者に依存せずに予測する市場
- 独立した大衆が未来予測を行い、多くの人が予測した結果は的中しやすいという統計がある。これにより精度の高い未来予測ができるのではないかと期待される。

身分証明

- ブロックチェーンの仕組みを用いて個人情報を管理することで、第三者に個人情報を開示することなく、身分の証明ができるようになる。
- ブロックチェーンに直接個人情報を書き込むのではなく、あくまでシステムの一部としてブロックチェーン利用する。



準備

- 4～5人のグループを作成する

- それぞれの項目について、15分程度時間をとってグループで考え、話し合った結果を代表者に発表してもらう。

発表の形式

- SNSは中央集権的に管理者が存在する仕組みとして運営した方がいい。理由は～～～なためです。
- グルメサイトの～～～点には非中央集権的の特性である、～～～を活かすことができる。
- オンラインサイトの～～～の部分は中央集権的に、～～～な部分は非中央集権的に運営したほうがいい。

令和元年度「専修学校による地域産業中核的人材養成事業」
スマートコントラクトを使用したシステム開発人材の育成

ブロックチェーン概論指導マニュアル

令和２年２月
学校法人　麻生塾　麻生情報ビジネス専門学校
〒812-0016　福岡県福岡市博多区博多駅南２丁目１２-３２