FUJITSU

「守る」技術

ブロックチェーンのセキュリティ強化技術

ご利用にあたっての注意
この講座は2017年当時の情報です。予告なしに更新、あるいは掲載を終了することがあります。あらかじめご了承ください。

最終更新日 2017年5月30日

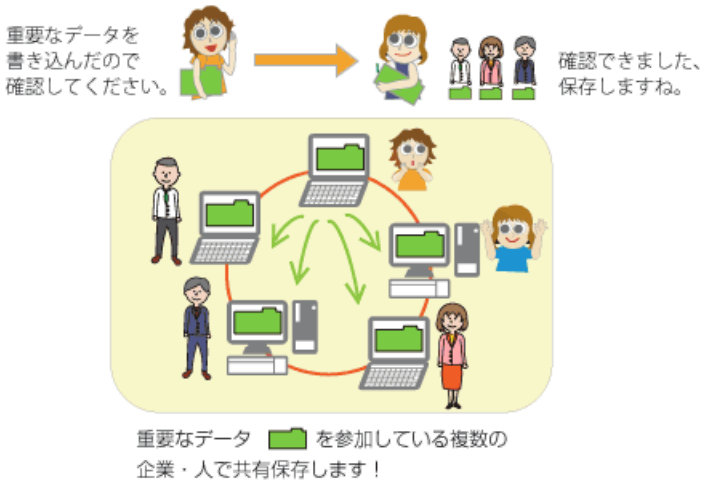
もくじ

「ブロックチェーン」って？

「ブロックチェーン」ってなんですか？

Copyright 1994 - 2025 Fujitsu

インターネットや企業間ネットワークなどの上で、重要なデータやコイン（仮想通貨）のやりとりを安心・安全に扱うことができる技術です。データを複数の企業・人で共有するので、**「分散型台帳技術」**とも呼ばれています。

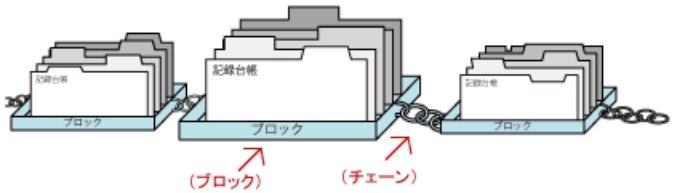


これだけでは、なぜブロックチェーンが注目されているのか、わかりづらいのですが・・・

それでは、なぜ「ブロックチェーン」というのか、そして何が良いのか、順番に説明しますね！

お願いします！それではまず、なぜ「ブロックチェーン」というのか教えてください。

はい、**「ブロック」**は、企業同士の取引情報、ビットコインの受け渡しなどの記録をまとめたもので、**「チェーン」**は、くさり状に各ブロックをつなげて保存していくことです。



「チェーン」と呼ぶのは、取引記録を単に保存しているのではなく、**ブロックごとに得られる値、つまり「ハッシュ値」を次のブロックに伝えていく**ことで、ブロック同士がつながっていることを表しています。

Copyright 1994 - 2025 Fujitsu

「ハッシュ値」ってなんだろう？

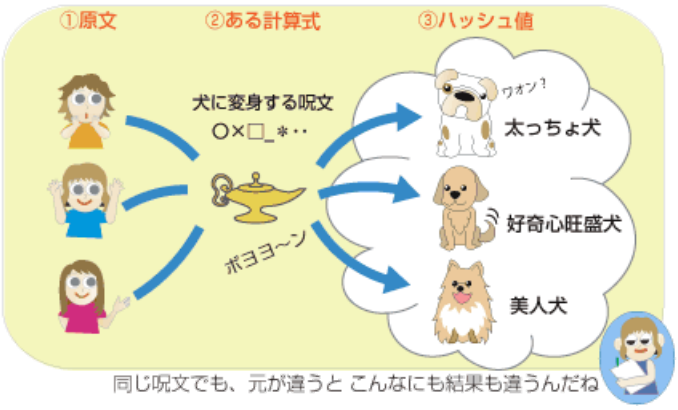
ブロックごとに得られる値の「ハッシュ値」ってなんですか？

ブロックの中の取引記録から、ある計算式によって作られるのが「ハッシュ値」です。その「ハッシュ値」を次のブロックにも伝えていくので、**常に前のブロックのハッシュ値が次のブロックのハッシュ値に影響**をあたえることになります。

「ハッシュ値」は、何のために必要なのですか？

はい、**取引記録の内容を勝手に変更されないようにする**ためです。勝手に変更すると、ハッシュ値が変わるのですぐにわかります。

つまり、元の情報を変えると、結果も変わってしまうってことなんだよね・・・



Copyright 1994 - 2025 Fujitsu

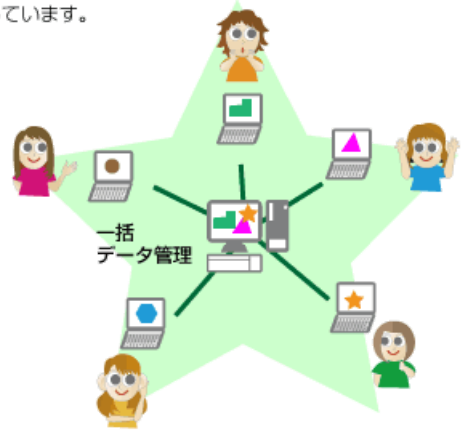
「ブロックチェーン」の良いところ

ハッシュ値が入っているから、勝手にデータを変更されにくい（変更するとすぐにわかってしまう）ということです。また、参加している人同士で取引記録を共有しているので、その記録の信頼性が高まる、ということです。

取引記録を参加している人同士で共有していることがなぜ信頼性が高まることになるのか、管理方法の違いを例にだして説明しましょう。

中央管理型

例えば、銀行でお客様のデータ（預金高など）は銀行のコンピュータが管理しています。



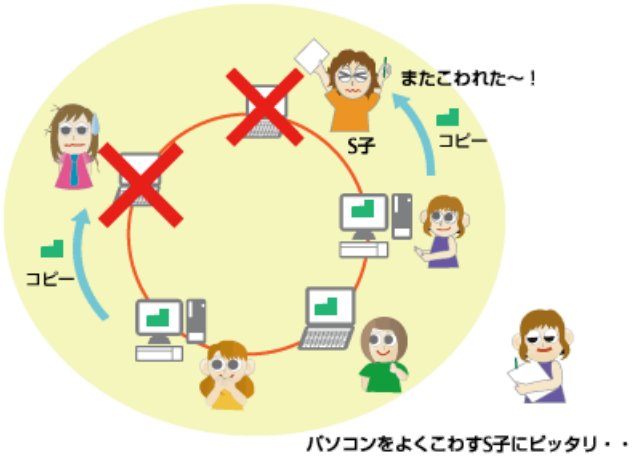
分散型（ブロックチェーン）

特定の会社がお客様のデータを管理するのではなく、ブロックチェーンに参加している人同士でデータを共有管理しています。

取引記録を参加している人同士で共有していると、なにが良いのですか？

Copyright 1994 - 2025 Fujitsu

共有していると、誰か1人が違う記録の場合、その人の記録は間違いということになります。みんなが同じ記録だと、その**記録の信頼性が高まります**。また、コンピュータが壊れて記録がなくなっても**コピーしてもらえる**、という利点もありますね！



ブロックチェーンで保存している取引記録の内容は、具体的に何ですか？

それは、関係者同士の大切な契約書だったり、文言だったりします。また代表的な例の一つとして、**ビットコイン**の取引記録もあります。

「ビットコイン」って？

「ビットコイン」って聞いたことがありますが、それはなんですか？

ビットコインは**仮想の通貨の一つ**です。実際の紙幣や硬貨は存在しませんが、パソコンやスマートフォンなどをお財布代わりにして、買い物などができます。

Copyright 1994 - 2025 Fujitsu

紙幣の偽札を防ぐのと同じように、ビットコインをある口座から別の口座にどれくらい送付したか、などの記録をブロックチェーンを使って保存すると、勝手に変更されにくいので安心です。

ブロックチェーンの課題

実際に使われているブロックチェーンですが、課題があります。「①他人による"なりすまし"の防止」と「②関係者だけの秘密保持を実現すること」です。

①ビットコインを使った他人による"なりすまし"の例

ビットコインを**勝手に他の人が使ってしまう**ことはないのですか？

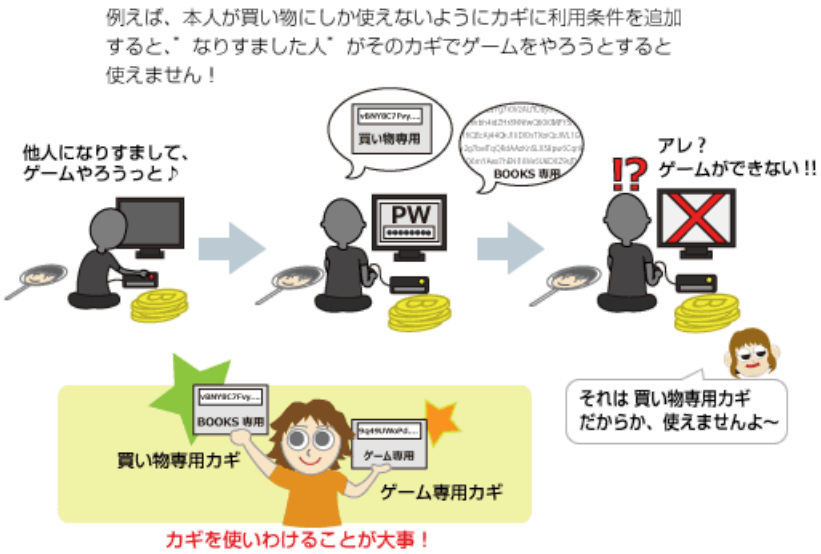
残念ながら**あります**。ビットコインには、通常、本人しか使えないパスワードのようなカギがあります。そのカギを盗まれてしまうと他の人に自分のビットコインを使われてしまうことがあります。

Copyright 1994 - 2025 Fujitsu

他人による"なりすまし"の被害を少なくするためには・・

カギを盗まれたらどうしよう・・・不安ですね。

カギを盗まれないようにするのが基本ですが、万が一、盗まれてしまった場合を考えて、カギを利用するときに条件を付けることができます。
被害を最小限に防ぐことができます。



②関係者だけの秘密保持を実現する例

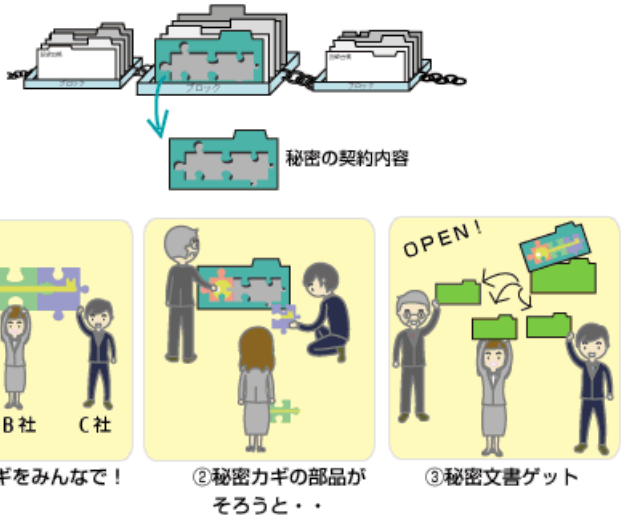
ブロックチェーンの取引記録は、同じネットワークに参加しているすべての会社に公開されているから、秘密を守ることはむずかしそうですね。

Copyright 1994 - 2025 Fujitsu

はい、実際には会社の契約内容までは知られたくない、という場合もありますよね。その場合は、関係者だけが持つ**秘密カギの部品**を使います。

秘密カギの部品ってどんなものですか？

秘密カギをバラバラにしたものです。この秘密カギ一つでは契約内容を見ることができません。複数の関係者が持つ**秘密カギの部品がそろってはじめて見ることができる**ため、秘密を守ることができます！



まとめ（富士通研究所が開発した技術）

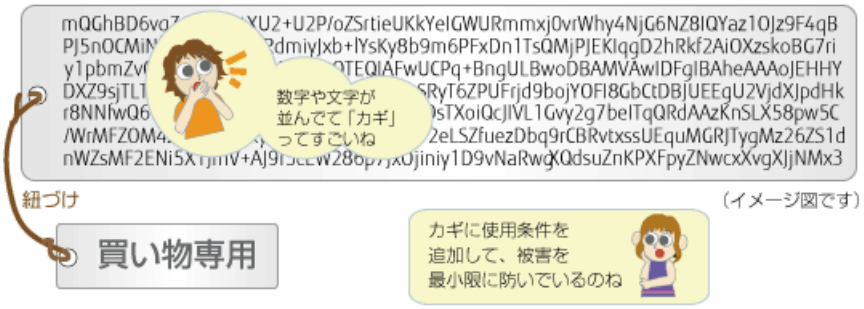
①他人による"なりすまし"の被害を最小限に防ぐ技術

ブロックチェーンを利用する際には、自分のカギ（パスワードのようなもの）を使います。そのカギを盗まれてしまうと、勝手に使われてしまいます。そこで被害を最小限に防ぐために、**カギに取引を制限する「条件」をつけます**。普段、本人はゲームをしないのに、なりすました人がゲームをしようとすると使えません。

条件付きのカギってどんなものですか？

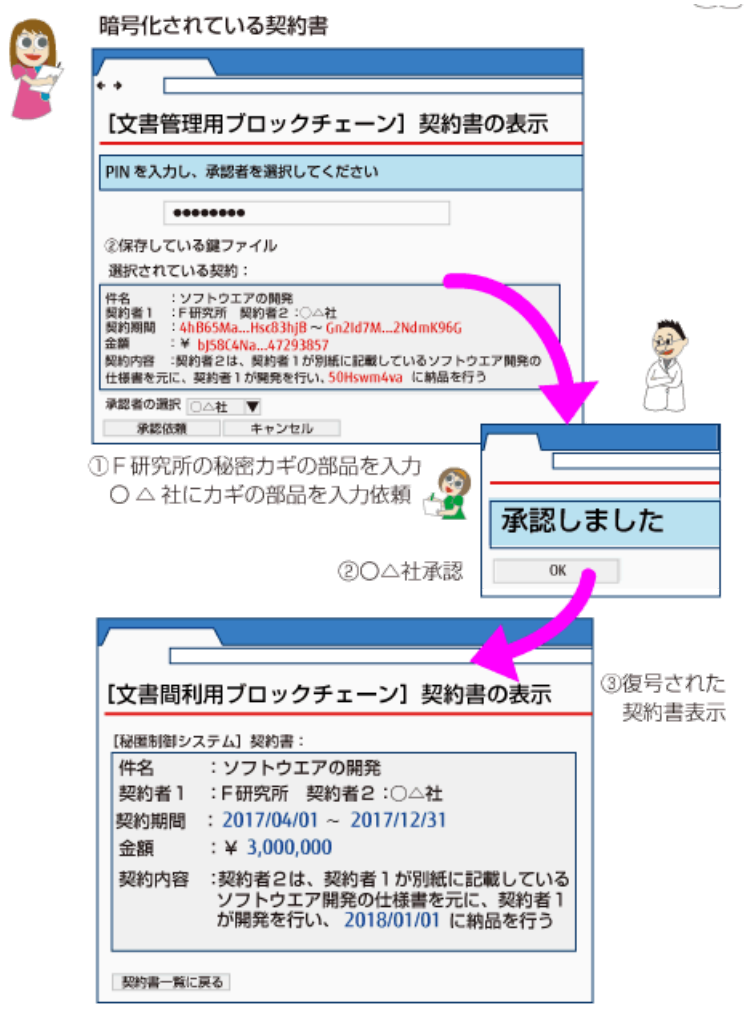
Copyright 1994 - 2025 Fujitsu

カギは数字や文字が並んだものです。このカギに取引を制限する「条件」を追加しています。



②関係者だけの秘密保持を実現する技術

通常使われているカギの部品を複数の利用者で管理し、一定数の部品がそろうと秘密情報を見られるカギを生成する仕組みを開発しました。



Copyright 1994 - 2025 Fujitsu

今後

金融分野をはじめ様々な分野でブロックチェーンの業務適用を想定した検証を進め、本技術の実用化を目指します。

関連リンク

プレスリリース

- ブロックチェーンのセキュリティ強化技術を開発（2016年10月19日）

Copyright 1994 - 2025 Fujitsu