

「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？
- ↓ 「ハッシュ値」ってなんだろう？
- ↓ 「ブロックチェーン」の良いところ
- ↓ 「ビットコイン」って？
- ↓ ブロックチェーンの課題
- ↓ まとめ（富士通研究所が開発した技術）
- ↓ 今後
- ↓ 関連ページへのリンク

## 「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？

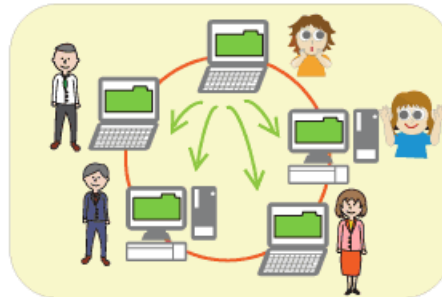
インターネットや企業間ネットワークなどの上で、重要なデータやコイン（仮想通貨）のやりとりを安心・安全に扱うことができる技術です。データを複数の企業・人で共有するので、「分散型台帳技術」とも呼ばれています。



重要なデータを書き込んだので確認してください。



確認できました、保存しますね。



重要なデータ  を参加している複数の企業・人で共有保存します！

II



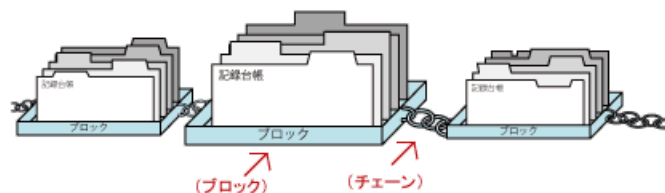
これだけでは、なぜブロックチェーンが注目されているのか、わかりづらいのですが・・・

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。

# 「ハッシュ値」ってなんだろう？



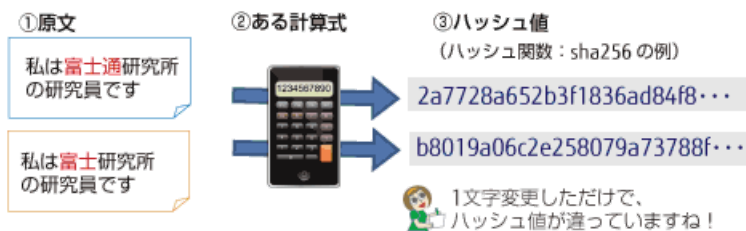
ブロックごとに得られる値の「ハッシュ値」ってなんですか？

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。

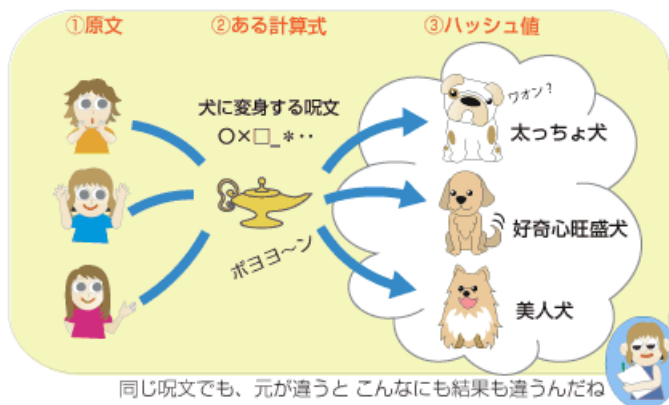


「ハッシュ値」は、何のために必要なのですか？

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・・・



# 「ブロックチェーン」の良いところ

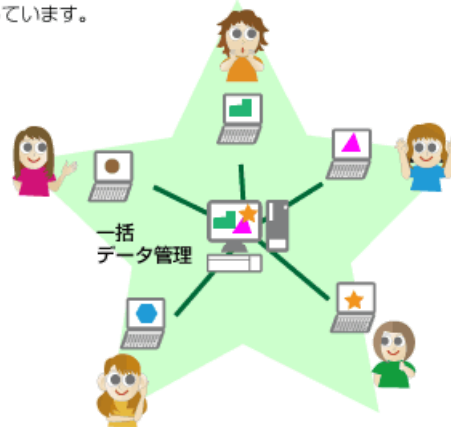
ハッシュ値が入っているから、勝手にデータを変更されにくい（変更するとすぐにわかってしまう）ということです。また、参加している人同士で取引記録を共有しているので、その記録の信頼性が高まる、ということです。

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。



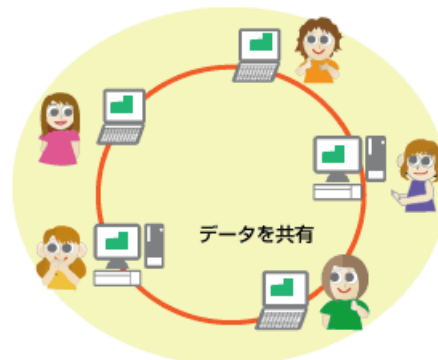
## 中央管理型

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？





実際の紙幣や  
硬貨は存在しません



ビットコインは  
仮想通貨の一つです

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。



S子の振込先教えて〜！



了解！この口座アドレスが入った  
QRコードにアクセスして振り込んで〜♪



拡大



## 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。





本人しか使えないカギを盗んで、勝手にビットコインを使ってしまおう！ウッシッシ

他人による“なりすまし”の被害を少なくするためには・・

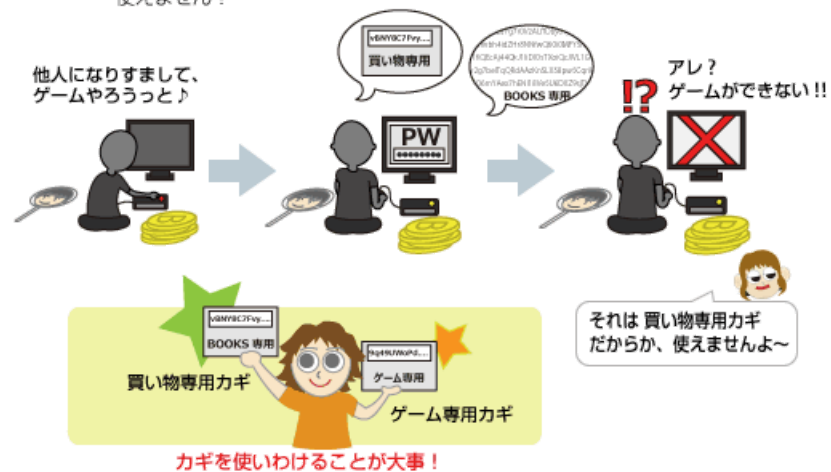


カギを盗まれたらどうしよう・・・不安ですね。

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。**



例えば、本人が買い物にしか使えないようにカギに利用条件を追加すると、“なりすました人”がそのカギでゲームをやろうとすると使えません！



## ②関係者だけの秘密保持を実現する例



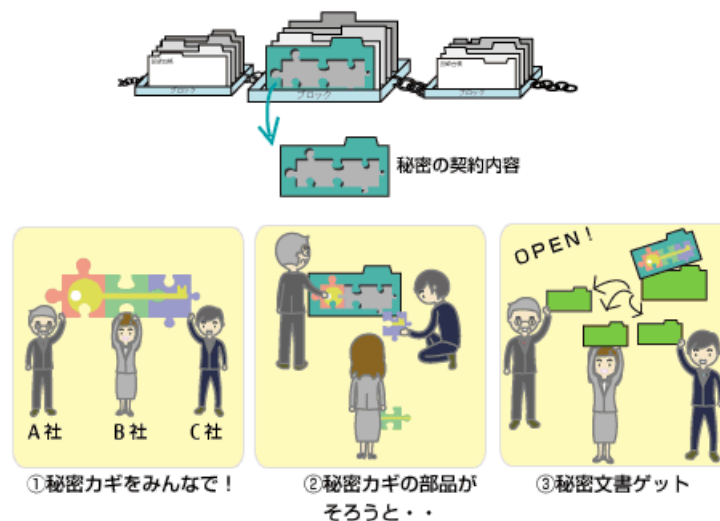
ブロックチェーンの取引記録は、同じネットワークに参加しているすべての会社に公開されているから、秘密を守ることはむずかしそうですね。

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初めて見る**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思えません。



条件付きのカギってどんなものですか？



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。



mQGhBD6vg7...XU2+U2P/oZSrtieUKkYeiGWURmmxj0vrWhy4NjG6NZ8lQYaz10Jz9F4qB  
PJ5nOCMiN...2dmijxb+YsKy8b9m6PFxDn1TsQMjPEklqgD2hRkf2AiOXzskoBG7ri  
y1pbmZvf...TEQIAFwUCPq+BngULBwoDBAMVÄwiDFglBAheAAaJJEHHY  
DXZ9sjTLT...5RyT6ZPUFrjd9bojYOFI8GbCtDBJUEEqU2VjdXJpdHk  
r8NNfwQ6...sTXoiQcJlVL1Gvy2q7belTqQRdAAzKnSLX58pw5C  
/WrMFZOM4...2eLSzfuezDbq9rCBRvtxssUEquMGRJTygMz26ZS1d  
nWZsMF2ENi5Xtjmv+Ajl9jccw28bpjxUjiniy1D9vNaRwgQdsuZnKPXFpyZNwccXvgXjJNMx3

数字や文字が  
並んで「カギ」  
ってすごいね

(イメージ図です)

紐づけ

買い物専用

カギに使用条件を  
追加して、被害を  
最小限に防いでいるのね

## 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と管理し、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。



暗号化されている契約書

◆ ◆

**【文書管理用ブロックチェーン】 契約書の表示**

PINを入力し、承認者を選択してください

.....

②保存している鍵ファイル

選択されている契約：

件名	：ソフトウェアの開発
契約者 1	：F 研究所 契約者 2：○△社
契約期間	：4hB65Ma...Hsc83hj8 ~ Gn2ld7M...2NdmK96G
金額	：¥ bj58C4Na...47293857
契約内容	：契約者 2 は、契約者 1 が別紙に記載しているソフトウェア開発の仕様書を元に、契約者 1 が開発を行い、50Hswm4wa に納品を行う

承認者の選択 ☒ ○△社 ▼

① F 研究所の秘密カギの部品を入力  
○ △ 社にカギの部品を入力依頼

**承認しました**

②○△社承認

**【文書利用ブロックチェーン】 契約書の表示**

【秘密制御システム】 契約書：

件名	：ソフトウェアの開発
契約者 1	：F 研究所 契約者 2：○△社
契約期間	：2017/04/01 ~ 2017/12/31
金額	：¥ 3,000,000
契約内容	：契約者 2 は、契約者 1 が別紙に記載しているソフトウェア開発の仕様書を元に、契約者 1 が開発を行い、2018/01/01 に納品を行う

③復号された  
契約書表示

# 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）