IoT eラーニング

IoTとブロックチェーン

（ブロックチェーンの概要、仕組み、IoTにおける活用）

国立大学法人　琉球大学

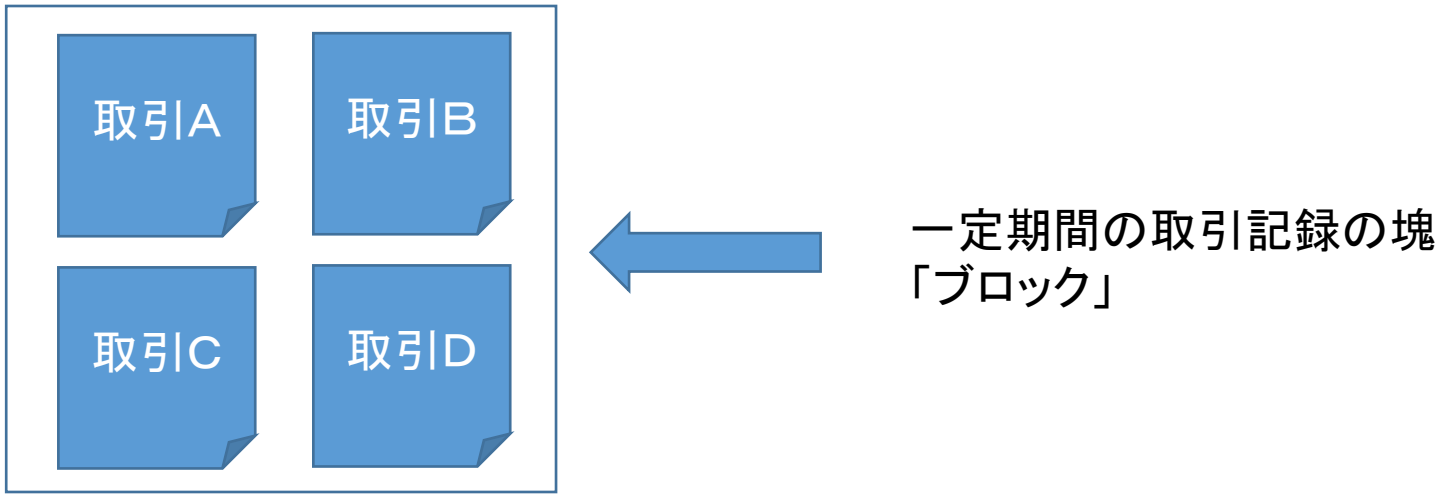
目次

ブロックチェーンとは

- **ブロック**

ブロックチェーンは仮想通貨「ビットコイン」の構成技術として誕生した。
「分散型台帳技術」と呼ばれてる。

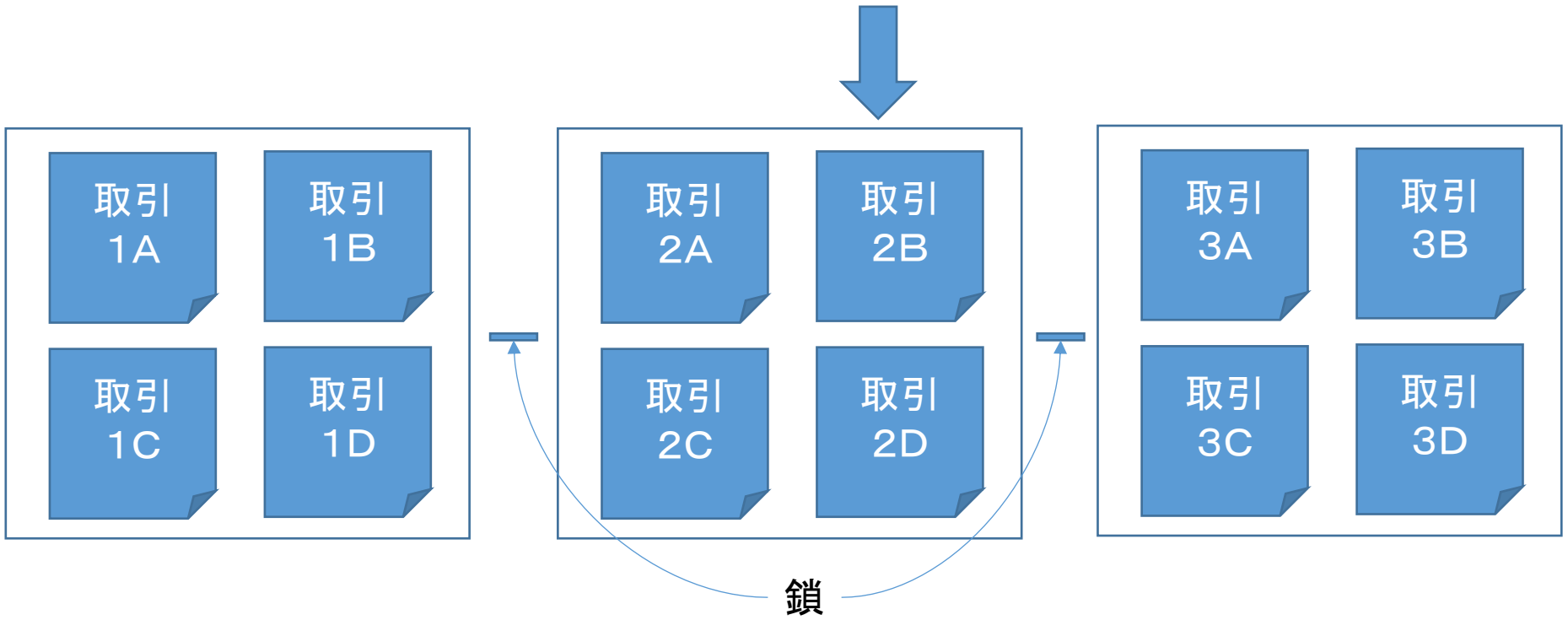
ブロックチェーンでは、一定期間の取引情報を「ブロック」という塊として扱っている。



ブロックチェーンとは

- **チェーン**

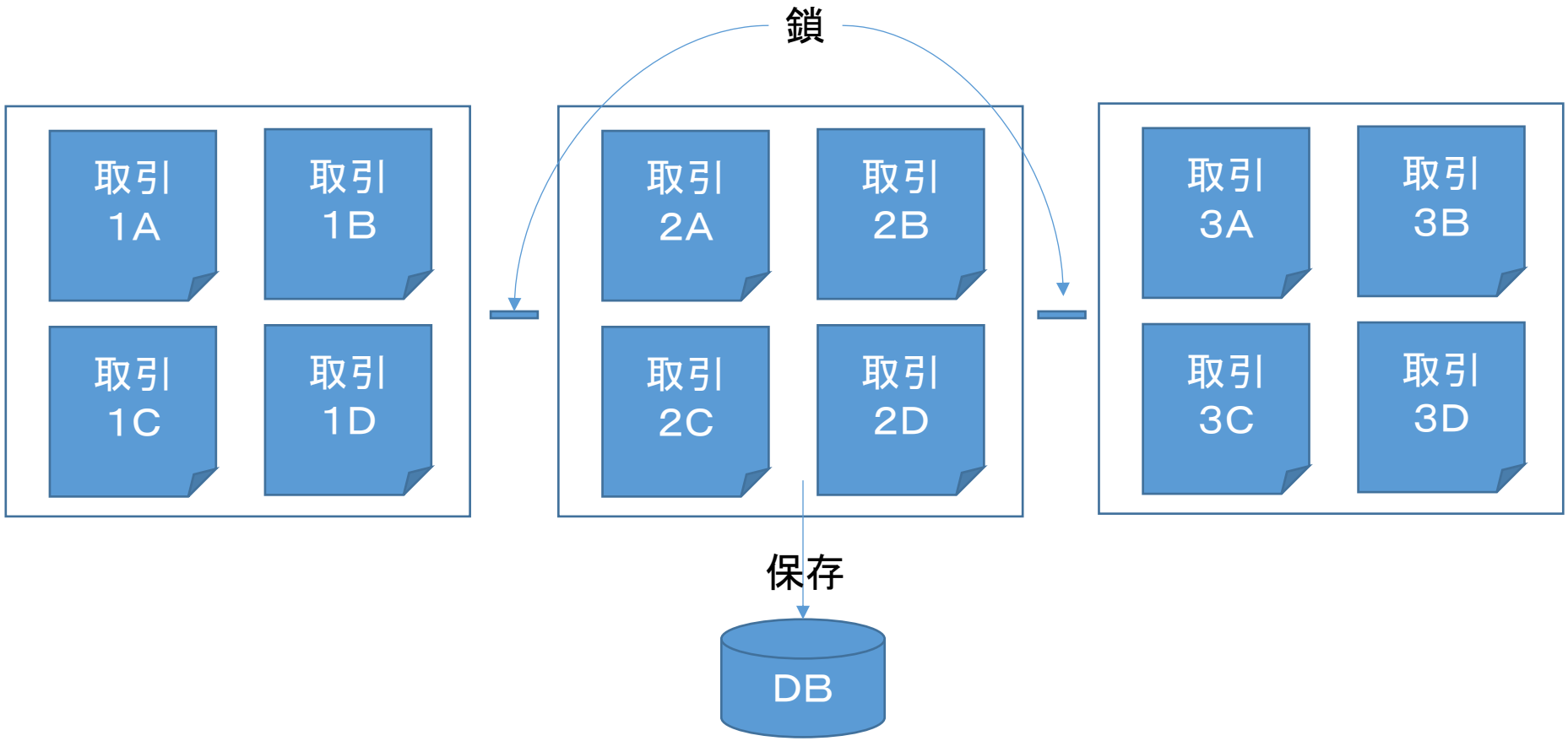
「ブロック」を取引の始まりから現在までのすべてを時系列に並べつなぎ合わせてブロック同士を関連付ける。
これを「チェーン」と呼んでいる。



ブロックチェーンとは

- **ブロックチェーンデータ**

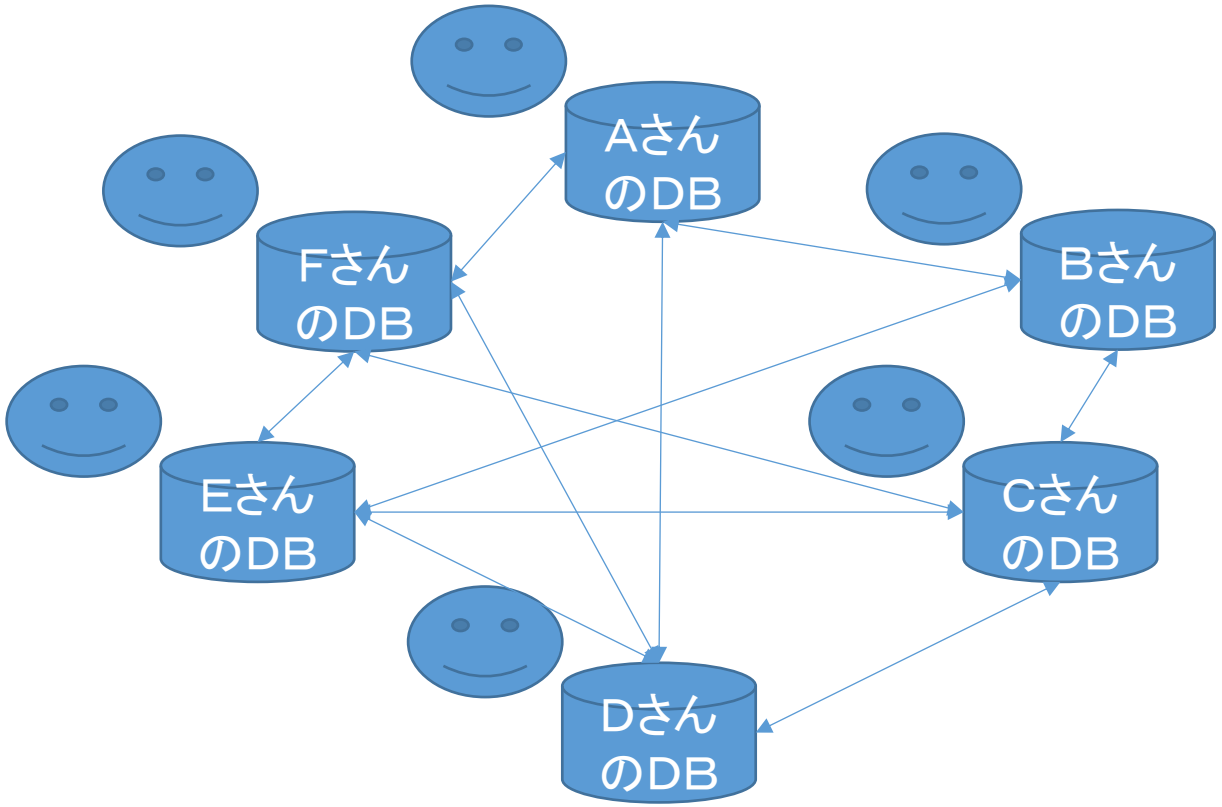
  各「ブロック」を「チェーン」によって関連付けられた情報をデータとしてデータベースへ保存する。



ブロックチェーンとは

- **データの共有**

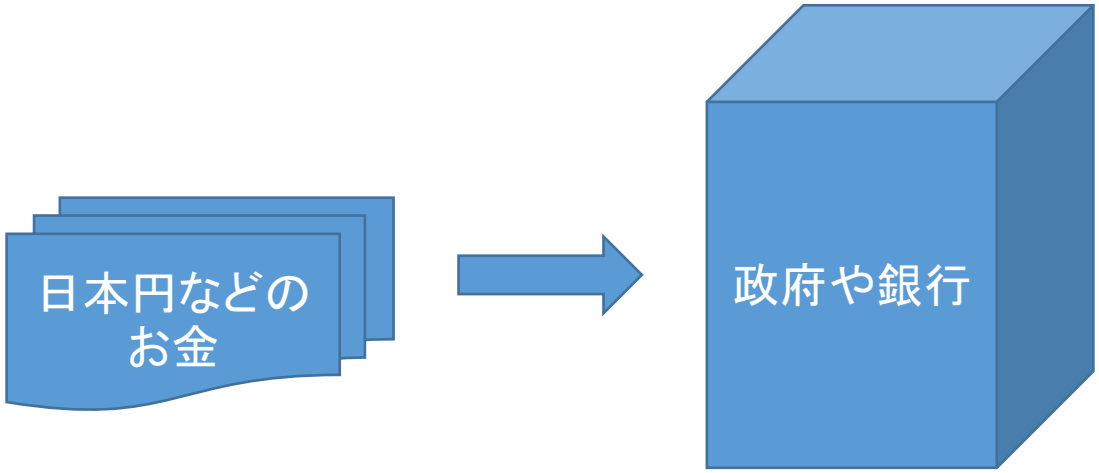
取引情報を参加者みんなで共有し維持することで、データの改ざんやトラブルに対処しやすい環境を作っている。
これがブロックチェーンの特徴の１つとなっている。



ブロックチェーンの誕生

- **実態通貨と仮想通貨**

ビットコイン等の仮想通貨の登場以前は、通貨取引では実態通貨が使用され、その実態通貨や取引記録は政府や銀行が集中して管理していた。

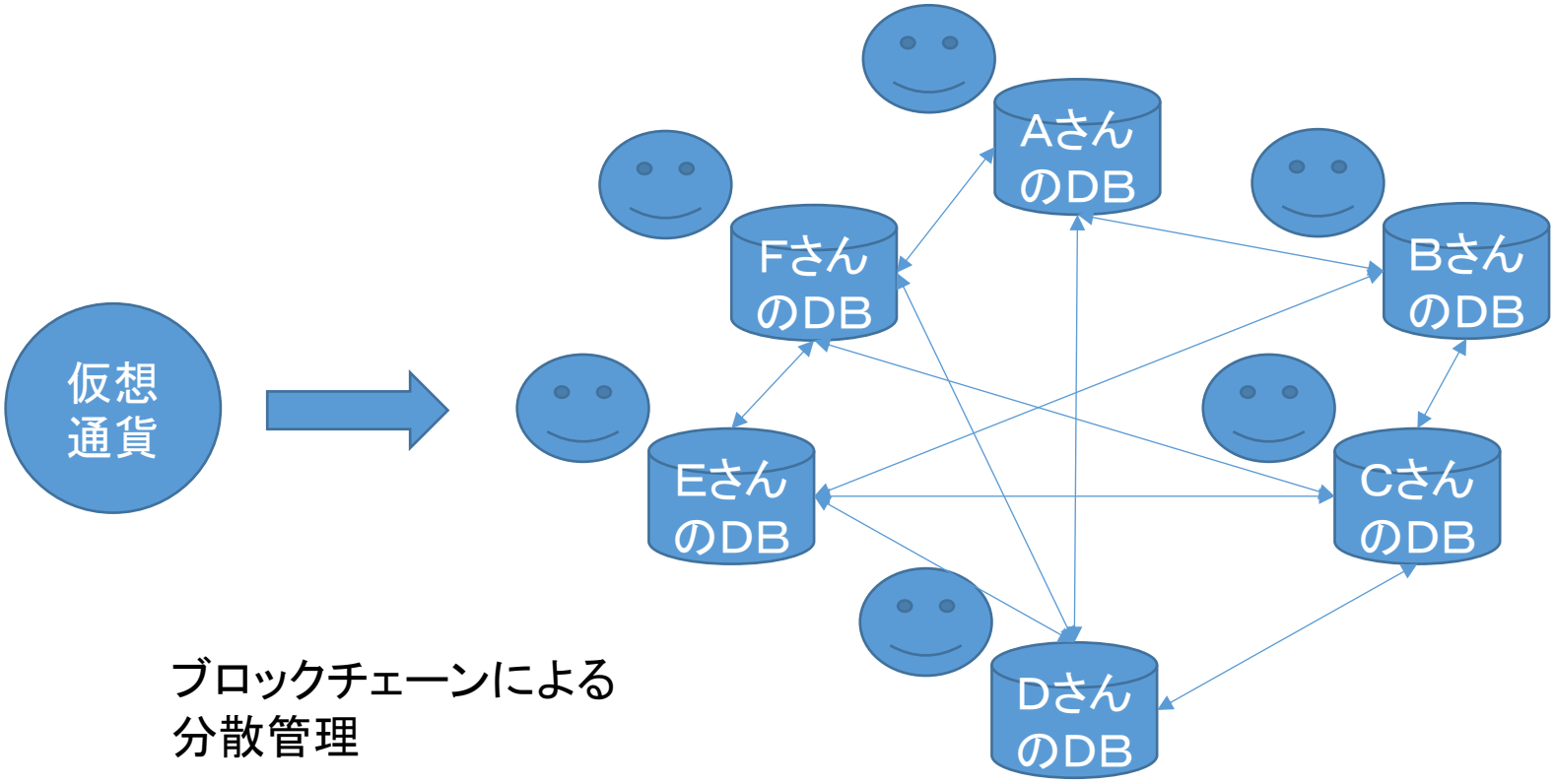


中央集権型管理

ブロックチェーンの誕生

- **ビットコインとブロックチェーン**

ビットコインでは政府や銀行などの公的な第三者を必要としない仮想通貨を取引に利用することを前提にしている。
そのため、不正の排除やシステムが停止しないことを保証する必要があり、その問題を解決する技術としてブロックチェーンが誕生した。



ブロックチェーンによる
分散管理

ブロックチェーンの考え方

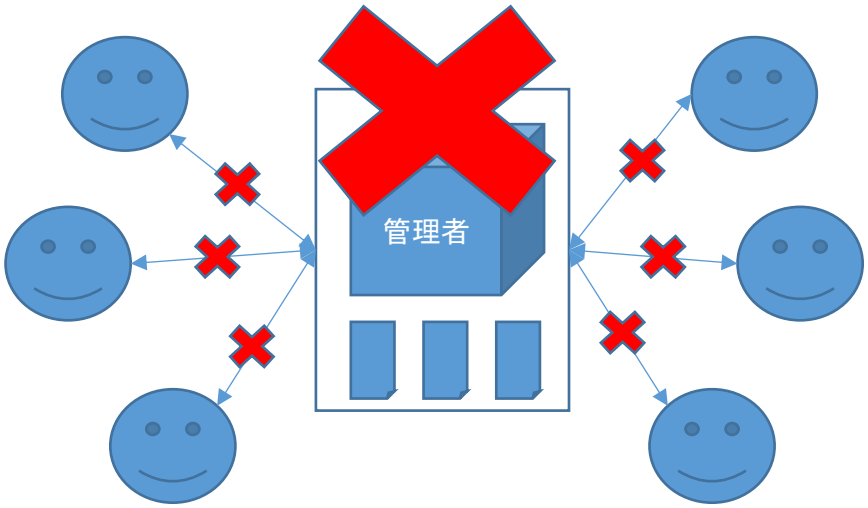
- **参加者みんなで監視**

ブロックチェーンは特定の管理者が取引記録のデータを管理していない。取引に参加している参加者みんなが確認しあって管理・維持している。

参加者みんなで支えあうブロックチェーンは、なぜ不正に強くシステムが止まらないのか？

これまでの管理方法では、取引の参加者の中央に管理者が存在し、データを集中して管理していた。もし管理者が管理しているシステムにデータ紛失やシステム停止が発生したら参加者はシステムが復旧するまで取引できなくなっていた。

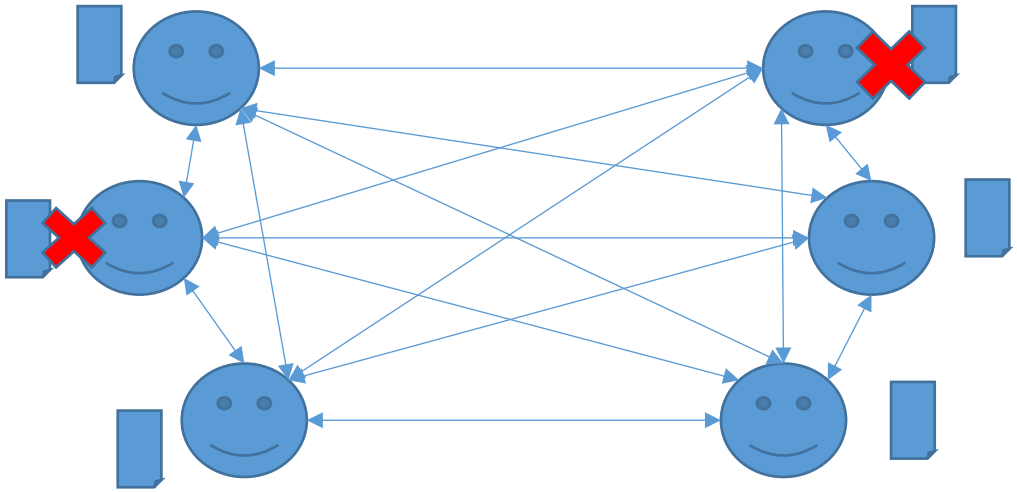
これに対して、ブロックチェーンは「管理者」が存在しないため、不正やシステム停止に強い構造となっている。



ブロックチェーンの考え方

- **ブロックチェーンデータの共有**

ブロックチェーンでは参加者みんなが同じデータを共有しているため、誰かがデータを紛失したり、誰かのシステム（参加者が使用しているコンピュータ）が停止したとしても、他の誰かが維持している共有データを使用することで全体のシステムは停止されることなく維持されている。



ブロックチェーンの考え方

- **不正が起きにくい構造**

参加者の中に悪意ある人がいれば、データを改ざんする恐れがある。

ビットコインでは台帳（データ）の検証作業を参加者に募り、一番速く作業を終わらせた人にビットコインを支払う競争システムを採用している。
この作業を「マイニング」と呼び、作業者を「マイナー」と呼んでいる。
「マイニング」作業の中には膨大かつ難解な計算問題も含んでおり、多大な労力を必要としている。
そのため、不正を行った参加者は、それが発覚しないために、誰よりも速く問題を解決することが必要となり、そのためのリソース（電力やコンピュータ等）が必要となる。

不正のためのリソースを維持する労力を考えると、真面目に参加したほうが得である状況を作り出すことで不正の防止を図っている。

仮想通貨以外への活用

● ブロックチェーンに対する期待

ブロックチェーンは現在も様々な課題を解決するために開発が進められている。
仮想通貨「ビットコイン」からスタートしたブロックチェーンも開発が進められることにより様々なサービスが提案されている。

経済産業省が発表したブロックチェーン技術に対する国内外の動向調査の中で次のサービスが活用の可能性があるとしている。

1）金融系
送金や決済のほか、証券や債券などの各種金融派生商品の取引等、様々な利用方法が提案されている。

2）ポイント／リワード
ポイントの発行や交換などの情報の維持にブロックチェーンの活用が進められている。

3）資金調達
クラウドファンディングなどの資金調達にブロックチェーンを活用する試みが進められている。管理者が必要ないなど、コストが低くなることによる集められた資金の取り分が大きくなるメリットが期待されている。

仮想通貨以外への活用

4）コミュニケーション
メッセージングサービスやSNSなどでブロックチェーンの利用が進んでいる。

5）資産管理
土地の登記など資産の売買記録の管理などでブロックチェーンの活用が始まっている。

6）ストレージ
ネットワーク上でデータを管理するサービスでブロックチェーンの利用が検討されている。顧客から預かったデータをブロックチェーン上で障害耐性の高いサービスが期待される。

7）認証
商品などの正当性を認証する仕組みとしてブロックチェーンを活用するサービスが考えられている。

8）シェアリング
カーシェアリングなどのシェアリングエコノミーで利用券や利用状況の管理にブロックチェーンが活用されている。

仮想通貨以外への活用

９）商流管理

電子データ交換（EDI）をブロックチェーンに置き換える利用だけでなく、商品の加工履歴（材料から製品まで）もブロックチェーンに登録することでトレーサビリティの実現が期待されている。

１０）コンテンツ

ネット上でのコンテンツ配信のサービスに利用状況や課金の情報などの管理に活用されている。

１１）将来予測

英国のブックメーカーをブロックチェーン上で提供するようなサービスが出現している。参加者が様々な事案について投票し合い、その結果によって報酬を得ている。

１２）公共分野

自治体などが提要する様々な公共サービスをブロックチェーン上で提供する仕組みを実現する試みが行われている。

１３）医療分野

カルテの記録や投薬状況など、医療に関わる情報をブロックチェーンで管理することで安全性の確保が考えられている。

仮想通貨以外への活用

１４）IoT分野

IoTでもブロックチェーンの活用が期待されている。センサーなどが管理者を介さずに、データをそれぞれ交換しながら処理を進めていく等の利用方法が想定されている。

ブロックチェーンの技術

- **従来からある技術を活用**

ブロックチェーンの特徴は
- 不正や改ざんに強い
- 中央集権型ではなく分散型の管理
- ダウンタイムゼロの実現

である。

これを実現するためにブロックチェーンでは次の技術を活用している。

- 暗号技術（ハッシュ・電子署名）
- P2Pネットワーク
- コンセンサスアルゴリズム

これらの技術は従来から存在し、「枯れた技術」と言われている。
ブロックチェーンはこれらの技術を組み合わせることで上記の特徴を実現している。

- **データ改ざんの発見（ハッシュ）**

ハッシュとは、データを定められた計算式に通すことで算出された値をもとに、データの改ざん、破損を検出するための技術である。
定められた計算式のことを「ハッシュ関数」と呼び、算出された値を「ハッシュ値」と呼ぶ。

ハッシュの特徴として

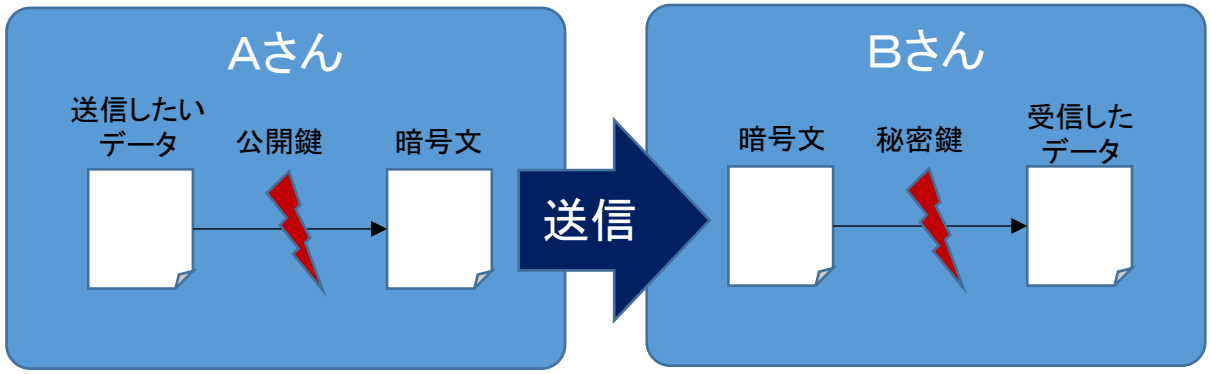
・ハッシュ値は元のデータサイズに関わらず一定の長さになる
・ハッシュ値から元のデータを求められない
・異なるデータから同一のハッシュ値は算出されない

がある。

ブロックチェーンでは、これらの特徴を生かしデータとハッシュ値を合わせて管理することにより、データが改ざん・破損していないかを検出する際に利用している。

● なりすましの防止（電子署名）

電子署名は、データが本人により作成された事とデータ改ざんされていない事を証明しデータの妥当性を保証する技術である。
これは既にある技術で様々な方式がある。ブロックチェーンのもととなったビットコインでは電子署名として「公開鍵暗号方式」を採用している。
公開鍵暗号方式は「公開鍵」と「秘密鍵」というキーで成り立ち、次のようにしてなりすましや改ざんを防止している。

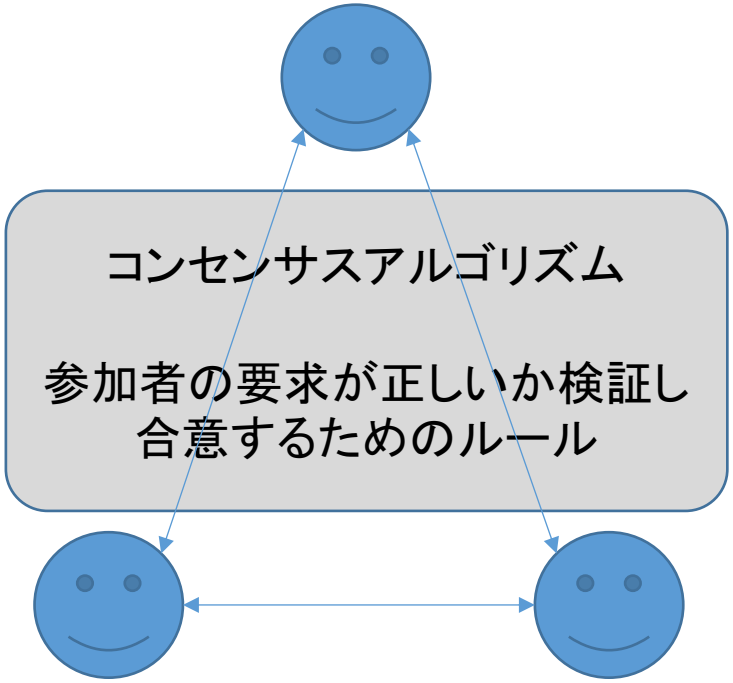


Aさんは、「Bさんの公開鍵」で暗号化　　Bさんは、「Bさんの秘密鍵」で復号

ハッシュ値も合わせて送ることにより、送られたデータに改ざんされていないかを確認できる。

- **コンセンサスアルゴリズム**

分散型のしくみを利用しているブロックチェーンで重要になってくるのが合意形成である。
保管するデータの妥当性を承認する作業ではネットワーク全体で合意を得る必要がある。
この承認者の間で合意形成を得る仕組みを「コンセンサスアルゴリズム」という。
ビットコインでは悪意ある参加者が参加することを想定し、「プルーフオブワーク（PoW）」というコンセンサスアルゴリズムを採用している。



- **プルーフオブワーク（PoW）**

ビットコインではコンセンサスアルゴリズムとして「プルーフオブワーク（PoW）」を採用している。

PoWとは膨大な計算量を必要とする問題に対して、最も速く解いた人に発言権を与え合意を形成することである。

ビットコインでは最も速く検証を行った人にBTC（ビットコインの仮想通貨）という報酬を与えている。
この報酬を得るために参加者間で競争が起こり、不正を行うにはその競争に勝つ必要があり多大なコストが必要となる。
そのため、不正を働かず承認作業に参加したほうが合理的であると判断されることを期待した仕組みである。

- **セキュリティ対策**

IoTではセキュリティ対策が大きな課題であると認識されている。

あらゆるモノがインターネットにつながるということは、あらゆるものがハッキング等の犯罪のターゲットにされる可能性があることを意味する。
そこで、ブロックチェーンの技術をIoTに取り入れることによりセキュリティ対策の向上が期待されている。

IoTも多くの機器がインターネットにつながり膨大なデータが行きかうため、中央集権型の管理よりも分散管理型の管理のほうが適しているのではないかと言われている。

そのため、分散管理型のブロックチェーンで活用されている認証処理のしくみをIoTに導入できれば利用者認証におけるセキュリティ対策が進むのではないかと期待されている。

- **負荷の軽減**

IoTの普及が進めば、今まで以上にインターネットにつながるモノとデータが増えていく。

従来のクライアントサーバ型の管理では、処理対象増加に比例し主にサーバの負荷の増大が見込まれている。

IoTを分散型で管理し、接続されているモノ同士でデータ等の取引を自律的に行えれば、システム全体の負荷が軽減されるのではないかと考えられている。

ブロックチェーンの技術をベースに、自律型分散技術、取引内容の確認と処理の実行を自動で行うスマートコントラクトが登場した。

この技術をIoTに取り込むことにより負荷の軽減が期待されている。

● 本人のみ受け取り可能な宅配ボックス

IoTとブロックチェーンの技術を活用した「本人のみ受け取り可能な宅配ボックス」サービスの実証実験を、2017年5月30日から6月9かけて実施したとＧＭＯインターネット、ＧＭＯグローバルサイン、セゾン情報システムとパルコが発表した。

実験ではＧＭＯインターネットが提供するブロックチェーンプラットフォームとセゾンが提供するIoT技術を利用した宅配ボックスを融合し、利用者に対して注文した荷物が宅配ボックスに配送された事の通知と荷物を本人のみが取り出せるサービスの検証が行われた。

IoTとブロックチェーンを融合したことによる

- 利用者の登録と本人認証
- トレーサビリティ
- スマートコントラクトによる取引の自動化
- 安全で安定したデータの連携

の実現を図っている。

IoTデバイス向けセキュリティサービス

アイビーシー株式会社は2017年12月5日にブロックチェーンの技術を利用した承認システムとデバイスプロビジョニングシステムで構成された、IoTデバイス向けセキュリティサービスの実証実験を開始したと発表した。
このサービスは、ブロックチェーン技術による電子証明システムとデバイスプロビジョニング技術で、IoTセキュリティをソフトウェアだけで実現することを目指している。

IoTの拡大によりIoTデバイスに対するセキュリティは大きな課題の１つであるが、IoTデバイスの性能による制約などにより従来のPC型セキュリティ対策を適用することは難しい。
最近の動向としては専用チップと認証局によるIoTデバイスのセキュリティ対策が注目されているがコストの増大などが課題と指摘されている。

これらのことを踏まえ、今回行われた実証実験のサービスで

- 専用チップを不要とする
- 認証局を不要とする
- マルウェア対策を不要とする

を実現することを推進している。