ブロックチェーンの技術について

1)ブロックチェーンは「共有の記録帳」

たとえば、クラス全員が同じノートを持っていて、

① 誰かが「A さんが B さんに 100 円渡した」と書いたら

② クラス全員のノートにも同じ内容が書き込まれ

③ しかも**過去のページを書き換えると、みんなのノートと矛盾してバレる**

というような状態を作るのがブロックチェーンです。

この「みんなで同じ記録を持つ」「過去の改ざんが難しい」を実現するために、いくつかの技術が組み合わさっています。

2）ブロックチェーンを支える技術（要素）と、具体的な使われ方

ここからが本題で、**“それぞれの技術”が何をしていて、現実でどう使われるか**を分解して説明します。

A. 分散ネットワーク（P2P）:「みんなが台帳のコピーを持つ」

何をする技術？

中央のサーバー1 台に記録を置くのではなく、参加者（ノード）がネットワークでつながり、**台帳のコピーを各自が持つ**形にします。

これがあると何が嬉しい？

- どこか 1 カ所が壊れても全体が止まりにくい（耐障害性）
- 誰か 1 社だけが勝手に記録を書き換えるのが難しい（検閲・改ざん耐性）

具体的な使い方・使われ方

- **暗号資産（送金）**：世界中のノードが同じ取引履歴を共有することで、銀行のような単一管理者なしに送金記録を維持できます。
- **企業間の共同台帳（コンソーシアム型）**：複数企業が参加して「取引履歴」「出荷履歴」を共同で管理する用途で使われます（参加者は限定）。

B. ハッシュ（指紋みたいなもの）:「改ざんを見破る仕組み」

何をする技術？

ハッシュ関数は、データから「短い文字列（ハッシュ値）」を作る技術です。特徴は：

- 元データが少しでも変わると、ハッシュ値が大きく変わる
- ハッシュ値から元データを復元するのは現実的に難しい

ブロックチェーンでの使い方

- ブロック（取引のかたまり）ごとにハッシュ値を作ります
- さらに、**次のブロックが前のブロックのハッシュ値を参照**します
  → これで「鎖（チェーン）」になります

なぜ改ざんが難しい？

過去のブロックのデータを 1 文字でも変えると、そのブロックのハッシュが変わり、次のブロック以降が全部つながらなくなるからです。

具体的な使い方・使われ方

- **証明・タイムスタンプ（存在証明）**：文書そのものをチェーンに載せず、文書のハッシュだけを載せる。
  → 「この文書はこの時点で確かに存在していて、その後改ざんされていない」を説明しやすい
- **サプライチェーン**：検査結果や証明書の“ハッシュ”を記録し、改ざんを検出しやすくする。

C. デジタル署名（公開鍵暗号）：「本人が承認したことを証明する」

何をする技術？

「秘密鍵」と「公開鍵」という 2 つの鍵を使います。

- **秘密鍵**：絶対に他人に渡してはいけない。署名に使う
- **公開鍵**：他人に公開して OK。署名の検証に使う

送金などの操作は、秘密鍵で「署名」して行います。
周りのノードは公開鍵で「確かに本人の署名か」を確認できます。

具体的な使い方・使われ方

- **ウォレット（財布アプリ）**：実は“お金”を持っているのではなく、秘密鍵を安全に管理して「署名」するための道具です。
- **ID／ ログイン**：パスワードではなく署名で「自分である」ことを証明する仕組み（分散型 ID の発想）にも応用されます。

超重要ポイント：
秘密鍵を失う＝資産や権限を失う、盗まれる＝乗っ取られる、という性質が強いです（取り消し・再発行が簡単ではない）。

D. ブロック（記録のかたまり）：「取引をまとめて確定させる」

何をする技術？

ブロックチェーンでは、取引（トランザクション）を 1 件ずつではなく、ある程度まとめて「ブロック」に入れて確定します。

具体的な使われ方

- **手数料（ガス代）**：ブロックに入れてもらうために手数料が必要な設計が多いです。混雑すると高くなる、などの現象が起こります。
- **確定時間**：すぐ確定する仕組みもあれば、何ブロックか積み重なってから「より安全」とみなす運用もあります。

E. コンセンサス（合意形成）：「正しい台帳はどれかを皆で決める」

何をする技術？

参加者が多数いると、悪意ある人が嘘を流したり、同時に複数案が出たりします。
そこで「どのブロックを正史（正しい履歴）として採用するか」を決めるルールが必要で、これがコンセンサスです。

代表例（イメージ重視）：

- **PoW（Proof of Work）**：計算競争で“正史”を作る権利を得る（電力や計算がコスト）
- **PoS（Proof of Stake）**：保有・預け入れ（ステーク）などを基に選ばれて提案する（仕組みはチ

ェーンによって多様）

- **BFT 系（企業向けで多い）**：参加者が限定され、投票で合意するような設計が多い

具体的な使い方・使われ方

- **パブリックチェーン（誰でも参加）**：不特定多数でも合意できるように PoW/PoS 系が使われがち
- **企業・行政の共同利用（参加者が決まっている）**：BFT 系や許可型の方式で、速さ・コスト・統制を重視することが多い

F. スマートコントラクト：「条件に応じて自動実行するプログラム」

何をする技術？

ブロックチェーン上で動くプログラムです。

「もし A が起きたら B を実行する」という約束を、**第三者なしで自動的に実行**できます。

たとえ話

- 自販機に近いです。お金を入れてボタンを押すと、店員がいなくても商品が出る。
- スマートコントラクトは「契約」そのものというより、**契約の一部を自動執行する装置**だと思うと誤解が少ないです。

具体的な使い方・使われ方

- **DeFi（分散型金融）**：交換（DEX）、貸し借り、担保管理、利息計算などを自動化
- **NFT**：発行、移転、ロイヤリティ設定（チェーンや規格による）
- **保険の自動支払い（条件付き）**：条件を満たしたら自動で支払う、などの設計が可能（ただし現実データとの連携が課題）

G. オラクル：「現実世界の情報をチェーンに持ち込む」

何をする技術？

ブロックチェーン単体だと「現実の天気」「為替」「試合結果」などは分かりません。

外部データをスマートコントラクトに届ける仕組みがオラクルです。

具体的な使い方・使われ方

- **保険**：航空便の遅延情報が来たら自動支払い
- **金融**：価格情報を基に清算や担保比率を計算
- **サプライチェーン**：IoT センサーの温度ログなどを取り込む（ただし“センサーが嘘をついたら？”問題は別途対策が必要）

H. トークン（FT / NFT）：「価値や権利を“記録”として表す」

何をする技術？

ブロックチェーン上のデータで、

- **FT（代替可能トークン）**：1 枚＝1 枚で同じ価値（通貨っぽい）
- **NFT（非代替トークン）**：それぞれが固有（会員証、チケット、証明書っぽい）

具体的な使い方・使われ方

- **決済・送金**：FT（暗号資産やステーブルコイン）で移転
- **ポイントや会員証**：NFT や FT で発行し、譲渡可/不可などのルールを設計

- **チケット**：NFT で「転売条件」「本人確認連携」を組み込む試み
- **ゲームアイテム**：所有・移転の履歴が残る（ただしゲーム運営側の設計次第）

注意：NFT は「画像そのもの」をチェーンに直接保存しない設計も多いです。
多くは「所有権を示す ID＋参照先（メタデータ）」を記録します。

3）取引は実際どう流れる？（ざっくり手順）

例：A さんが B さんに送金する

1. A さんがウォレットで「B へ〇〇送る」を作成
2. A さんが**秘密鍵で署名**する（「本人の承認」の証拠）
3. 取引がネットワークに配られる（P2P）
4. ノードが「署名が正しいか」「残高（状態）が足りるか」などを検証
5. まとめてブロックに入り、コンセンサスで確定
6. B さん側のウォレットが受け取りを表示（チェーン上の状態が更新された結果）

4）ブロックチェーンの種類と、向いている使い方

パブリック型（誰でも参加できる）

向いている：公開性・中立性・検閲耐性が重要な場面

- 国境を越えた送金、オープンな金融、誰でも検証できる証明、オープンな資産管理 など

課題になりやすい：手数料、処理速度、プライバシー、規制対応

プライベート/コンソーシアム型（参加者が決まっている）

向いている：企業間の共同台帳、監査、ガバナンスが重要な場面

- 貿易・物流、証明書管理、企業間決済、トレーサビリティ など

課題になりやすい：

「それって普通のデータベースでよくない？」が常に問われます。
ブロックチェーンにする価値は主に**“複数組織での共同管理”**にあります。

5）具体的な活用例（「どう使われているか」）

① 送金・決済（暗号資産 / ステーブルコイン）

- 銀行の営業時間や国境の壁を越えて移転できる設計がある
- ステーブルコインは価格変動を抑える設計で、決済・精算に使われやすい

使い方（ユーザー目線）

ウォレット作成 → アドレスに送る → 手数料を払って送金 → 受取側で確認

② DeFi（分散型金融）

- 交換（DEX）、貸し借り、利回り運用、担保による借入などをスマートコントラクトで実現

使い方

ウォレットで DApp に接続 → 交換や預け入れを操作 → 取引がチェーンに記録される

注意点

バグ・ハッキング・設計ミスのリスク、価格急変、手数料、操作ミスがそのまま損失になることも

③ NFT（デジタル所有・会員証・チケット）

- 「誰が持っているか」「いつ移転したか」をチェーンで追跡

使われ方

デジタルアート、ゲームアイテム、ファン会員証、イベントチケット（転売制限を設計する試みも）

④ 証明・監査（改ざんされにくいログ）

- 契約書・検査結果・研究データなどのハッシュを記録
- 後日「当時の内容と一致する」と説明しやすい（監査に強い）

使われ方

社内外の監査ログ、提出書類の真正性確認、タイムスタンプ的な用途

⑤ サプライチェーン（トレーサビリティ）

- 原材料→加工→輸送→販売までの履歴を複数企業で共有

使い方（現場のイメージ）

製品に QR コード等 → 各工程で記録 → 関係者が同じ履歴を確認

注意点

「最初の入力が嘘なら？」問題は残るので、IoT・監査・権限管理などとセットで設計することが多い

⑥ ID・認証（分散型 ID の考え方）

- パスワード中心から、署名ベースで本人性を確認する発想へ
- 証明書（資格・所属など）を“検証可能”にする仕組みと組み合わせる例がある

6）ブロックチェーンが向いている問題・向かない問題

向いている

- **複数の組織・人が関わり、中央管理者を置きにくい/置きたくない**
- **履歴の改ざんが困る**
- **「誰がいつ何をしたか」の追跡が重要**

向かない（または工夫が必要）

- 1 社だけで完結するなら普通の DB の方が速く安いことが多い
- 個人情報や機密情報をそのまま載せるのは危険（公開性との相性）
- 高速大量処理（例：SNS の全投稿を全部オンチェーン）はコストが重くなりがち

---

7)まとめ

ブロックチェーンは、

① みんなで同じ台帳を持ち（分散）

② 本人が署名して記録し（デジタル署名）

③ ブロックを鎖でつなぎ（ハッシュ）

④ どれが正しい履歴かを合意して（コンセンサス）

⑤ 必要なら自動実行もできる（スマートコントラクト）

仕組みです。