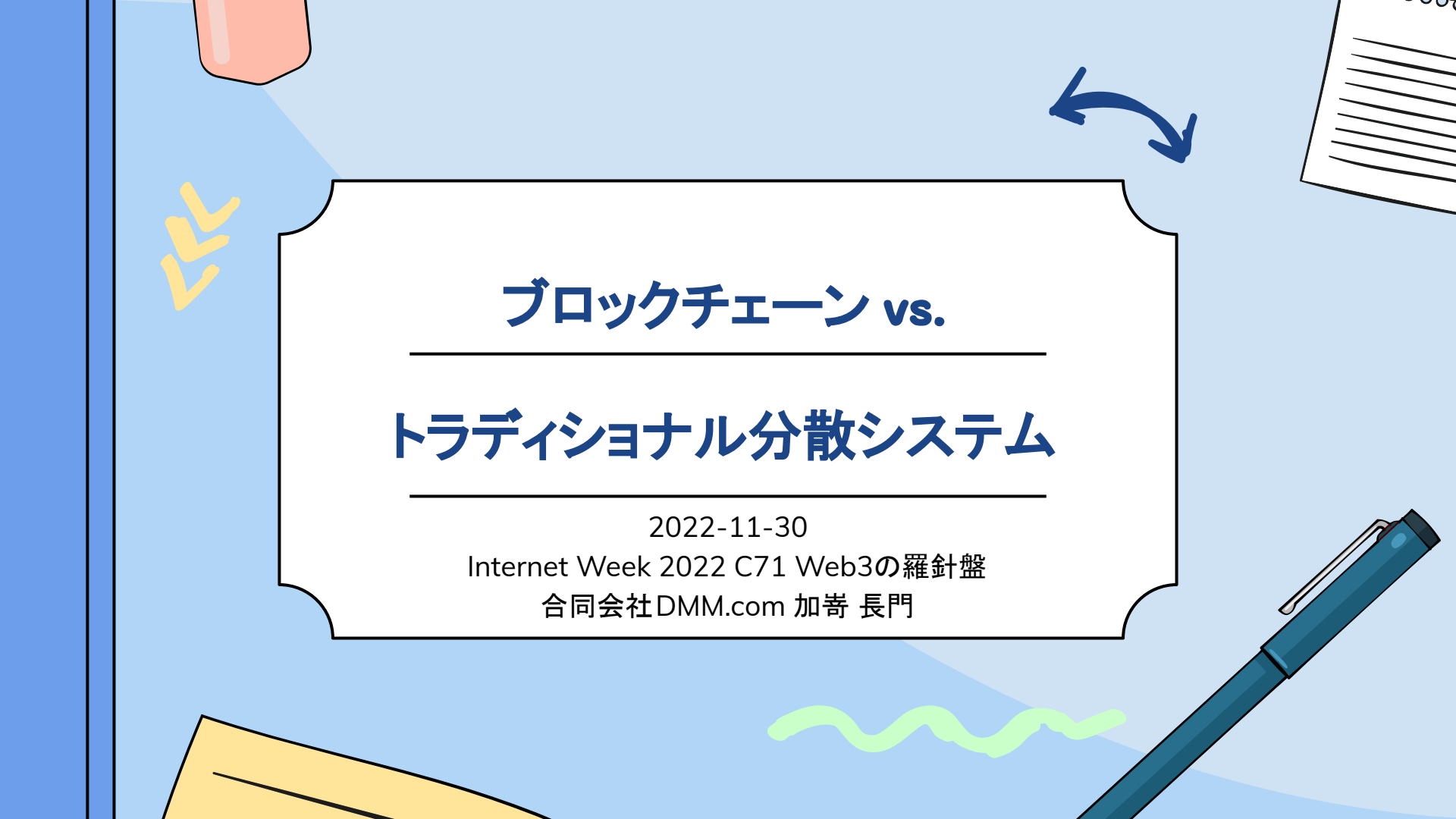

ブロックチェーン vs.
トラディショナル分散システム
2022-11-30
Internet Week 2022 C71 Web3の羅針盤
合同会社DMM.com 加嵜 長門

自己紹介

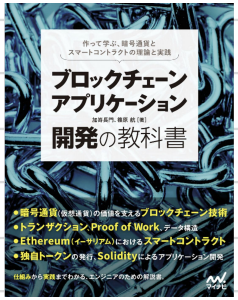
■ 加嵜 長門 (Kasaki Nagato)

来歴

2014.4 DMM.comグループ 入社
2014.6~2018.4 CTO室/ビッグデータ部:
　　データ分析基盤システム立ち上げ・レコメンド開発
2018.5~2021.3 スマートコントラクト事業部 /ブロックチェーン研究室 :
　　ブロックチェーン活用事業企画・技術開発
2022.5~ Web3事業部: テックグループリーダー

著書

『試して学ぶ スマートコントラクト開発』(マイナビ出版)
『ブロックチェーンアプリケーション開発の教科書』(マイナビ出版)
『ビッグデータ分析・活用のための SQLレシピ』(マイナビ出版)
『詳解Apache Spark』(技術評論社)



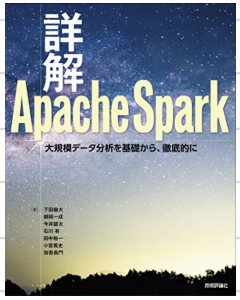
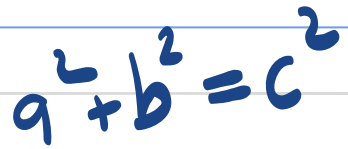
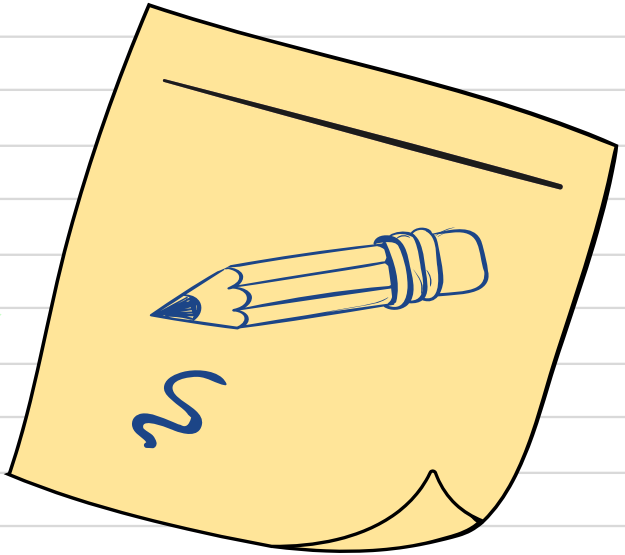


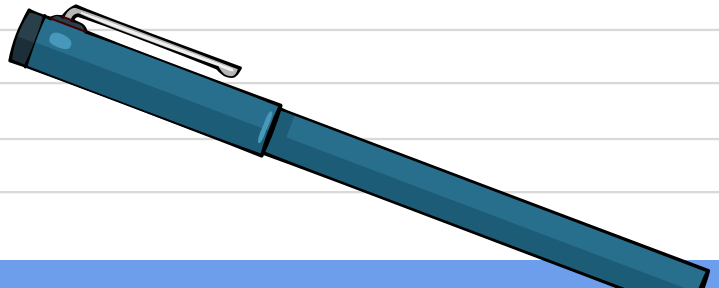
Table of Contents



ブロックチェーンとはなにか



ビットコイン論文から
ブロックチェーンの定義を探る



ブロックチェーンの一般的な定義

狭義のブロックチェーン

- 「**ビザンチン障害**を含む**不特定多数のノード**を用い、時間の経過とともにその時点の **合意が覆る確率が0へ収束するプロトコル**、またはその実装をブロックチェーンと呼ぶ。」

広義のブロックチェーン

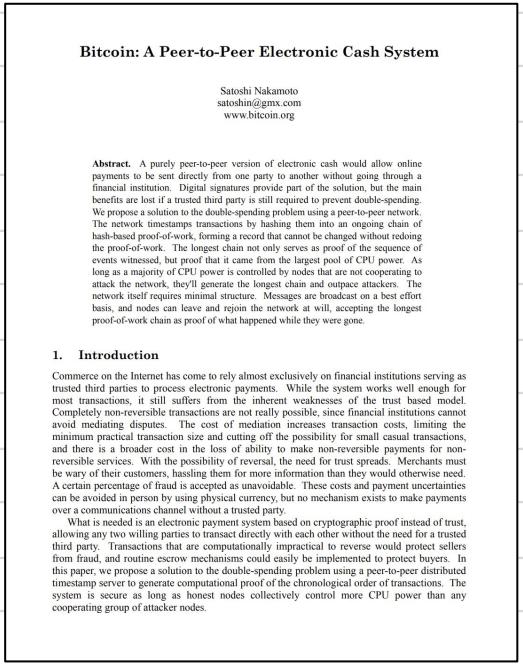
- 「**電子署名**と**ハッシュポインタ**を使用し**改竄検出が容易なデータ構造**を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、 **高可用性及びデータ同一性等を実現する技術**を広義のブロックチェーンと呼ぶ。」

JBA 一般社団法人 日本ブロックチェーン協会「ブロックチェーンの定義」

「オリジナル」のブロックチェーン

ビットコイン論文

- 2008年10月 Satoshi Nakamotoを名乗る人物（実在性は未確認）により公開される
- 「現在のインターネット上の商取引は殆ど例外なく、電子取引を処理する信用の置ける第三者の金融機関に依存している」
- 「必要なのは信用ではなく、暗号学的証明に基づいた電子取引システム」
- 「本論文では、取引が時系列に行われたかについて、計算に基づいた証明を生成する **P2P 分散型タイムスタンプサーバ** を使用し、二重支払い問題の解決策を提案する」



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

bitcoin.org

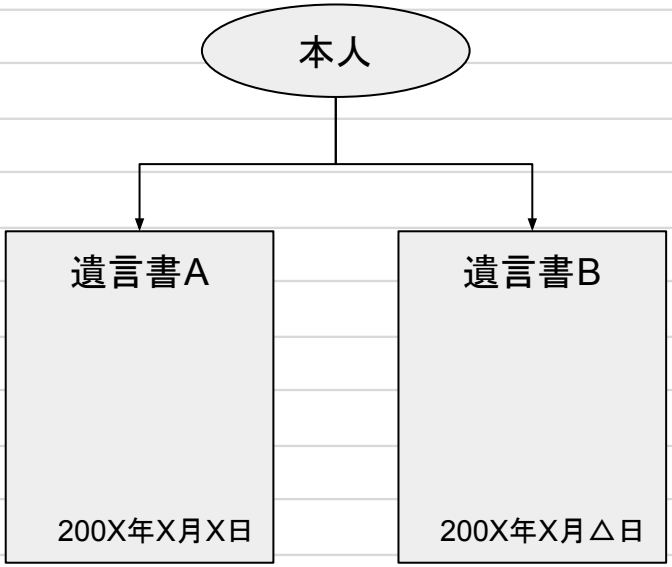
「タイムスタンプサーバ」とは

電子署名とタイムスタンプ

- 電子データの原本性を保証するための重要技術
- 電子署名：本人性を証明
- タイムスタンプ：データの存在や前後関係を証明

遺言書の例

- 本人の作成した遺言書が 2通ある場合
- 2通の遺言書に競合が発生した場合、どちらが優先されるのか？
  ⇒ 後に作成された方が優先される
  ⇒ 本人が作成したことだけでなく、「いつ」作成されたのかという情報が重要



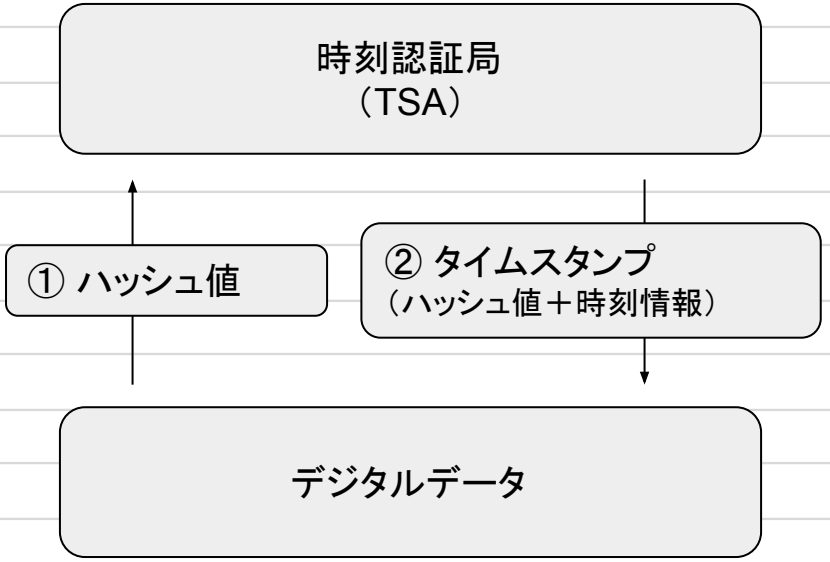
時刻認証局の必要性と課題

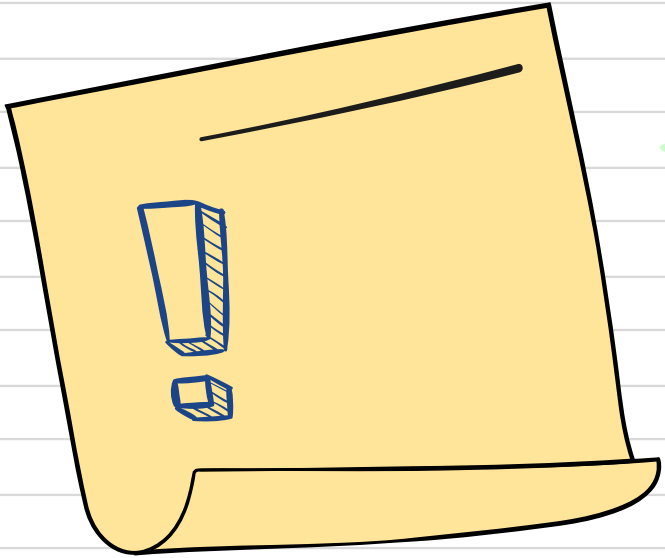
時刻認証局

- デジタルデータのハッシュ値に対して、現在時刻を組み合わせたタイムスタンプを発行
- 過去時刻に遡ったタイムスタンプは発行しないことを保証している

- 時刻認証局を「信用」しなければならない
  時刻認証局が停止したら？
  時刻認証局が不正をおこなったら？

- ⇒ これらの「信用」リスクを、**「P2P」「分散型」**システムにより解決しようとした仕組みが **ブロックチェーン**





分散システムの障害モデル

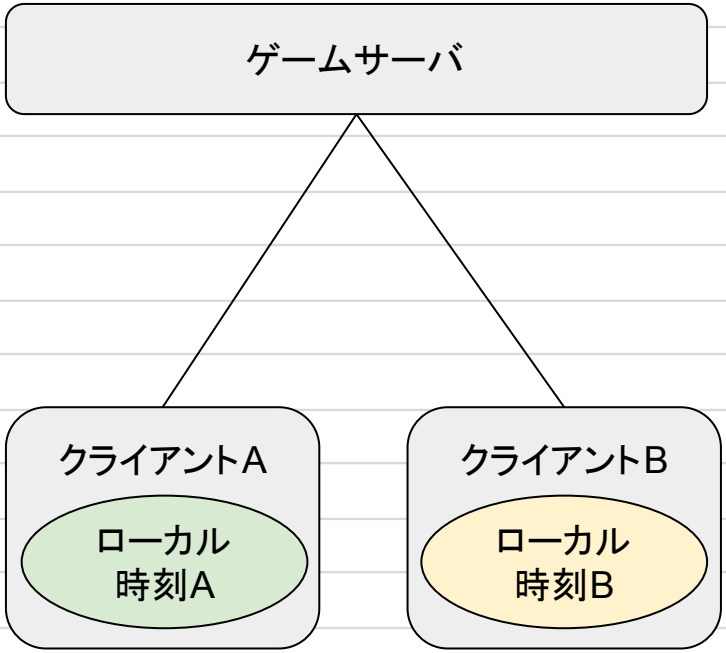
さまざまな障害モデルの類型を知る

分散システムにおける時刻同期

ソーシャルゲームの例

- ソーシャルゲームにおいて、ある特定の時間帯のみに参加できる限定イベントの実装を考える

- 時刻の判定を、各プレイヤーのクライアント側のローカル時刻を参照する場合：
- 必ずしも各クライアントのローカル時刻が正しいとは限らない
- 不正にクライアント側のローカル時刻を操作して、運営が意図しない時間帯に限定イベントをプレイできてしまうかもしれない

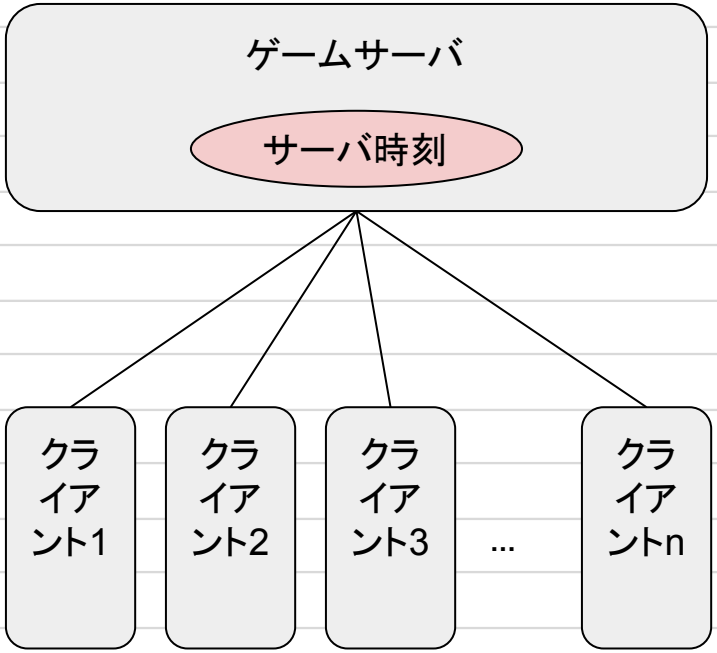


分散システムにおける時刻同期

ソーシャルゲームの例

- ソーシャルゲームにおいて、ある特定の時間帯のみに参加できる限定イベントの実装を考える

- 時刻の判定を、ゲームサーバ側のサーバ時刻を参照する場合：
- クライアント間の時刻不一致や不正行為は解消される
- 特定時刻にサーバへのアクセスが集中し、負荷が高まる（**単一障害点：SPoF**）
  ⇒ 単一障害点を排除するための分散技術が発展



分散システムにおける障害の種類

単一障害点における「障害」とは

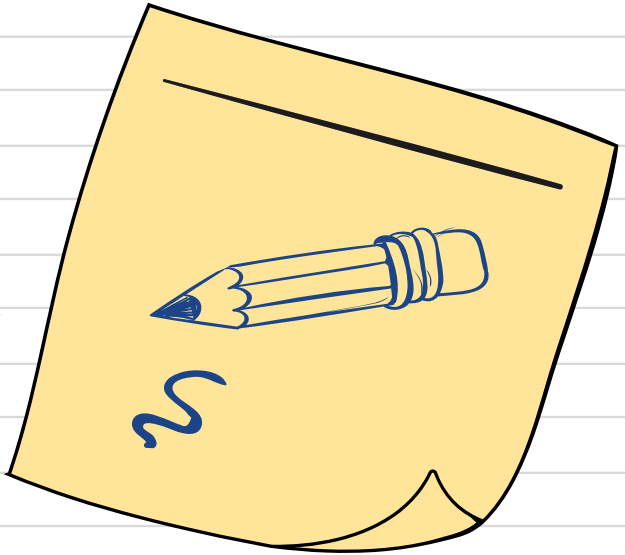
- **クラッシュ障害**
  サーバがクラッシュ（停止）する
- **欠落障害**
  サーバがリクエストへの応答に失敗する
- **タイミング障害**
  サーバが想定しているタイミング内に応答できない
- **応答障害**
  サーバの応答内容が間違っている
- **ビザンチン障害（任意障害）**
  その他発生し得るすべての障害
  （例えば、特定のリクエストだけ意図的に応答しなかったり、応答を改変したりする）
  ⇒ P2Pシステムでは、ビザンチン障害が発生しても正常に機能するシステムが求められる

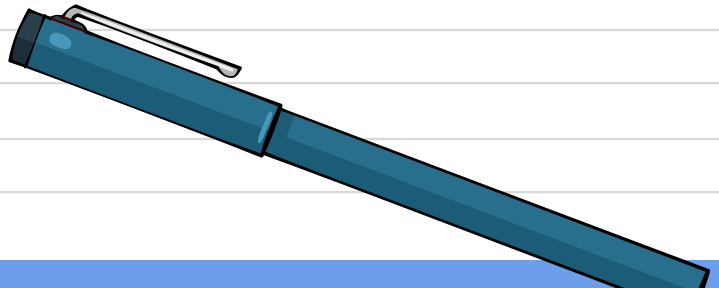
これらの障害に対しては、サーバの冗長化や負荷分散技術により対処可能なことが多い

多くのWebサービスでは、クラッシュ障害やタイミング障害などは考慮しても、ビザンチン障害までは考慮していない

ブロックチェーンの新規性

それまでの分散システムと
ブロックチェーンはなにが違うのか？





ブロックチェーンの新規性考察

- **タイムスタンプサーバを「分散化」したこと？**
  ⇒ レスリー・ランポートの「論理クロック」ですでに提唱されているアイデア
  Time, Clocks, and the Ordering of Events in a Distributed System（1978年）

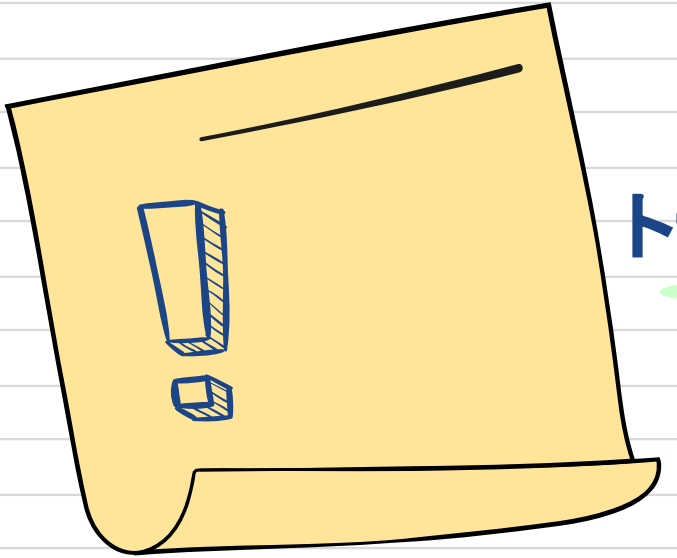
- **ビザンチン障害耐性を持った分散システムを実現したこと？**
  ⇒ 同じくランポートらにより定式化され、後に実用的なアルゴリズム（ PBFTなど）も発明されていた
  The Byzantine Generals Problem（1982年）

- これらの特性は**トラディショナルな分散システムでも実現できていた**
  （一般的に普及していたかどうかは別問題）

ブロックチェーンの新規性考察

- **不特定多数のノードが参加するネットワークでビザンチン障害耐性を実現したこと？**
  ⇒ これは新規性と言える
  ※ ただし、完全なビザンチン障害耐性は実現できていない
  （確率的に覆る可能性が 0にならないので、合意形成ができたとは言えない）

  従来のビザンチン障害耐性アルゴリズムは、全ノードのうち障害ノードが 3分の1未満であることが条件だった
  ビットコインのような不特定多数のノードが自由に参加できるシステムでは、悪意を持った人物が大量のノードを参加させ、システム全体の 3分の1以上のノードを支配してしまうことができる（**シビル攻撃**）
  ビットコインのアイデアは、Proof of Workと確率的合意アルゴリズムにより、**シビル攻撃に対して実用的な範囲で耐性を持つ**ことに成功した



ブロックチェーン vs.

トラディショナル分散システム

ブロックチェーンをめぐる対立・
トレードオフの論点を知る

障害耐性のトレードオフ

- **シビル攻撃耐性 vs. パフォーマンス**
  ビットコインブロックチェーンは、ビザンチン障害モデルにおけるシビル攻撃耐性を得た反面、実用的な合意形成までに相応の時間がかかってしまう（ 6承認で約1時間）

- 一般的に、障害耐性モデルのレベルを上げるほど、システムのパフォーマンスは落ちる

- **秒間あたりの処理可能トランザクション数の目安**:
  クラッシュ障害耐性システム ... 秒間 数万トランザクション程度（一般的なWebシステム）
  ビザンチン障害耐性システム ... 秒間 数千トランザクション程度（PBFT系DLTなど）
  ビザンチン障害＆シビル攻撃耐性 ... 秒間 数トランザクション程度（Bitcoin, Ethereumなど）

ブロックチェーンのビジネス活用化

広義のブロックチェーン

- ビットコインで実用性が証明されたブロックチェーン技術は、ビットコインのような電子通貨の送金だけでなく、さまざまな電子取引の場面にも応用可能であると考えられた
（国際金融取引の効率化、転職市場のリファレンスチェック等々）

- しかし、その多くは「データの改ざん耐性」や「検閲耐性」（≒ビザンチン障害耐性）を備えれば十分であり、シビル攻撃耐性までを考慮したシステムが要求されることは少なかった

- そこで、シビル攻撃耐性の特性を取り除き、「データの改ざん耐性」や「検閲耐性」を備えつつ、ビットコインブロックチェーンより高パフォーマンスを実現する**【広義のブロックチェーン】**が活用され始めた

ブロックチェーンの解釈を巡る派閥

サトシ・ナカモト派

- サトシ・ナカモトの発明したビットコインブロックチェーンの **新規性**に着目し、シビル攻撃耐性を備えたパブリックブロックチェーン（狭義のブロックチェーン）こそが本来のブロックチェーンであると考える派閥（**Web3 / パブリックブロックチェーン推進派**）

ランポート派

- ビットコインブロックチェーンの実証したシステムの有用性は認めつつ、その新規性は捨象して、現実の課題を解決するための **実用性**を重視した広義のブロックチェーンを活用しようとする派閥（**DLT / パーミッションドブロックチェーン推進派**）

あいまい派

- 狭義のブロックチェーンと広義のブロックチェーンの区別があいまいな層
- 理念としてはサトシ・ナカモト派に共感しつつ、やろうとしていることはランポート派に近いことが多い

各派閥間の断絶

- **ランポート派 vs. サトシ・ナカモト派＆あいまい派**
  ランポート派の視点からは、サトシ・ナカモト派の人とあいまい派の人は同一派閥に見える
  （発言していることが類似しているので）
  本来、狭義のブロックチェーンを活用するべきでない課題解決のために、むりやりブロックチェーンを使おうとしているように見える

- **サトシ・ナカモト派 vs. ランポート派＆あいまい派**
  サトシ・ナカモト派の視点からは、ランポート派の人とあいまい派の人は同一派閥に見える
  （やろうとしていることが類似しているので）
  ブロックチェーンの新規性を理解せず、レガシー（トラディショナル）な技術に捕らわれているように見える

ELI5: まとめ

ブロックチェーンの技術的意義

- **ビザンチン障害耐性を持った分散システム** は、ランポートらによって1980年代には存在していたが、障害ノードが3分の1未満であることなど **前提条件が厳しく、シビル攻撃耐性もなかった**
- ブロックチェーン技術により、不特定多数のノードが参加する分散システムで、ビザンチン障害や **シビル攻撃に実用的なレベルで対処できるようになった**（100%解決できた訳では無い）

ブロックチェーンの社会的影響

- 伝統的な分散システムでは、クラッシュ障害やタイミング障害などは考慮しても、ビザンチン障害までは考慮されないことが多かった
- ビットコインの登場により、分散システムにおける **ビザンチン障害耐性の必要性が社会的に認知** されるようになった（運営主体による顧客データの不正利用や、検閲などが社会問題化した）
- しかし、**シビル攻撃耐性まで求められるかという点については意見が分かれている**（Web3/パブリックブロックチェーン派 vs. DLT/パーミッションドブロックチェーン派）

Web3の羅針盤に代えて

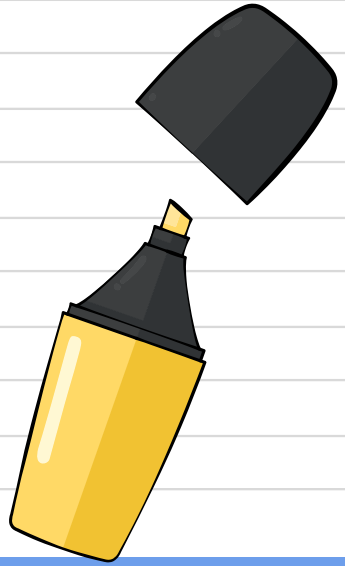
用語の意味を文脈から捉えよう

- ある用語（例：ブロックチェーン）の意味は、発言者や発言の文脈によって異なることが多い
- ある用語の意味を画一的にしか捉えていないと（例：「ブロックチェーンの意味は〇〇だ」と固定的に考えていると）、他の意味でその用語を使っている人とのコミュニケーションができなくなる

用語の意味を相手に押し付けない

- 相手の考えている用語の意味が自分の解釈と異なっていても、相手が間違っていると断定して解釈を変えさせようと説得する行為は無意味（解釈は多様な価値観に依存する）
- 多様な解釈があることを前提にして相手の主張を理解することに努め、その上で建設的な議論をしていくことが必要

Thanks!



質問・ご意見など

kasaki-nagato@dmm.com