

PLASMA ON PLASMA

次世代システム研究室

今日話すこと

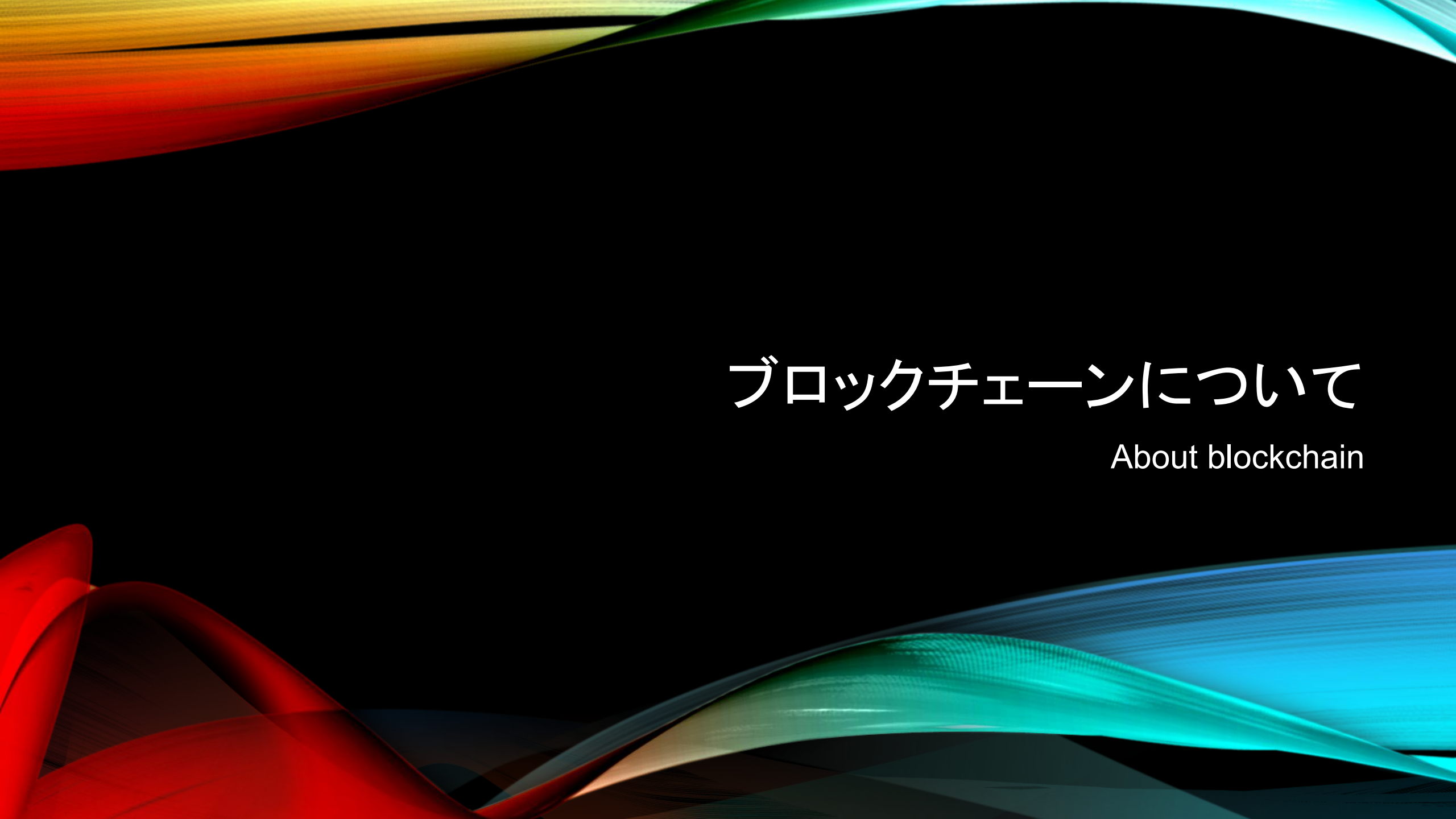
端的に言うと...

ブロックチェーンの上にブロックチェーンを乗せる話



もくじ

1. ブロックチェーンについて
2. サイドチェーンについて
3. コントラクトについて
4. Plasmaについて



ブロックチェーンについて

About blockchain

一言で

自分以外全員が悪意あるユーザーであっても
安全にお金(コイン)の所有権が送金できる分散システム

→ 誰も信用しなくていい(トラストレスな)仮想通貨が作れる

得意なこと

- 特定の人間が不正をできないようにする

従来のRDBMSでは管理者が自由に値を変更できる

- 名前、住所必要なしに、公開鍵だけ知っている相手に送金する

インターネットごしの人に送金するには、郵便書留などが必要だった

- 送金したことを他人に証明する

たとえば今までは収入印紙を発行していた(=発行元を信頼する必要がある)

苦手なこと

- 高速な送金

送金に数分～数十分かかるのが現状

- エコな送金

誰かが高速にハッシュ計算をする必要がある

- 手数料が安い送金

クレジットカードの加盟店ほどではないが、数円～十数円かかるのが現状

ブロックチェーンの革新


2011年：匿名の人物により初期のビットコインが開発される

2013年：ビットコインに汎用計算能力を持たせる研究が始まる

2015年：初期のEthereumが開発

2017年：Plasmaの概念が提唱される

2018年：世界初のPlasma実装が完成する



サイドチェーンについて

About sidechain

サイドチェーンとは

- 複数のブロックチェーンをまたいで、お金の送金する技術が研究される
- 既存のブロックチェーンを改良するために、後から機能を追加する研究がされる

→ 既存のブロックチェーンから、より高機能な別のブロックチェーンにお金を移管し、演算、送金、契約ができる技術が誕生する = サイドチェーン

サイド: 側、かたわらの意味で、メインのブロックチェーンの側に居ると言う表現



スマートコントラクトについて

About smart contract

スマートコントラクトについて

About smart contract

コントラクト: 直訳で契約

スマートコントラクトについて

ビットコインでは、お金の所有権を特定の秘密鍵を持つ人間に移動できる。しかし、お金の所有権の移動条件を、これ以外にも追加したい人たちが現れた。例えば...

- 「2人の賛成がないと使えないお金」
 - 所有権を2人で所有し、2人の秘密鍵がないと送金できないようにしたい
- 「特定のハッシュ値のsourceを知って居る人間」
 - 事前に公開鍵を知らなくても、特定のハッシュ値の答えを知って居る人間なら誰でも送れるようにしたい
- 「10日間立たないと送金できないお金」
 - 送金された後、次の送金に使われるのに10日経たないといけないお金を作りたい

スマートコントラクトについて

実は初期の段階のビットコインに似た技術は存在した。

Bitcoin script: コインに条件式を埋め込み、コインに自分の使われ方、振る舞いを指定できる

例:

- 署名を2つ引数にとり、両方とも正しいければ送金可能にする条件式
- 文字列を引数に取りハッシュ化して、事前に指定しておいた値と同じでなら送金可能な条件式
- 現在の時間を引数に取り、事前に指定した値+10日間より後なら送金可能な条件式

まさに、意志を持ったお金

もちろん、デフォルトは「署名と公開鍵をつ取り、署名が正しいかと事前に指定した公開鍵と同じか判定する条件式」

スマートコントラクトについて

- Bitcoin Scriptはただの条件式だった。
- より高機能に条件式を定義したい

→ Ethereumの誕生

- 条件分岐、ジャンプ、関数呼び出しができる汎用スタックマシン、つまり高機能なスマートコントラクトが提案された。
- 条件式を、コインではなくユーザー側に追加した
- 実はスマートコントラクトという名称が生まれたのも恐らくこの時

スマートコントラクトとは

- Ethereumで動くのはEVM(Ethereum Virtual Machine)と呼ばれる機械
- EVMは、x86やマイコンに似た、スタックポインタの概念、レジスタの概念が存在する
- コインではなく、アカウント側に条件式が付与されて居る、そのため...
 - 2人の署名がないとお金を送金しないアカウント
 - 特定のハッシュ計算の答えを言われないと送金しないアカウント
 - 一定時間経ってないとお金を送金しないアカウント
 - 100人に合計100コイン送金されたら特定の人間に全部送金するが、100コイン集まらないと全員に返却するようなアカウント

が実装できる。

こちらはまさに「意志を持ったアカウント」



PLASMAについて

About plasma

PLASMAについて

- ブロックチェーンが普及するにあたり、送金が遅いことが問題になった
- 問題点は二つ
 - 一度に送金できる人間の数が少ない
 - 送金要求をした後実際に送金が確定するまでの時間が長い
- これを解決したいが、やはり特定の人間を信用しなくてよい方法が望まれた

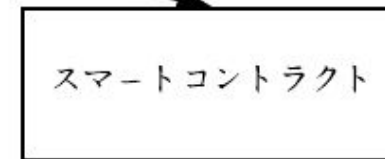
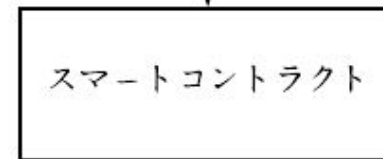
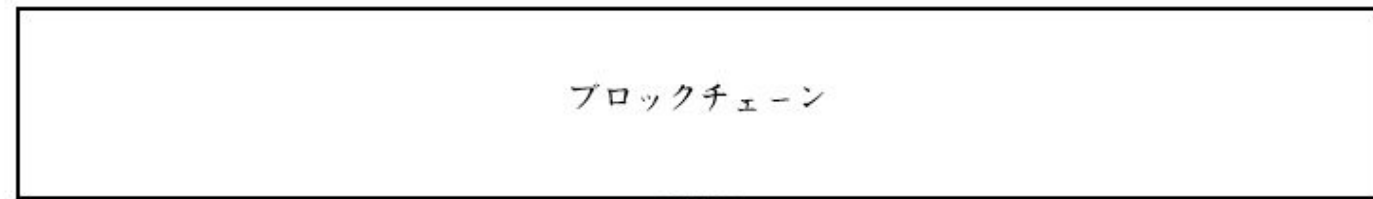
PLASMAについて

- スマートコントラクトが状態を保存でき(永続的なヒープ領域が実はある)、かつ汎用的な計算ができるのであれば、ブロックチェーンの上にブロックチェーン何百個もを再実装することが可能ではないのか
- そんなブロックチェーンがあれば、普段の送金はそこで行い、必要な時だけメインのブロックチェーンに戻って来ればいいのではないのか

→ 外部にブロックチェーンを作り、そのブロックチェーンのデータ構造をEthereumのスマートコントラクトに保管する技術が生まれた

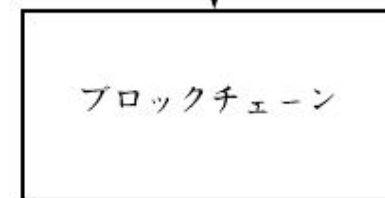
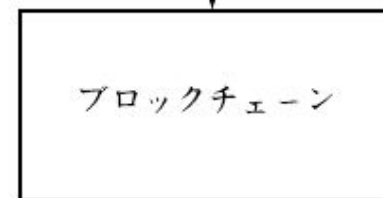
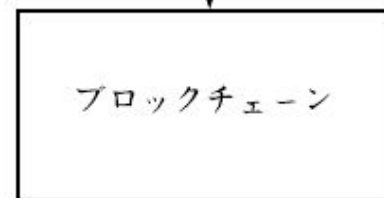
これがPlasmaと呼ばれる技術

メインのEthereumチェーンを上位チェーン、親チェーン、メインチェーンと呼ぶ



Ethereumブロックチェーン

外の世界



PLASMAについて

Plasmaのメリット

- 下位のブロックチェーンのデータをハッシュ値として上位に保存するので、つまりデータを圧縮していることになる。環境に優しい。
- 下位のブロックチェーンは中央集権的でも構わない。最終的に判断は最上位のスマートコントラクトが機械的に行うため「不正をしても認められない」ことになる。
- 中央集権的ということは、ハッシュ計算(マイニング)や検証作業をまたないため、下位ブロックチェーンを使用しているクライアントのハードウェア限界まで速度を引き上げられる

PLASMAについて

Plasmaのデメリット

- 構造上、下位ブロックチェーンの不正を上位ブロックチェーンで判断するのに7日間ほどかかる
 - →下位から上位にお金を戻す際に時間がかかる
- ユーザーは、下位ブロックチェーンと上位ブロックチェーン両方のデータを監視する必要がある
- ユーザーは下位ブロックチェーンのデータを全て持っていないといけない、容量の問題が発生

PLASMAについて

つまり...

- 一度に送金できる人間の数が少ない
- 送金要求をした後実際に送金が確定するまでの時間が長い

この2つの問題点のうち上の方が解決できるようになった

PLASMAについて

Depositについて

- Ethereumの外にサイドチェーンを作成する
- そのブロックチェーンのデータをEthereumのスマートコントラクトに保管する
- Ethereum内で、そのスマートコントラクト(意志のあるアカウント)に送金がされると、そのお金はスマートコントラクトの中にロックされる
- ロックされるのを確認すると、サイドチェーン上で同じ額のコインを新規作成する

PLASMAについて

Exitについて

- サイドチェーンのユーザーが、メインチェーンのスマートコントラクトにExitを依頼する
- スマートコントラクトは、サイドチェーン側にユーザーのコインがあることを確認すると、そのコインを使用不可にするようサイドチェーンに指令した上で、そのコインと同額のコインを自身のスマートコントラクトからアンロックする



今回作ったPLASMA ON PLASMAについて

About Plasma on Plasma

PLASMA ON PLASMA

- PlasmaブロックチェーンにさらにPlasmaブロックチェーンを実装する技術。
- 論文において提案、概念としては存在したが、(自分の観測範囲において)実装した人はどこにもいなかった
- 恐らく世界初？なのではないか

Plasma on Plasmaを使うメリット

- 手数料をより削減できる
- 速度をより引き上げられる

デメリット

- 監視すべきブロックチェーンが増える
- 対応しなければならない攻撃が増える

PLASMA ON PLASMA

具体的にやったこと

- 今回、PlasmaMVPと呼ばれる世界初のPlasma実装コードを元にした。
- Plasmaチェーンに、スマートコントラクト同等の機能をつけた
- Plasmaチェーンに、上位のチェーンがEthereumではなくPlasmaチェーンでも動作するように修正を加えた

これにより、Plasmaチェーンは下にも上にも、Plasmaチェーンと接続できるようになった



デモ

Demo

PLASMA ON PLASMA

今後の展望

- 「対応しなければならない攻撃が増える」について、攻撃例と、その対策を考えた。
 - オペレーターがブロックを含めない嫌がらせ
 - 解決策: もっとも上位のスマートコントラクトに、下位の全ブロックチェーンを構成する木を与え、検証してもらう。メインのEthereumのスマートコントラクトだけが唯一の司法機関であることを利用する。その後、skip exitを行う。
 - オペレーターが2重支払いをしようとした場合
 - 解決策: 上位のチェーンにChallengeを申告する。上位のチェーンも不正支払いに加担しようとした場合に、下位ブロックチェーンを構成する木を最上位であるEthereumのスマートコントラクトに申告し、状態遷移を拒否してもらう。

PLASMA ON PLASMA

今後の展望

- 未だ実装が完成していない部分について
 - 先ほどの攻撃への対策
 - Merkle proofの検証の実装
 - Challengeの実装
 - UTXOを再帰的な検証の実装
 - Spent transactionリストの実装
 - UTXO contract自体のexitを拒否する振る舞いの実装

インターンを通しての感想

よかったとこ

- 立地がいいので出社しやすかった
- コーヒー無料なのが最高
- MacBook Proをダメ元で希望してみたら貸与された

改善して欲しいとこ

- 他のインターン生との交流を用意してもらえると嬉しかった(ランチなど)
- インターンシップ応募する際に、実際のインターンシップの内容を知りたかったが、調べても見つからなかった。ネットで過去のインターン生の業務内容などが公開されていると嬉しい



おわり

ご静聴ありがとうございました。