APTOS

初学者でも基礎から丸わかり！

L1チェーンAptos徹底解説

Aptos Japan

はじめに

「Aptos」は、元Meta社のエンジニアが開発しているということで、メインネットローンチ前に関わらず大型の資金調達に成功していたりと、話題になることの多いL1ブロックチェーンです。

ブロックチェーン領域の情報収集をしていると「Aptos」という言葉は最近よく耳にするし、どんな特徴があるのか知りたいと感じている方もいらっしゃるのではないでしょうか？

一方で、学び始めたばかりの方にとっては、専門用語の多い記事やホワイトペーパーでは、理解を深めるのはハードルが高く、なかなか学習が進みませんよね…。

そこで、Aptosの特徴やメリットを、初学者の方向けになるべく分かりやすいようにまとめました。

本資料がAptosに関する理解を深める手助けになりましたら、とても嬉しいです。

INDEX

1. Aptosとは
2. なぜAptosが必要なのか
3. どのように実現するのか
4. Aptosに興味を持ってくださった方へ

1. Aptosとは

Aptosとは

元Meta社の「Diem」に携わったメンバーによって開発された
レイヤー1（L1）ブロックチェーン

Diemとは

Meta社によって開発されたブロックチェーン
※現在は売却済み

L1ブロックチェーンとは

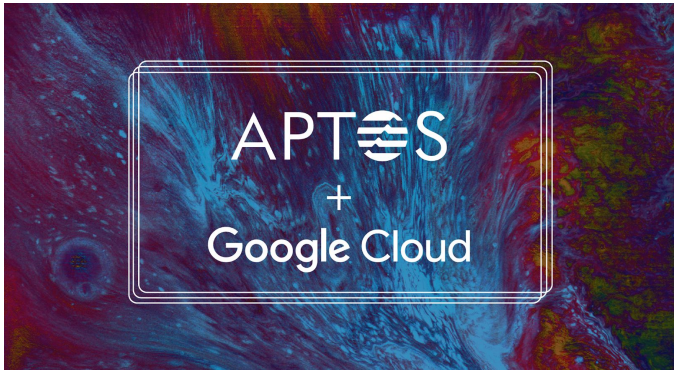
- L4：サービス
- L3：アプリケーション
- L2：拡張
- **L1：ブロックチェーン**
- L0：ネットワーク

基盤となるブロックチェーンのことで、
「プラットフォーム」のような役割

Aptosとは

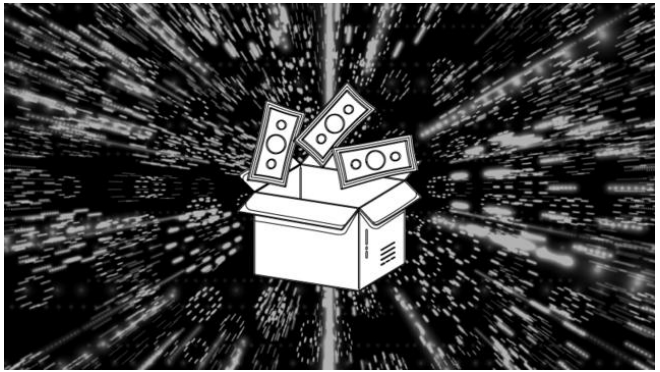
2022年9月現在、トークン発行前だがビッグテックとの提携や大型の資金調達に成功するなど注目を集めている

Googleとの提携



2022年4月、Google Cloudとの
パートナーシップ提携を発表

業界大手の投資機関から資金調達

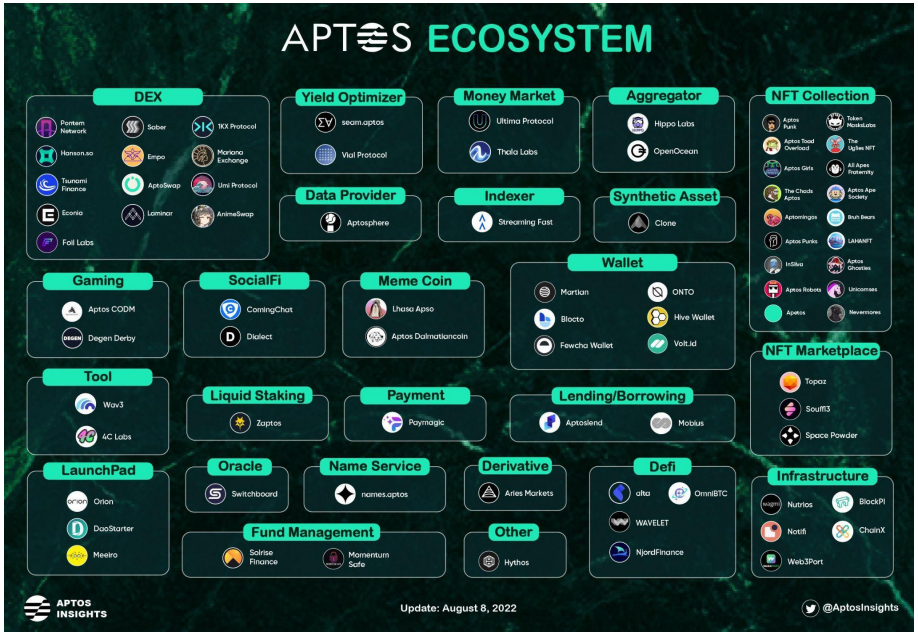


a16z、FTX、Jump Cryptoらから
1.5億ドルの資金調達に成功

Aptosとは

テストネットの段階だが、Aptosエコシステムで

すでに100以上のプロジェクトが構築されている



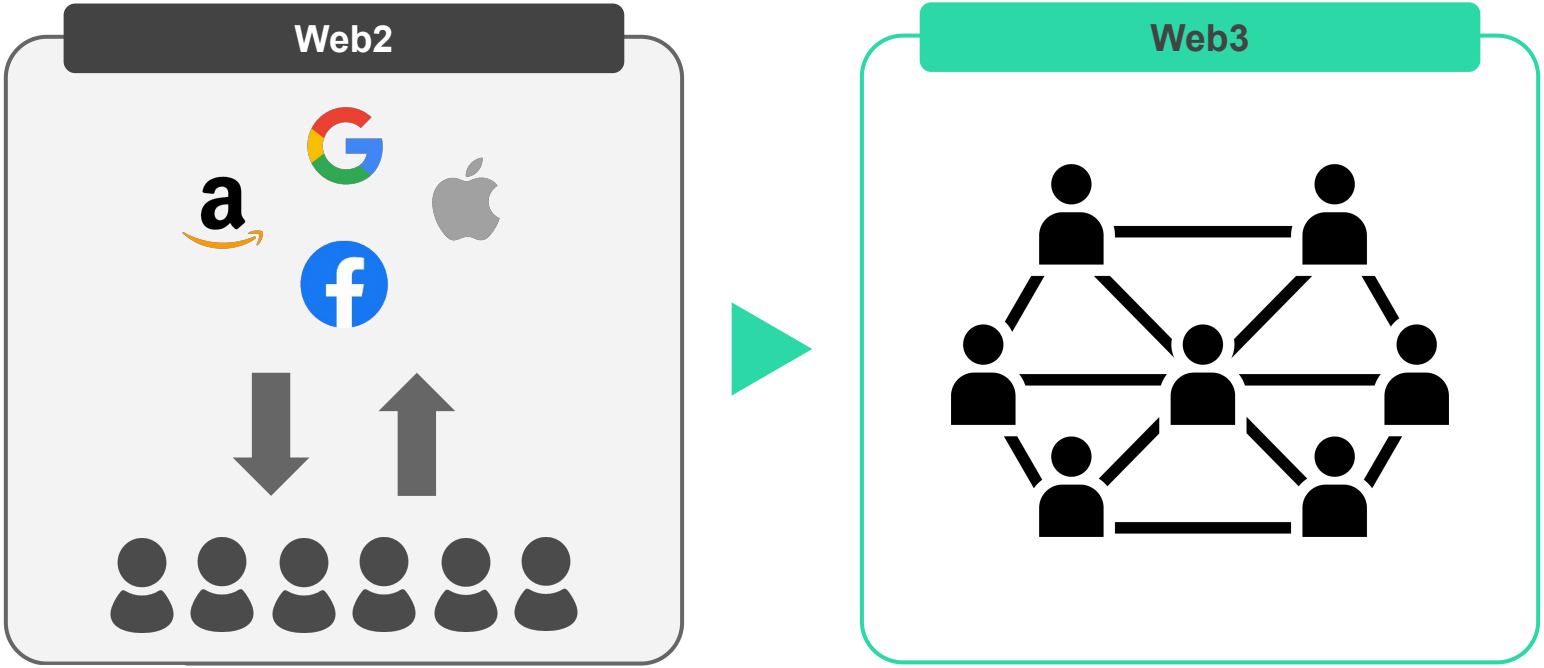
@AptosInsights

MoveMarketCapで全てのプロジェクトをチェックすることが可能です！

2. なぜAptosが必要なのか

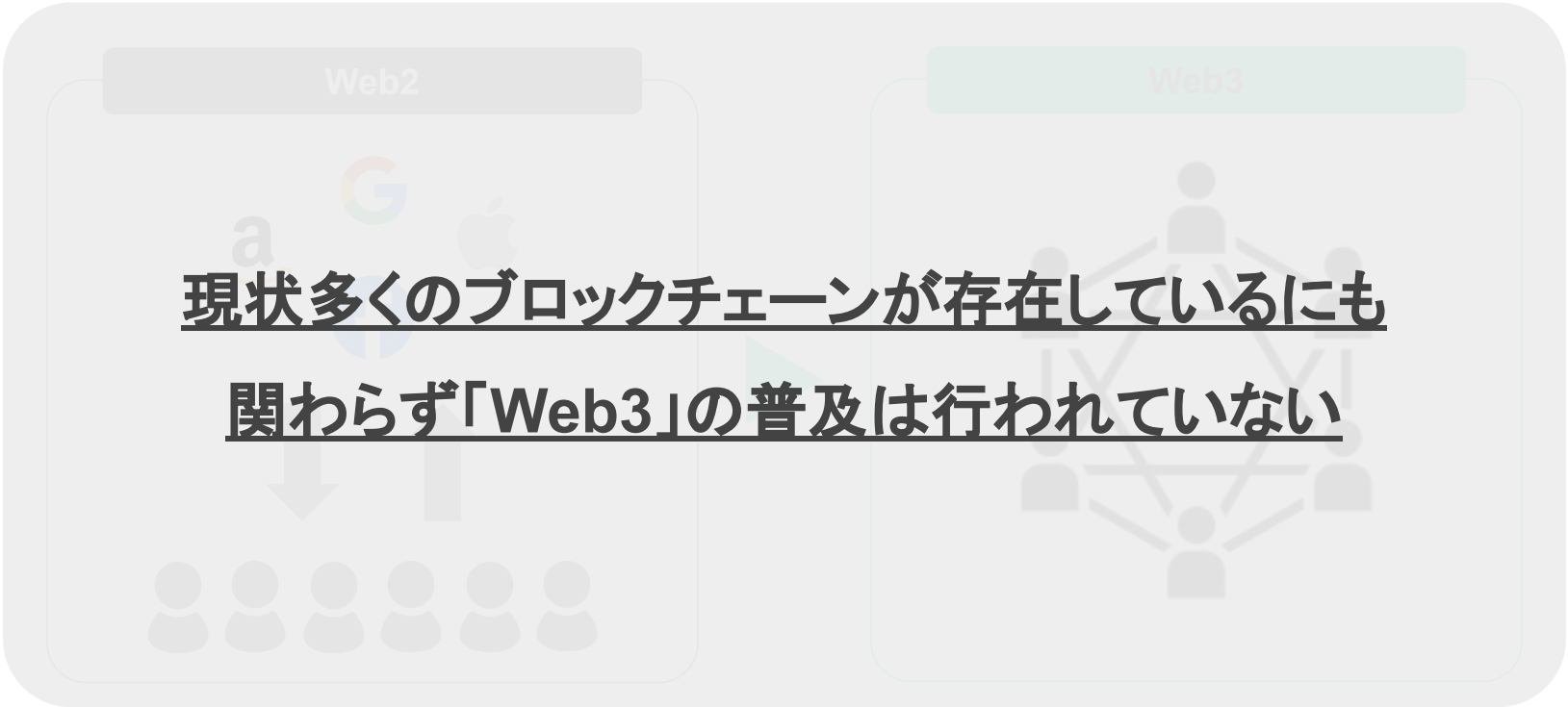
Web2からWeb3へ

中央集権性の強いWeb2の課題を解決するために、「Web3」に向けた取り組みが始まった。「ブロックチェーン」の登場により、中央集権的な存在がいなくても、ユーザーは互いに安全かつ確実なやりとりが技術的には可能に・・・。



Web2からWeb3へ

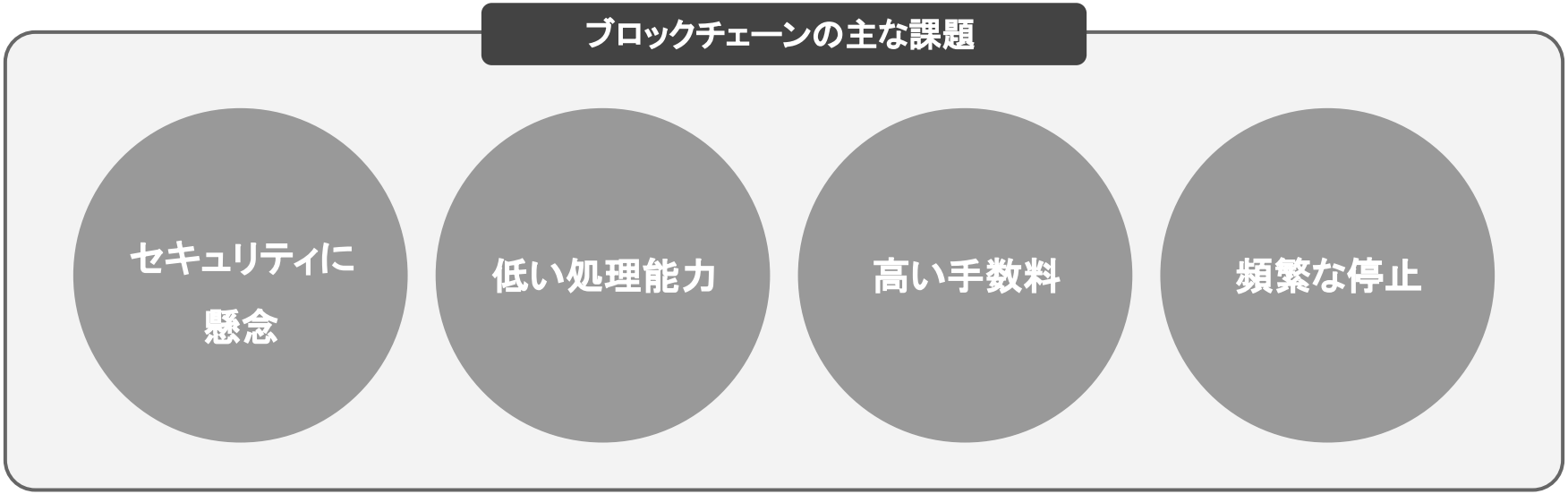
中央集権性の強いWeb2の課題を解決するために、**「Web3」**に向けた取り組みが始まった。**「ブロックチェーン」**の登場により、中央集権的な存在がいなくても、ユーザーは互いに安全かつ確実なやりとりが技術的には可能に・・・。



現状多くのブロックチェーンが存在しているにも関わらず「Web3」の普及は行われていない

Web3実現のためのブロックチェーンの課題

テクノロジーは発展し続けているが、**既存のブロックチェーンは信頼性が低く、ユーザーに高い取引手数料を課す**など様々な課題がある。

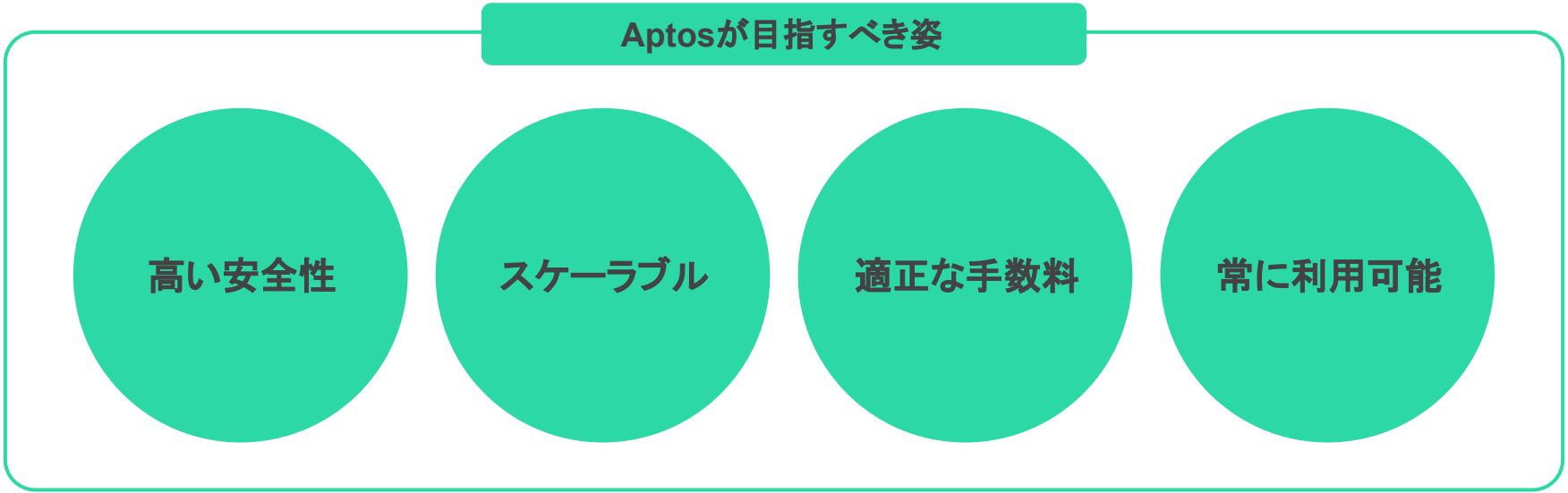


Web2のクラウドインフラがサービスを数十億人に届けることを可能にしたのに対し、

Web3のブロックチェーンは、まだ実現できていない

Aptosのビジョン

Aptosのビジョンは、**Web3に主流をもたらすことができるブロックチェーンを提供し、現実世界のユーザーの問題を解決する分散型アプリケーションのエコシステムを強化すること** である。



Aptosによって、Web2のクラウドインフラと同様に

ブロックチェーンが当たり前の存在となることを目指す

3. どのように実現するのか

どのように実現するのか

1. Move言語
2. Bullshark
3. 秘密鍵
4. アップグレード性

どのように実現するのか

1. Move言語
2. Bullshark
3. 秘密鍵
4. アップグレード性

Move言語とは

元々はDiemのために開発された

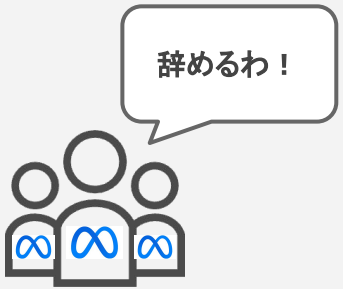
安全で信頼性の高い「Move言語」をAptosでも利用している

Meta社にてMoveで

Diemを作る

Diemは解散

メンバーはMetaを離れる



元メンバーにてMoveで

Aptosを作る

Move言語の特徴

「Rust（ラスト）」というプログラミング言語をベースに作られている

Rustの特徴①：所有者の概念による安全なメモリ管理

※メモリとは、一時的にデータを置いておく場所（イメージ例：机の上）

バグが起きやすい

従来

指定をしないとぐちゃぐちゃに

データの保管場所を指定しないと
どんどん机が散らかっていく

Rust

勝手に整理整頓されていく

データの保管場所を指定しなくても
自動的に整理整頓される

バグが起きにくい

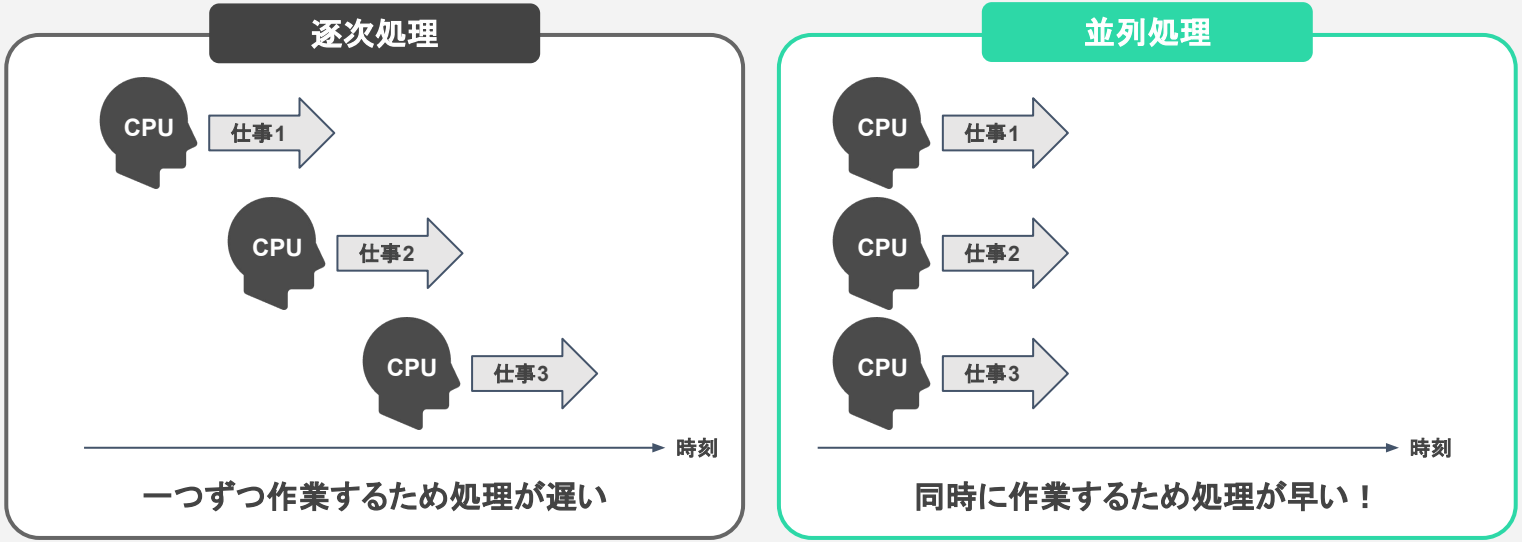
参考：https://azby.fmworld.net/usage/closeup/20131023/page2.html

Move言語の特徴

「Rust（ラスト）」というプログラミング言語をベースに作られている

Rustの特徴②：マルチスレッドを利用し、複数のタスクを並列処理

※マルチスレッドとは、複数のCPUがあることを指す（CPUのイメージ例：頭脳）



Move言語の特徴

「リソース指向のプログラミング言語」である

リソース指向の2つの特徴

デジタル資産に向いている

例：日本円

コピー・削除不可、所有権の転送のみ可能

バグが少ない・開発速度が早い

他の言語に比べてコード量が少なくすむ

Move言語の特徴（まとめ）

「セキュリティ」と「スケーラビリティ」両方に対応しているため

ブロックチェーンのプログラミングに最適である

セキュリティ

コードの脆弱性や

悪意ある攻撃者に対する耐性

＋

スケーラビリティ

ネットワークの規模が拡大しても

適切に機能する能力

引用：https://coinpost.jp/?p=371960

どのように実現するのか

1 Move言語

2 Bullshark

3 秘密鍵

4 アップグレード性

Bullshark（ブルシャーク）とは

Aptosのコンセンサスアルゴリズムは

「Bullshark」や「Aptos BFT」と呼ばれている

コンセンサスアルゴリズムとは

ブロックチェーンの取引を、承認・記録するためのルール

ルールなし

意見がバラバラ・・・

ルールあり

意見が一致！

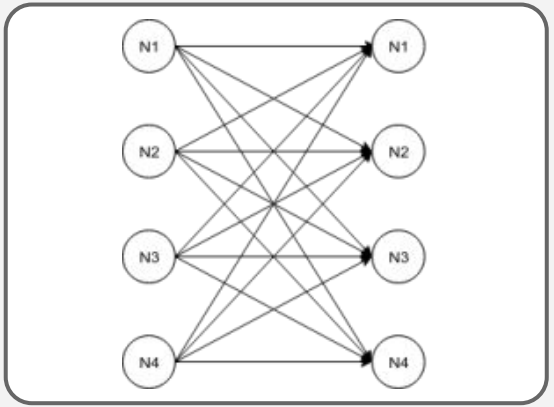
条件を満たせば誰でも承認者・記録者になることが可能のためルールを制定しておく必要がある

Bullshark（ブルシャーク）とは

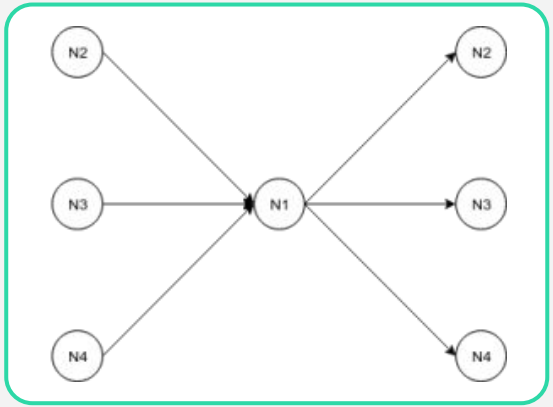
Bullsharkは「HotStuff」というコンセンサスアルゴリズムが
ベースとなっている

HotStuffの仕組み

従来：全ノードが互いにコミュニケーションを取る



HotStuff：選出されたリーダーがノード間の連携を司る



ノード間のやりとりが減り、コンセンサスにかかる時間が短縮される

※ノード：合意形成する人

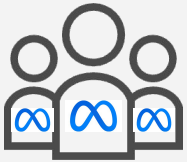
Bullshark（ブルシャーク）とは

「HotStuff」をベースに、現状の課題である**高速でスケーラブルかつ**

安全性の高いコンセンサスアルゴリズムを実現するために改良を重ねている

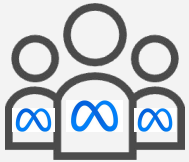
コンセンサスアルゴリズムに
HotStuffを採用
名前を「Libra BFT」に！

Libra BFT



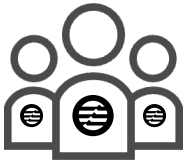
LibraからDiemに改名
Diem BFTとして改良を重ねる

Diem BFT



現在はAptos BFTとして
更なる改良を加えている

Aptos BFT



Bullsharkの何が良いのか

3つのコンセンサスアルゴリズムで比較を行った

Aptos独自の
コンセンサスアルゴリズム

Bullshark

Sui独自の
コンセンサスアルゴリズム

Tusk

一般的な
コンセンサスアルゴリズム

Hotstuff

予備知識：スループットとレイテンシ

スループット（TPS）：時間あたりどれくらいの取引を処理できるか

レイテンシ（遅延時間）：データベースに結果が反映されるまでの時間

スループット（TPS）

例：道路の広さ

道路が広い方がより多くの車が通ることが可能

（より多くの取引を処理することが可能）

レイテンシ（遅延時間）

例：目的地まで到達する時間

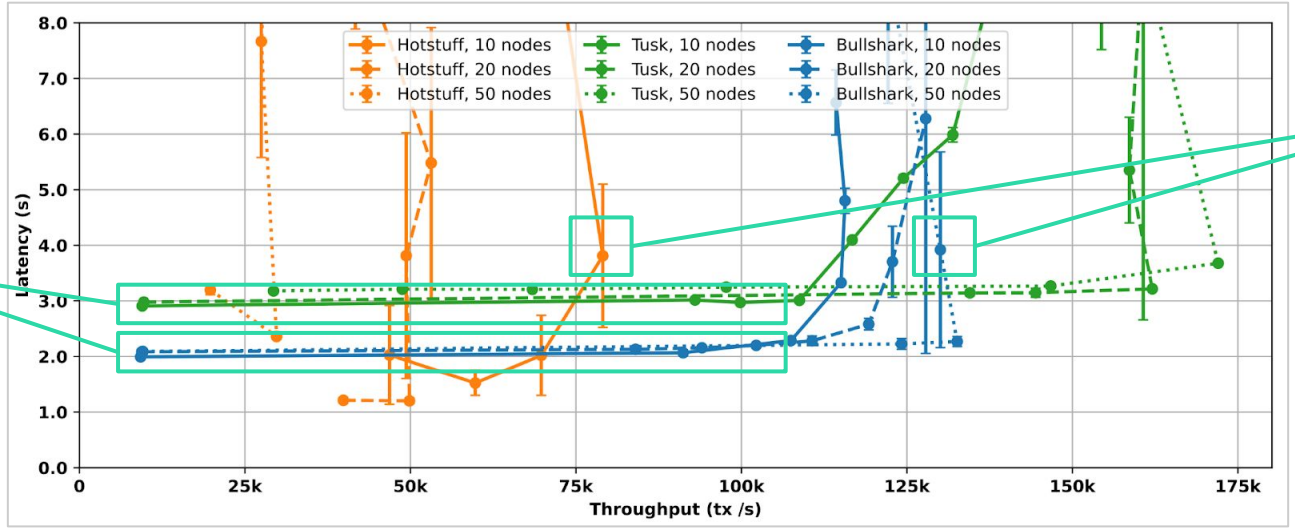
目的地にどのくらいの時間で到達できるか

（どのくらいの時間でデータベースが反映されるか）

Bullsharkの何が良いのか

BullsharkのHotStuffの**約2倍TPSが高く**

Tuskよりも**低遅延**を実現



Bullsharkの方が
レイテンシが低い

Bullsharkの方が
約2倍TPSが高い

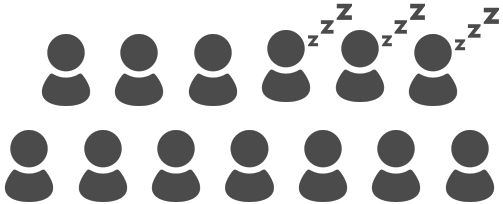
引用：https://arxiv.org/pdf/2201.05677.pdf

Bullsharkの何が良いのか

Hotstuffの弱点は「耐障害性の低さ」である

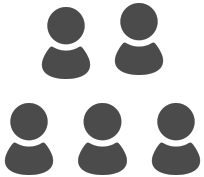
Hotstuffは、ノードが増えても減ってもデメリットがある

ノードが増える



合意形成する人が増えると休む人も増える
→故障率が上がってレイテンシが高くなる

ノードが減る



合意形成する人が少ない
→分散性が低くなり中央集権化する

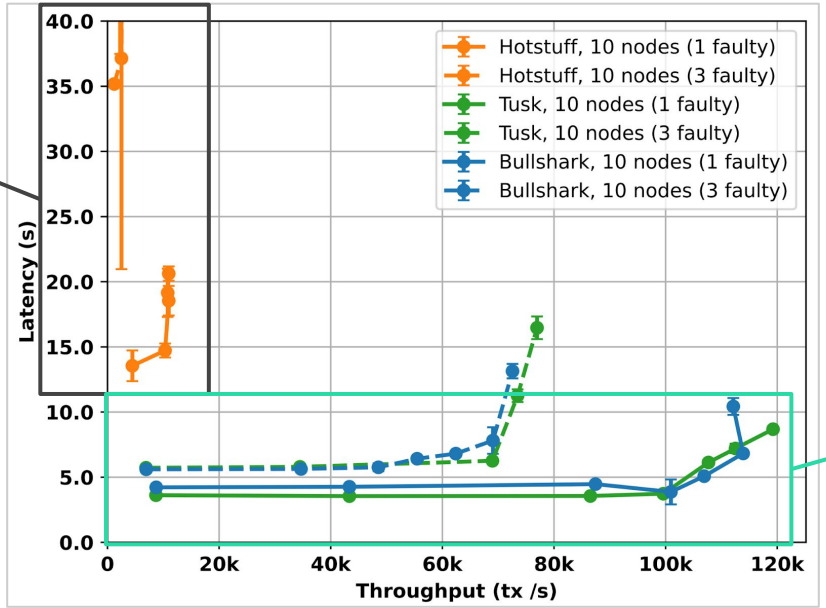
※ノード：合意形成する人

Bullsharkの何が良いのか

BullsharkやTuskは、

Hotstuffの弱点である**「耐障害性の低さ」**を克服

Houstufはレイテンシが高いため
遅延が大きい



Bullshark・Tuskは
TPSが高く、レイテンシが低いため
遅延が起きにくい

引用：https://arxiv.org/pdf/2201.05677.pdf

どのように実現するのか

1 Move言語

2 Bullshark

3 秘密鍵

4 アップグレード性

ブロックチェーンの秘密鍵と公開鍵

暗号資産を購入すると「公開鍵」と「秘密鍵」が発行される

それぞれメールアドレスとパスワードのような関係である

公開鍵

例：メールアドレス

他の人と共有

秘密鍵

例：パスワード

誰とも共有しない

自分だけが秘密鍵にアクセスできる限り、安全に管理でき

インターネットに接続していれば、世界中のどこにいても管理が可能

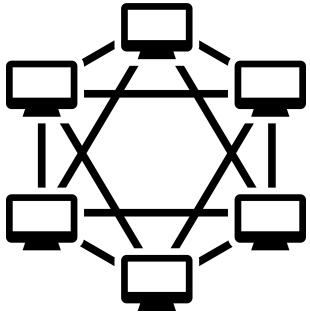
秘密鍵をなくすと・・・？

秘密鍵を紛失すると**再発行はできず**、その暗号資産は使用できなくなる

Web2

- 中央で管理
- パスワードの再発行可能

Web3



- 分散型のため中央での管理なし
- パスワードの再発行不可

ブロックチェーンは、銀行のように中央で管理するものはいない

秘密鍵の盗難や紛失などのリスクを自分で管理する必要がある

秘密鍵の盗難防止と紛失による秘密鍵の回復

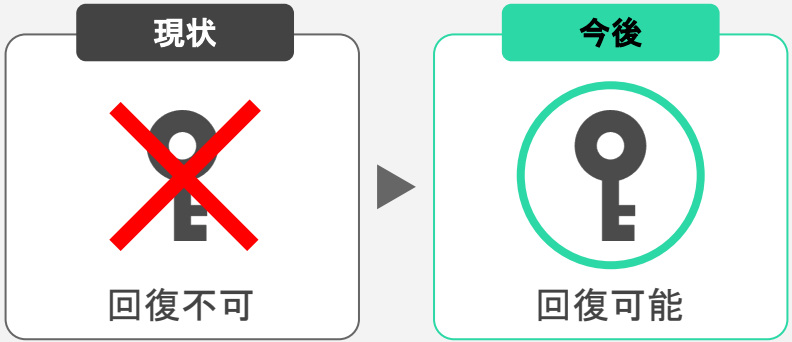
Aptosは、秘密鍵の盗難防止のための**セキュリティを強化**しており

紛失による**秘密鍵回復に関する開発**にも取り組んでいる

秘密鍵の盗難防止

ローテーション

秘密鍵の回復



どのように実現するのか

1 Move言語

2 Bullshark

3 秘密鍵

4 アップグレード性

従来のブロックチェーンのアップグレード性

理想

進化するWeb3のニーズに対して
ブロックチェーンを改善

現実

ブロックチェーンの多くは
ローンチ後の大幅な改善が難しい

大幅なアップグレードを試みたブロックチェーンの中には、
何時間ものシステム停止や偶発的な仕様変更が起きてしまったことも・・・

従来のブロックチェーンのアップグレード性

「アップグレード性の低さ」が

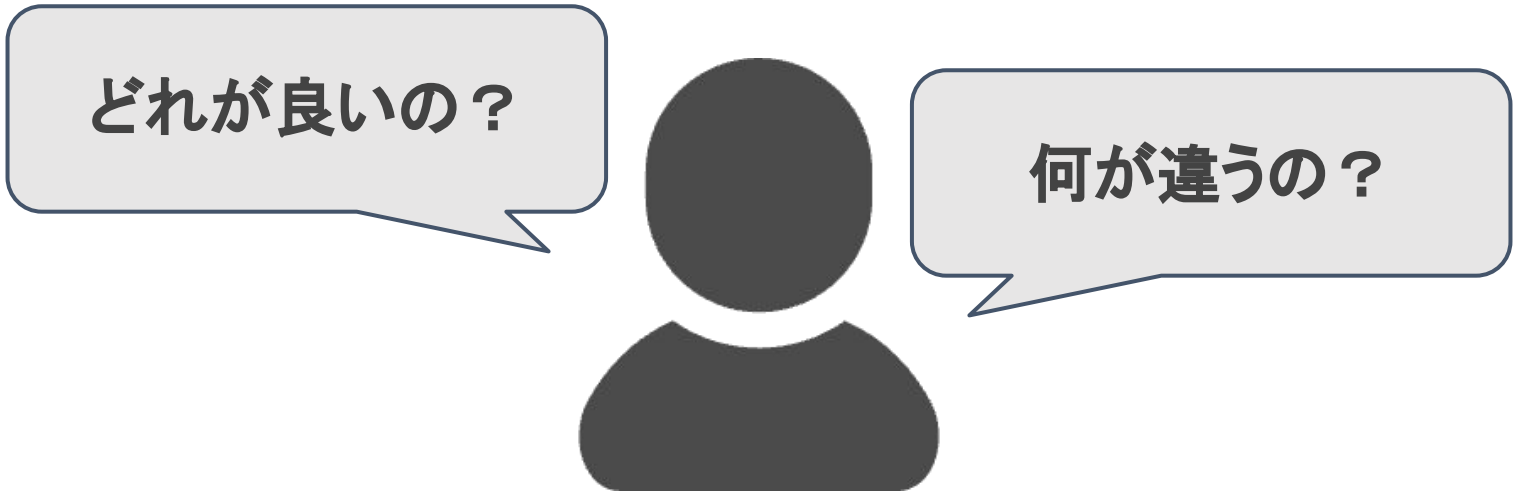
新しいブロックチェーンが乱立される

要因の一つだと考えている

新しいブロックチェーンが乱立すると？

ユーザーは、利用用途に最適なものを見極めるために

多くのブロックチェーンに精通する必要がありユーザー体験的に良くない



<u>ブロックチェーンの普及が減速してしまう可能性がある</u>

Aptosのアップグレード環境

従来のブロックチェーン

ブロックチェーンの多くは

ローンチ後の大幅な改善が難しい

Aptos

進化するWeb3のニーズに対して

ブロックチェーンを改善可能に

容易にアップグレードできるように設計・構築し、

ダウンタイムなしに安全で信頼性の高い環境を開発中

今後の計画

2022 Q1	デベロッパー向けテストネットの立ち上げ
2022 Q2	インセンティブ付きテストネットの立ち上げ
2022 Q3	メインネット立ち上げ ← 現在はココ！
2022 Q4 ～ 2023 Q1	重要な機能を備えたメジャーリリースをデプロイ

4. Aptosに興味を持ってくださった方へ

Aptos Japan紹介

「開発者による開発者のためのコミュニティ作り」を理念として有志により発足。
各自コミュニティの成長のために自律的に行動する、小さな DAOのような形式を取っている。

現在のメンバー

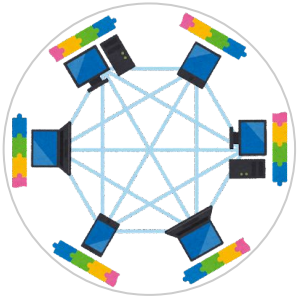
コミュニティマネージャー

@Takeshi_TGAL

開発者

@0xHanasaka

ノードオペレーター



@qyeah33

マーケター

@ogurin__

今後も開発やデザイン、記事の作成が得意な方などと一緒に

取り組んでいければ嬉しいです！

Aptos Japanの取り組み

「Aptosの日本での認知拡大」を目的に、様々な取り組みを行っている

日本語版Twitter	日本語版Medium運営	日本独自のDiscord運営
@aptos_japan	https://medium.com/aptoslabs-japan	https://discord.com/invite/SBaUHhHYVG

イベント開催	Aptos公式への積極的な提案	Aptos Koreaとの連携
		Aptos Japan / Aptos Korea

将来的には、アジア地域でのAptosハッカソンの開催などの

取り組みへと発展させていく予定です！

Aptos Japanの取り組みに参加する

Aptosの日本での普及のために

一緒に日本コミュニティを盛り上げていきましょう！

Discordへの参加

Discord

https://discord.com/invite/SBaUHhHYVG

イベントへの参加

特に開発やデザイン、記事の作成が得意な方は

Aptos Japanの運営にも携わっていただきたいです！

Aptosの情報をキャッチアップ

Aptosに関する最新情報はAptos Japan Twitterにて発信中

ぜひフォローをお願いします！

おわりに

本資料を最後まで読み進めていただき誠にありがとうございます。初学者の方にとってお役に立てるような内容だったでしょうか？

もし不明点や疑問点等ございましたら、Aptos Japan TwitterのDMにて、ご連絡をお願いいたします。

また、本資料に記載ミスや誤った情報等ございましたら、併せてご連絡いただけますと幸いです。

引き続き、Aptos Japanをよろしくお願いいたします。

＜Aptos Japan＞

Twitter：https://twitter.com/aptos_japan

Medium：https://medium.com/aptoslabs-japan

Discord：https://discord.com/invite/aptoslabs