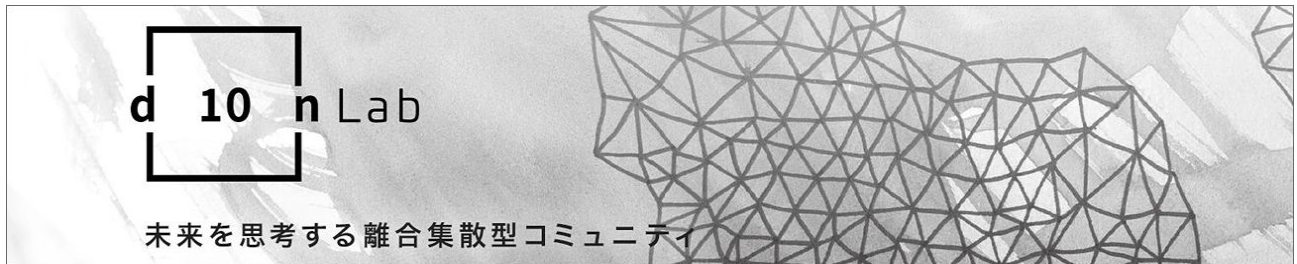


Ethereum2.0 コンプリートガイド (2019年7月版)

EthereumのPoSへの移行はどのように行われるか

- ◆本レポートは、暗号通貨/ブロックチェーンの情報プロバイダ「d10n Lab」が提供しています。
d10n Labにご入会頂くと過去の800本以上のレポートやコラムが全て閲覧できる他、不定期で行われるブロックチェーン関係イベントなどにアクセスできます。
詳細・ご入会はこちらから <https://d10nlab.com/>



目次

- [前提](#)
- [これまでのEthereumの開発と現在地点について](#)
- [Ethereumの各アップデートのプロセスについての詳細手順](#)
- [Ethereum2.0のアーキテクチャとデザインゴール](#)
- [Ethereum2.0を分解した各フェーズ。および明らかになっているスケジュール](#)
- [フェーズ0 : Beacon Chainのローンチ、Casper FFG](#)
- [フェーズ1 : Sharding、Cross-Link](#)
- [フェーズ2 : eWASM](#)
- [Ethereum 1.xのロードマップ](#)
- [レイヤー2の開発 \(Plasma、State channel、サイドチェーンetc\)](#)
- [PoSのステーキングに参加してバリデータになるには](#)
- [PoS参加に対するETHの報酬、インフレーションレート](#)
- [バリデータへのペナルティ・スラッシュ](#)
- [フェーズ2まで到達したEthereum2.0はどのくらいのトランザクション性能があるのか？](#)
- [Ethereum2.0の主要クライアント](#)
- [Ethereum2.0の開発資金は誰が拠出するのか？](#)
- [不明点や懸念点](#)
- [総論](#)
- [参考リンク](#)

■前提

本レポートでは、EthereumのPoSの移行、**Ethereum2.0 (Serenity)** について解説をします。

EthereumのPoSの移行は長い間議論されているトピックですが、いよいよその移行の第一段階が始まるタイミングに差し迫っています。

Ethereum2.0についてはd10n Labの過去のレポートでも取り上げてはいますが、やや情報が古くなっている部分もあるので、本レポートで2019年7月時点での全体像を改めて取り上げることとします。

■これまでのEthereumの開発と現在地点について

前提知識としてEthereumのこれまでの開発や、開発プロセスについて触れます。

Ethereumは、ホワイトペーパーリリース時点から4段階のフェーズに分けて開発されることが発表されていました。

その後、実際にはその4段階のフェーズは更に細分化されてリリースされています。

- Frontier (2015/07)
- Homestead (2016/03)
- Metropolis - phase 1: Byzantium (2017/10)
- Metropolis - phase 2: Constantinople (2019/02)
- Serenity: Ethereum2.0 (2020-2024?)

さらにMetropolisとSerenityの間には、Ethereum1.xと呼ばれるIstanbul (2019/10) などのアップデートが予定されています。

Ethereumはこれらの大型アップデートが行われる度に双方互換性のないクライアント、つまりハードフォークを伴うアップデートを行いネットワークの開発をしています。

この際、ハードフォークによって互換性のないクライアント、つまり古いチェーンはアップデートの度に破棄されています。

PoSの移行は、Serenityのアップデートに含まれ、PoS導入はホワイトペーパーリリース時点から予定されていたロードマップです。

SerenityとEthereum2.0、Eth2.0などの単語は明確な定義はありませんが、それぞれほとんど同一のものを指すと捉えて良いでしょう。

後述しますが、Serenity: Ethereum2.0を（2020-2024?）と表記したように数年の長い期間をかけて行われます。

ゴールはPoSへの完全移行や、eWASMという新しいバーチャルマシンの実装、シャーディングの実装です。（シャーディングとは、詳しくは本レポート内[■フェーズ1: Sharding、Cross-Link](#)にて説明）

現時点のEthereumの数千倍の処理能力を目指します。

■Ethereumの各アップデートのプロセスについての詳細手順

また、本題に入る前に、Ethereumのネットワークのアップデートがある際にどのような手順でソフトウェアがリリースをされるかを解説します。

ブロックチェーンはP2Pのネットワークなので、互換性のあるクライアントが通信しあって形成されます。

このクライアントの実装パターン（Ethereumであればgo-ethereum、Parityなど）がいくつかありますが、クライアントソフトウェアのリリース自体まで到達すること全体を指してブロックチェーンの開発と呼べるでしょう。

これらのクライアントはそれぞれ別の開発チームが行っています。

なお蛇足ですが、全てのクライアントはオープンソースであり、収益が生まないので、それぞれの開発チームはEthereum Foundationからグラントを受け取っているか、別の営利事業を持っているかなどをしている場合が多いです。

このクライアントリリースまで到達するには大まかに下記のような道のりを経ます。

1. 将来のEthereumの実装について日常的に議論される。（ethresearchや開発者イベントなどの場が中心）
2. それらの議論を元に、分解した機能や規格ごとにEIPという形式でGitHubのEIPレポジトリ（参照:<https://github.com/ethereum/EIP>）にプルリクエストが行われる。プルリクエストは誰でも可能で、EIPステータスはDraft（提案）、Accepted（承認）、Final（実装済）の段階を経て実装まで向かう。Deferredは現時点では実装しないEIPで将来的に再考慮されるかもしれないEIPステータスである。
3. 次の大型アップデート（ハードフォーク）にどのようなEIPが実装されるかなどの期限を決めて、アップデートスペックの決定をする。これをスペックのフリーズと呼ぶ。
4. EIPによって決定されたスペックを元に各クライアントのGitHubのレポジトリに機能が追加する開発が行われる。それぞれのクライアントにコアコントリビュータは存在するが、オープンソースなので誰でもプルリクエストは可能である。
5. クライアントのテストネットをリリース。
6. 通常、数ヶ月のテストネットの運用期間で安全性の確認を経て、メインネットのソフトウェアをリリース。
7. 日時を決めハードフォークをスケジュールし、この時にマイナーやフルノードオペレータ、取引所は新しくリリースされたクライアントにアップデートを行う。（アップデートをしなければ互換性のない古いクライアントで動かしているノードはネットワークと通信できなくなる。）
8. 無事にネットワークのアップデート完了。EIPに含まれていた新機能などがメインネットで使えるようになる。

このようにしてEthereumのネットワークはアップデートを繰り返します。

Ethereum2.0のリリースも大まかにこのような手順を踏襲します。

しかしながら、後述しますがEthereum2.0は全く新しいブロックチェーンであり、ハードフォークを必要としません。

いずれにしても議論→スペックの決定→各クライアントの開発→リリースという流れは変わらず、Ethereum 2.0もこれに沿って開発されます。

■Ethereum2.0のアーキテクチャとデザインゴール

Ethereum2.0のアーキテクチャの最も重要な点として2.0は、これまでのEthereumと異なるブロックチェーンとしてローンチします。

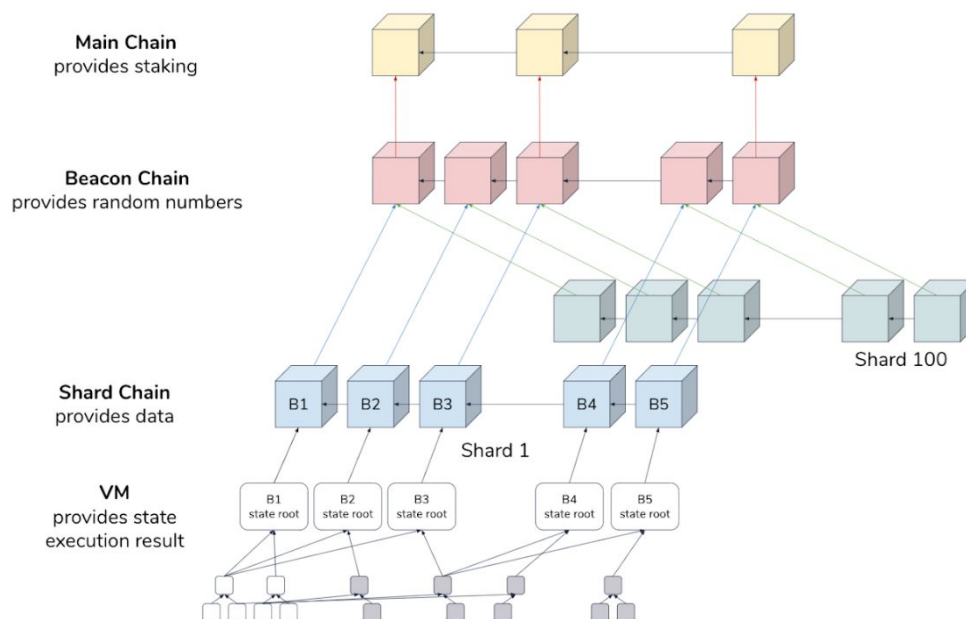
その後しばらく（少なくとも5年以上）現在のEthereumとEthereum2.0は並存をします。

新しい2.0チェーンは**Beacon Chain**と呼ばれます。

さらにBeacon Chainから1024のシャードチェーンを実装して、並列処理を行います。

現在のPoWのEthereumは最終的にはなくなりますが、今後もかなり長い期間アンカリングレイヤーとして機能します。

このアーキテクチャを図にすると下記のようになります。



参照：

https://docs.google.com/presentation/d/1G5UZdEL71XAkU5B2v-TC3ImGaRlu2P6QSeF8m3wg6MU/edit?fbclid=IwAR02snrGkuhD1w_vXohCA8UOkMexlrX-7UoUjCu297IY6ePSDAQZ1B5-4bM#slide=id.g3c326bb661_0_58

このアーキテクチャを目指して3-5年程度のアップデートが行われます。

しかし後述しますが、一度にアップデートを行うのではなく、フェーズを細分化して行い、その最初のフェーズは2020年の頭です。

ブロックチェーンが2つになるため、新しいブロックチェーンであるBeacon Chainのクライアントが必要です。

Beacon Chainクライアントは現在複数のチームによって開発されています。

また、Ethereum2.0のデザインは下記を重視して行われます。

- **Decentralization（分散性）**

ノートPCでもバリデータとしてネットワークに参加でき、ノードが分散している状態をつくる

- **Resilience（弾性）**

多くのノードがオフラインになっても稼働し続けるネットワーク

- **Security（セキュリティ）**

多くのバリデータが参加してセキュリティの高いネットワーク

- **Simplicity（シンプル）**

多少の効率性を失ってもシンプルさを重視した設計を優先する

（バグが複雑な設計にこそ発生し、シンプルでない設計はアップデートの自由を損ないやすいため）

- **Longevity（持続性）**

量子耐性、コンポーネントの可換性による持続性

また、同時にこれまでのEthereumチェーンもしばらく残り、その間にアップデートはされます。

この従来のチェーンのEthereumを **Ethereum 1.x** と呼びます。

■Ethereum2.0を分解した各フェーズ。および明らかになっているスケジュール

上述したようにEthereum2.0は複数のフェーズに分けてローンチされます。

大まかには下記のようになります。

- フェーズ0**： 新しいブロックチェーンであるBeacon Chainのローンチ
PoS機能のCasper FFGの実装（2020年1月）
- フェーズ1**： Shardingの実装、Beacon Chainとそれぞれのシャードを繋ぐための
Cross-Linkの実装（2020年内）
- フェーズ2**： eWASMの実装、コントラクトが扱えるようになる
（2020年-2021年）
- ==
- フェーズ3**： ライトクライアントの実装
- フェーズ4**： シャード間のトランザクション
- フェーズ5**： メインチェーンとの結合（Casper CBC “Correct-by-construction”）
- フェーズ6**： さらに複数の指数関数的なシャーディングの実装



参照 : <https://media.consensys.net/the-roadmap-to-serenity-bc25d5807268>

執筆している2019年7月時点ではフェーズ0の実装開発と、フェーズ1~2のスペックの議論がEthereum2.0の開発コミュニティでの主要トピックとなっています。

本レポートでもそれらの点は詳細を解説しますが、フェーズ3以降について深く取り扱いません。

フェーズ3のローンチは少なくとも2021年以降になる予定で、そこに含まれる機能も未だ流動的で、確定していないことが多いからです。

いずれにしても現在、コミュニティはBeacon Chainのローンチと、その後のフェーズ2を大きなマイルストーンとして動いています。

フェーズ0は、既に開発スペックがフリーズされ、2020年の1月3日にローンチが予定されています。

フェーズ1のスペックは2019年Q3にフリーズされ、2020年内にローンチが予定されています。(参照 :

https://www.reddit.com/r/ethereum/comments/cdg8v6/ama_we_are_the_eth_20_research_team_pt_2/etv8ios/)

本レポートでは、フェーズ0-2について解説します。

■フェーズ0 : Beacon Chainのローンチ、Casper FFG

フェーズ0は、Beacon Chainのローンチ、Casper FFGの実装を含みます。また、Beacon Chainのローンチにあたり新しいETHが生まれます。

フェーズ0に含まれる機能の詳細は以下の通りです。

1. Beacon Chain

Beacon Chainはフェーズ0以降に実装される1024のシャードチェーンをマネジメントするEthereum2.0のコアです。

トランザクション情報や、スマートコントラクトの実行、Stateの更新はシャードチェーンで行われますが、Beacon Chainはそのシャードチェーンにファイナリティを与えます。

シャードチェーンはフェーズ1ですが、先にBeacon Chainだけフェーズ0でローンチをする形になります。

2. Casper FFG (Friendly Finality Gadget)

CasperはEthereumで使用されるPoSの総称です。

Casper FFG (Friendly Finality Gadget) と Casper CBC (Correct-by-Construction) と呼ばれるものがありますが、Casper FFGが先に実装される仕様です。

Casper FFGはPoWとPoSのハイブリッドです。

ブロックの生成は引き続きEthereum 1.xのチェーンによってPoWで行われますが、Beacon Chain上のPoSによって選出されるバリデータによって、5ブロックごとにチェックポイントを設けて、ファイナリティを与えます。

Bitcoinなどのブロックチェーンでは確率的ファイナリティでありファイナリティの確定がありませんが、Casper FFGを実装したEthereumでは2/3以上のバリデータが正しいブロックであるとしたブロックは以後覆ることはありません。

3. Beacon Chain上のETH (ETH2、bETH)

Beacon Chain上のローンチに際して、Beacon Chain上に新しいETHが誕生します。これをETH2、またはbETHと仮称します。

これまでのEthereumチェーンのETHを、これまでのEthereumブロックチェーン上にデプロイするコントラクトアドレスであるregistration contractにデポジットします。

Beacon Chainはこのコントラクトを監視し、ここにデポジットをしたアカウントはBeacon Chain上のETH、つまりETH2アセットに変換できます。

Beacon Chainのバリデータになる際は、ETH2トークンが32必要になります。

Beacon Chain上でPoSの実装は行われており、バリデータはブロック報酬をBeacon Chain上でETH2トークンを受け取ります。

* フェーズ0はBeacon Chainがローンチされるだけであり、この新しいチェーン上にはバーチャルマシンなどが存在しなく、スマートコントラクトは実行できません。つまりフェーズ0がローンチしても、フェーズ2に到達するまでの期間、トランザクションやコントラクトの実行は、Ethereum 1.xチェーンで行われます。

Beacon Chainのローンチには、約2,000,000のETHがステーキング、65536のノードが参加することが求められています。

10月に開催されるDevcon 5でdeposit ceremonyというイベントが開催される予定です。これより少ないノード数の場合、ネットワークのセキュリティにリスクを抱えるとされ、Beacon Chainはローンチ出来ません。

また、重要な点として、フェーズ0時点でETH2を1.xチェーンに引き出すことはできません。この時点でのBeacon Chainではコントラクトの実行が出来ないためです。

■フェーズ1 : Sharding、Cross-Link

フェーズ1はシャードチェーンの実装です。

1. シャーディング

Ethereumのスケーリングを劇的に改善する手法としてシャーディングを実装します。

shard（シャード）という概念で、これは細かい個々のチェーンによる並列処理で、スマートコントラクト、トランザクション、ステートを管理します。

このシャードチェーンは1024に分かれることで、トランザクション性能の桁が変わります。1024のシャードチェーンのそれぞれのブロック生成をBeacon Chainのバリデータが行います。

どのシャードにどのバリデータがブロック生成を行うかはセキュリティを高めるために、周期を決めランダムで選出される必要があります。このランダム性の担保手法に持たせるためにVerifiable Random Function（VRF）の研究が行われています。

2. Cross Link

それぞれのシャードチェーンの最新の状態は6分ごとにBeacon Chainにハッシュで記録されます。

Beacon Chainにハッシュが書き込まれた時点で、各シャードはファイナリティを得ます。

* フェーズ1時点でのシャードチェーンはアカウント情報の保持やスマートコントラクトの実行は出来ません。

フェーズ1は、シャーディングのテスト実装のようなフェーズです。

しかしフェーズ2が完了すると、このシャードチェーン上でコントラクトの実行やトランザクションを行い、現時点と比較して桁違いのトランザクション性能を獲得します。

シャードチェーンは、1024の存在し、各シャードに128のバリデータが必要です。

$1024 \times 128 \times 32 \text{ETH} = 4,194,304 \text{eth}$ がステーキングされる必要があります。

これは執筆時点のEthereumの供給量の4%超にあたり、最低でもこれだけのETHがステーキングされない場合、フェーズ1への移行が出来ません。

■フェーズ2：eWASM

フェーズ1はシャードチェーンの実装です。フェーズ2は、eWASMの実装です。この段階でいよいよEthereum2.0はスマートコントラクトの実行が出来るようになります。

1. eWASM

Ethereum2.0チェーンにeWASMというバーチャルマシンが実装されます。

この新しいこれまでのバーチャルマシンであるEVMとは異なり、バイトコードがOPCODEからWASMへ変更されています。

WASMはW3C（World Wide Web Consortium）で標準化されているWeb Assemblyという仕様であり、eWASMのベースとなっています。

もともとはWebでもCやC++並みの実行速度を実現するという目的で、asm.jsから派生した仕様です。

WASMはどのような環境であれ、ブラウザ上で動きます。

これは、WebあるいはブラウザがWindowsやMac OS X、Linuxのような広義な意味でのOSとなることを意味しています。

eWASMは、このWASMに準拠した形でのバーチャルマシンで、Ethereum-flavored Web Assemblyを略してeWASMと呼びます。

これによってSolidityだけでなく、様々な言語でEthereumの開発が行えるようになり、開発者の参入ハードルが大幅に下がることが期待されます。

2. Ethereum2.0でのスマートコントラクトの実行

eWASMによって、それぞれのシャードチェーンはアカウントとコントラクトの保持、Stateの保持と更新が出来るようになります。

しかしこの時点で、各シャードチェーンはシャードチェーン間のコミュニケーションができません。

数分ごとにBeacon Chainにハッシュが書き込まれ、ファイナリティを得るので、異なるシャードのコミュニケーションにはタイムラグが発生することになります。

■Ethereum 1.xのロードマップ

Beacon Chainという新しいブロックチェーンが開発され、それと平行してこれまでのEthereumチェーンであるEthereum 1.xも残るということは説明した通りです。

この間、Ethereum 1.xチェーンにアップデートがないということはありません。

そもそもフェーズ2に到達するまでは、スマートコントラクトやアセットの発行などは引き続き、このチェーンで行われます。

1.xチェーンで予定されていることは明確ではないですが、特に重要なテーマをいくつか整理します。

1. VMのアップグレード

Ethereum2.0と同様に、1.xでもeWASMへバーチャルマシンのアップデートが予定されています。

2. フルノードの運用を持続可能にする。

増加するブロックチェーンのデータサイズを抑制する提案が複数あります。

その中でも主なトピックはState Rentと呼ばれるもので、Rent Fee（手数料）を支払えないコントラクトのState Root HashとCode Hashを残してデータが削除されるなどの仕様が検討されています。

フルノードの持続性等に関する問題は下記のレポートでも取り上げています。

* レポート：ブロックチェーンにおけるフルノードの役割と、その肥大化など恒久的に考えられる問題への理解や解決アプローチについて

（d10nLab会員のみ閲覧可能）

3. Beacon Chainとの連携

Beacon Chainは、1.x chainをファイナライズしますが、そのコネクションを作ることが必要とされます。

■レイヤー2の開発（Plasma、State channel、サイドチェーンetc）

また、Ethereum2.0に加えてレイヤー2という括りでカテゴライズされるPlasmaやState Channel、サイドチェーンなどの技術が、コアのEthereum以外で開発されています。これらは何かしらの形式でメインチェーン以外でトランザクションを行い、トランザクション性能向上やメインチェーンにはない機能を拡張させることを目的としています。これらについては以下のレポートで解説をしています。

* レポート：Plasma概観。Ethereumをはじめとしたブロックチェーンを拡張させるレイヤー2技術の基礎的理解（d10nLab会員のみ閲覧可能）

* レポート：Celer Networkの概要。Ethereumのレイヤー2であるState Channelを用いたプロジェクトの仕組み・トークン設計など（d10nLab会員のみ閲覧可能）

* レポート：SKALEの概要。汎用性のあるサイドチェーンによりEthereumの拡張レイヤーを目指すプロジェクト（d10nLab会員のみ閲覧可能）

■PoSのステーキングに参加してバリデータになるには

次にバリデータの参加についてです。

Ethereum 2.0は多くのユーザーがバリデータに参加できることを優先順位の高くデザインされており、ラップトップPCやラズベリーパイのようなシングルボードコンピュータでも運用ができます。

1ノード32ETHをステーキングして、ラップトップの場合3~10スロット、ラズベリーパイで最大3スロット程度のノード運用できる見通しがされています。

100スロット（3200ETHのステーキングなど）の場合は、専用サーバーなどの環境が推奨されます。

一定期間のオフラインがある場合、スラッシュが行われ、一部ETHが没収されます。Ethereumのステーキングの参加は他のブロックチェーンと比較して簡単ですが、それでも一般の人が確実にオンラインの環境を自宅で整備することは一定のハードルがあると言えるでしょう。

この課題を踏まえてステーキングのためのライトクライアントなどもフェーズ2以降で提案される可能性もあります。

また、既に述べているように、フェーズ0でステーキングしたユーザーはそのETHを1.xチェーンに引き戻すことは、しばらく出来ません。

恐らくフェーズ2のローンチまで時間がかかるはずであり、つまり1年半-2年間の間（フェーズ2のローンチが遅れればそれ以上の期間）、1.xチェーンにETHを戻せない可能性を考慮してステーキングに参加する必要があると言えます。

（参照：

https://www.reddit.com/r/ethereum/comments/cdg8v6/ama_we_are_the_eth_20_research_team_pt_2/etv8ios/)

■PoS参加に対するETHの報酬、インフレーションレート

PoSのステーキングに参加してどの程度の報酬を得られるかは下図をご参照ください。

ETH validating	Max annual issuance	Max annual return rate
1,000,000	181,019	18.10%
3,000,000	313,534	10.45%
10,000,000	572,433	5.72%
30,000,000	991,483	3.30%
100,000,000	1,810,193	1.81%
134,217,728	2,097,152	1.56%

参照 : <https://github.com/ethereum/eth2.0-specs/pull/971>

これは2019年4月にVitalikが提案したもので、ステーキングされているETHの総量とリワード率（≠インフレ率）が反比例します。

ステークされるEtherの数が増えれば増えるほど、バリデータノード1つあたりのリワード率は減っていくような仕様になっています。

ノードの数が少ない時には報酬率が高く、ノードの参加を促す仕組みになっています。

* レポート：各ブロックチェーンがステーキングに対するリワードをどのように決定しているか。ブロックチェーンにセキュリティを加えるためのコストの決定方法

(d10nLab会員のみ閲覧可能)

■バリデータへのペナルティ・スラッシュ

バリデータノードがオフラインになった場合、または悪意のある行動をした際の罰則について解説します。

ステーキングしたETHが没収される罰則を設けることにより、ノード運営者が正しく運用することを期待しています。

これは2種類の罰則が設けられています。

- **Inactivity leaks**

バリデータノードがオフラインになった場合に発生するペナルティです。

一つの基準として18日間オフラインになった場合、最大でステークしているETHの60.8%がスラッシュされます。

- **Slashing**

バリデータが二重署名などを試みたと判断された場合にスラッシュがおきます。

最低で1ETHの罰則ですが、ネットワーク内で複数のノードが同時に二重署名を起こした場合などは、より悪意がある行動されスラッシュされるETHの量は比例して大きくなります。

■フェーズ2まで到達したEthereum2.0はどのくらいのトランザクション性能があるのか？

フェーズ2まで到達したEthereum2.0がどの程度のトランザクション性能があるのでしょうか。

これについて正確な理論値を今の時点ですることは不可能ですが、下記に試算があります。

Value	Current Chain	Shasper
shards	1	1024
block(slot) time	14.5	8
blocks/minute	4.1	7680
blocks/day	5,959	11,059,200
blocks/year	2,174,896	4,036,608,000
block gas limit	8,000,000	8,000,000*
daily gas cap	47,668,965,517	88,473,600,000,000
avg gas/tx	76,364	76,364
tx/day cap	624,237	1,158,582,857
tx/min	434	804,571
tx/sec	7.2	13,410

参照：<https://ethresear.ch/t/transaction-throughput-under-shasper/3467>

この試算によると、Ethereumのトランザクション性能はおおよそ1800倍になります。各シャードのBlock Gas Limitによって大きく異なってきますが、ここでは800万程度の数字を当てはめて試算がされています。いずれにしてもフェーズ2のEthereumでは劇的なトランザクション性能を得ることになります。

■Ethereum2.0の主要クライアント

Ethereum2.0の主要クライアントを紹介します。

- **PRYSM (PRYSMATIC LABS)**

Go言語での実装です。

GitHub : <https://github.com/prysmaticlabs/prysm>

- **NIMBUS (STATUS)**

Nimでの実装

GitHub : <https://github.com/status-im/nimbus>

- **LIGHTHOUSE (SIGNA PRIME)**

Rustでの実装です。

GitHub : <https://github.com/sigp/lighthouse>

■Ethereum2.0の開発資金は誰が拠出するのか？

ブロックチェーンのクライアントはオープンソースであり、その開発者の給与は誰が支払うかの問題が浮上します。

Ethereum2.0でもこの問題は上がっており、様々な議論や提案がなされています。

この開発費をどのように拠出するか of 主要な提案が下記です。

- **EIP2025**

EIP2025という提案がEthereumコミュニティで議論されています。

EIP2025で提案された内容は、18ヶ月間ブロック報酬をブロックごとに0.0055ETH増やし、合計で17050ETHの資金を、Ethereum1.xの開発者のために拠出しようという提案です。

こういったプロトコルレベルで規定してインフレーションレートを開発者のための資金に割り当てるということは、他のブロックチェーンではEOS、Decredなどが挙げられますが、BitcoinやEthereumのようなメジャーなブロックチェーンでは導入された事例は過去にありません。2019年7月の執筆時点では、この提案の議論は具体性があるレベルまで進んでいるようには見えず、また否定派も多く見受けられ即時に現実になる可能性は低いと言えるはずですが、しかしこういった手法で開発者資金を拠出することも潜在的にはあり得ます。

- **Moloch DAO**

このDAOは寄付金を管理するようなDAOで、誰でも寄付が出来、寄附金額に応じた投票権利を得られて、その投票権利を持って寄付金の使用方法や配布先をガバナンスしていくという仕組みです。

そしてこのDAOはEthereum上にデプロイされており、スマートコントラクトで制御されています。

この仕組みを通して、Ethereum2.0クライアント開発資金を拠出しようとしています。

同DAOにはVitalikやJoseph Lubinも寄付しており、相当額が管理されています。
Moloch DAOについては、下記のレポートでも解説しています。

* レポート：DAOを構築するMoloch DAO。クラウドファンディング的なDAOプロトコルの概要・仕組み（d10nLab会員のみ閲覧可能）

- **Ethereum Foundationからの助成金**

Ethereum Foundationは、保有しているETHをコミュニティのための助成金として使用しています。

2019年の助成金予算では「(i) Building the Ethereum of tomorrow」という枠で、Ethereum2.0のクライアント開発者への助成金予算が組まれています。

既にNimbus、Prysm、Sigma Prime、Substrate Shasperが助成金を受け取っています。

（参照：

<https://blog.ethereum.org/2019/05/21/ethereum-foundation-spring-2019-update/>）

■不明点や懸念点

よくある不明点や懸念点について、筆者の認識する限りの見解を書きます。

1. ETH2の取引所の上場とはなにか？

既に述べているようにフェーズ0時点でETHのデポジットをすると、フェーズ2まで1.xチェーンに引き出しなどは出来ません。

しかしながらBeacon Chain上のETH2トークンは、別のブロックチェーン上で存在します。

このETH2トークンが取引所に上場することも考えられるはずであり、ETHとETH2が別々のアセットとして市場で取引される可能性もあります。

2. 現在のEthereumのアセットをどのように2.0に引き継ぐのか？

1.xチェーンのアセットをどのように2.0に引き継ぐかについて、現実的な議論になるのはフェーズ2以降でしょう。

それ以前はバーチャルマシンも保持しない2.0に移行するニーズもないですし、移動することも難しいです。

フェーズ2の段階で、両ブロックチェーン上での2wayペグや、一方通行のブリッジのコントラクトが複数開発されるのではないかと予想されます。

そのコントラクトを用いて各アプリケーションが対応していくと思われれます。

3. 1.xチェーンはいつまで存在するのか？

PoWの1.xチェーンはいつまで存在し、完全にPoSだけで機能するネットワークはいつになるのかという問いに現時点で明確な解答はありません。

1.xチェーンは少なくとも5年は存在すると思われれます。

■総論

本レポートでは、Ethereum2.0について2019年8月時点で明らかになっていることを幅広く解説しました。

レポート全文を読まれた方は、EthereumのPoSへの移行はどのように行われるかについておおよその理解が出来たでしょう。

一方、レポート中で示した通り、フェーズ2から先はまだ不透明な点も多いです。

同時にフェーズ1とフェーズ2もまだ先であり、これから仕様変更やローンチの遅れが発生する可能性も十分にあり得ます。

しかしながらEthereum 2.0が、フェーズ2まで完了をした際のスケーラビリティやeWASMは、これまでのパブリックブロックチェーンから大きく異なるものになるでしょう。

■参考リンク

<https://github.com/ethereum/eth2.0-specs>

<https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/>

執筆者：平野 淳也

初出：2019年7月

- ◆本レポートは、暗号通貨/ブロックチェーンの情報プロバイダ「d10n Lab」が提供しています。d10n Labにご入会頂くと過去の800本以上のレポートやコラムが全て閲覧できる他、不定期で行われるブロックチェーン関係イベントなどにアクセスできます。詳細・ご入会はこちらから <https://d10nlab.com/>

