初学者のための Polkadot 入門

非中央集権化 | ブロックチェーン | Polkadot

gbaci 著

原著：Polkadot for Beginners: A non-technical guide to decentralization, blockchains, and Polkadot

著者：gbaci（ラゴス, ナイジェリア）

編集：AnaelleLTD 初版

日本語版：初学者のためのPolkadot入門 非中央集権化、ブロックチェーン、Polkadotの非技術者向けガイド

日本語版翻訳：KumaGorow、Yoshida2、ek

＜翻訳にあたっての注意事項＞

本書に登場する「私」「著者個人」は全て原著者であるgbasi氏を指します。

本書を翻訳するにあたり原著の表現は最大限尊重しつつ、日本語読者の皆様に分かりやすいよう一部表現を加筆・修正しています。また暗号資産を取り巻く状況は発展が目覚ましく、翻訳時の状況と執筆内容に顕著な違いが認められた場合には、推敲を重ねた上で同様に修正を行っています。

表現には最大限の配慮を行なっていますが、明かな誤訳、事実と異なる記載があれば

Twitter: @kuma56_munage

までご連絡下さい。検討の上、必要があると判断した場合には修正致します。

謝 辞

この本は、PolkadotのオンチェーンTreasury（PolkadotコミュニティがPolkadotテクノロジーの採用を促進するためのプロジェクトやアイデアに資金を提供できる仕組み）によって実現しました。

まず、Raul Romanuttiには私のTreasury proposalの草稿を作成する際に、手助けや指導をしていただきました。

また、ネットワークの長期的な安定と成長に向けて監督し、舵取りをするありがたい仕事を担っているPolkadotの評議会メンバーにも感謝します。彼らの献身的な努力なしには、このエコシステムが過去2年間にこれ程の進展を遂げることはなかったでしょう。

加えて、本書の内容の技術的なレビューにおいてEmre Surmeli氏には非常に有益なご指導をいただきましたので、感謝申し上げます。Web3 Foundationの教育部門責任者であるBill Laboonも、この本の実現に大きく貢献していただきました。

そして、Anaelle LTDの専門的な編集作業とブロックチェーン技術に関する見識のおかげで、本書がとても読みやすくなったことに御礼申し上げます。

最後に、ツイートや投票、ドラフトレビューの呼びかけに応えて、本書の制作に参加してくれたPolkadotコミュニティのメンバーに感謝します。コミュニティはそのメンバーの献身的な努力によってのみ強くなるものであり、私は互いに助け合うことに対して熱意を持った人々で満たされたエコシステムの一員であることに、感謝しています。

目 次

はしがき

15世紀までのヨーロッパの商業は、地中海貿易を支配していたヴェネツィアとジェノバの商人によって支配されていました。インドから運ばれた商品をエジプトのアレキサンドリア港の商人らが購入し、紅海を経由してエジプトへと運んだ後にカイロで売られ、スルタンによって重税を課された後にアレキサンドリアの商人のもとへと届きます。それをヴェネツィアやジェノバの商人が購入し、ヨーロッパ中に高価な品物を流通させて富を得ていたのですが、一部の者が利益を得て他の者が犠牲になるこの非効率的なシステムに対して異議を唱える者が出てきたのです。
その後の15世紀末、ポルトガル人がインドへの直行ルートを発見し、ヨーロッパ大陸の人々がこれまで支払っていた金額の何分の一かで製品を輸送することを可能にしました。これにより、旧世界の運営方法は激変し、数年のうちにヴェネツィアやジェノバは東洋との貿易には接点を持たない存在となったのです。

ここでブロックチェーン技術を「ポルトガル人が発見したインドへの直行便」と考えてみましょう。旧世界を破壊するためには一定のインフラが整備されている必要がある、という意味です。上記の例ではルートの発見から数年間は、港を確保し、連絡を取り合い、サプライヤーを確立するまではあまり多くのことはできませんでした。最終的に、このインフラの導入こそがヴェネツィア人を滅ぼし、全く新しい商業・貿易のあり方を打ち立てる最後の一撃となったのです。

今日、ブロックチェーンが離陸し、旧世界の破壊の地盤を固めるために必要なインフラが構築され、ゲームと暗号、アイデンティティと暗号、金融と暗号など、さまざまな業界が融合し始めています。このように業界が絡み合うとき、どのような魔法が起こり、どのようなイノベーションが生まれるのかについては私たちは推測することしかできません。ブロックチェーンのプロジェクトは、他のプロジェクトや暗号の世界以外の関係者とコミュニケーションをとり、相互運用しなければならない事が明らかになってきています。
現状では世界はもはや単一のブロックチェーンに支配されているわけではなく、すでに「マルチチェーン時代」に突入しており、そこで大きな役割を果たすのが本書を通して学んでいただく「Polkadot」です。

伝統的な金融業界では、Bitcoinとその影響すべてに対してやや傲慢な態度があり、（私を含め）多くの人がブロックチェーン技術の初期段階での利点を理解することを妨げてきました。幸いなことに、この態度は変わりつつあります。
この業界は世界の金融・経済システムに根強い悪影響を与えているにもかかわらず、まだ乗り越えられていない多くの課題を抱えています。例えば、伝統的金融の中の銀行業は他の市場参加者と一致しない報酬体系を採用しています。銀行員もその一員であり、近視眼

的で年度末のボーナスを重視し、自分の行動に責任を持ちません。金融危機の際に「安全だと思われていたのに実は非常にリスクの高い投資商品」が欲に駆られて販売されたように、このような仕組みがあまりに受け入れがたい銀行業務につながったのです。依然として投資家のためになることではなく、あくまでも手数料の額や中央集権的な組織に蓄積されたデータに基づいて投資推奨が行われています。

私はブロックチェーン技術を学び始めてから、非中央集権型（分散型）のパーミッションレスネットワークこそが信頼とセキュリティの問題を解決するものであり、もはや企業だけに頼る必要はないことを知りました。そしてブロックチェーンのプロトコルに組み込まれた報酬の仕組みは経済的な利害を一致させ、参加者が責任を負うことを保証するものであるということもです。ネットワークを利用したい人、ガバナンスについて提案したい人、ネットワークのセキュリティ確保に協力して報酬を得たい人は当該プロジェクトの「トークン」を所有しなければなりません。そうでなければ、参加者は資本を失うリスクがあるため、これは最終的に参加者に対して「良い行い」を取らせるように働きます。

一方で私の場合は、Bitcoinという新しい通貨について学び、その出現が私たちの通貨取引を補完するものであることを理解するのに時間がかかりました。まず手始めにBitcoinの取引を記録するためのプロトコルであるBitcoinブロックチェーンの仕組みについて学びました。Ethereumは「プログラムで制御可能」なブロックチェーンで、その上にアプリケーションやスマートコントラクトを構築し、オンチェーンでの取引を記録できるプロトコルを持っています。Bitcoinのブロックチェーンが通話専用の固定電話であるのに対し、Ethereumはアプリケーションをダウンロードして実行できるスマートフォンと考えてみてください。

Ethereumはブロックチェーン技術で何ができるかという点でパンドラの箱を開けたと言えますが、Ethereumのブロックチェーン上のトラフィックが爆発的に増加するにつれ、その欠点が明らかになり始めました。よく知られていることとしてガス代が高い、トランザクションが遅いなどの点もありますが、隠れた問題もあります。Ethereumのブロックチェーンはあまり頻繁に更新されるように設計されていないため、アップグレードをする場合、実行は非常に困難で時間がかかるのです。またEthereumのブロックチェーンは当初の設計では相互運用性の問題を考慮していなかったため、他のチェーンと通信するように作られていないことも欠点ですが、そうした問題点こそがPolkadotを生んだのです。

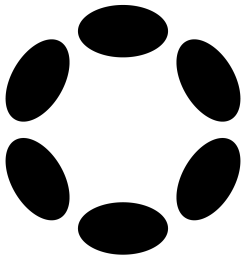
Polkadotは「パラチェーン」と呼ばれる独立したブロックチェーンがPolkadotに接続できる仕組みであり、基本的に接続とセキュリティを代行します。Polkadotは時間とともに自身のデザインを変更可能で、異なる「チェーン」間の相互運用が可能になるのです。Polkadotはブロックチェーン空間全体をよりスケーラブルにし、ネットワーク効果を高めるものであり、例えるなら都市をつなぐ鉄道のように経済活動を盛んにします。

ブロックチェーンの革新のスピードが速く、また私自身がコンピューター科学者や開発者でないため、どのブロックチェーンプロジェクトが違いをもたらすかについて正しく理解するのは困難でした。想像してもらいたいのですが、先ほど見たポルトガルの事例でもしあなたがリスボンにいて輸送ルート発見のことを知ったら、一隻の船に投資して自分の個人的なビジネスのために使用していたかもしれません。
しかし、当時は無事に帰ってこられる船は少なかったので、航海自体は非常に危険なことでした。それよりも船工場のような、作った船を売るだけでなく遠征の成功によって得られるロイヤリティで利益を得られる、より良い投資先があるはずです。

私は正にPolkadotをそのようなものと捉えています。Polkadotでは独立したブロックチェーンがオークションを勝ち抜き、スロットを確保することでPolkadotのインフラに接続し、パラチェーンとなることを前提としています。つまり、プロジェクトは自分たちのユースケースに集中し、セキュリティや接続性についてはPolkadotに任せることができるのです。パラチェーン候補のプロジェクトのサポーター達はPolkadotのネイティブトークンであるDOTを預け、該当プロジェクトがパラチェーン枠を獲得すればプロジェクト独自の暗号資産で報酬を得ることができるでしょう。このシステムはプロジェクトがその品質、エンドユーザーとの関連性、そしてコミュニティのサポートを維持し、スロットリース終了後もPolkadot上で稼働し続けることを保証しています。この特別な機能により、Polkadotのエコシステムは常に最高のプロジェクトを獲得し、革新の先頭に立ち続けることができるのです。これがPolkadotがブロックチェーン分野で重要な役割を果たすと私が考える理由です。

オープンソースのプロトコルに何百万人もの非常に賢い人々が同時に取り組んでいるという事実は過去にはなく、ブロックチェーンの世界において類を見ない発展をもたらしました。私たちはまだ始まったばかりで、生きているだけで素晴らしい時代なのです。この本を読めばBitcoinへの投資は「価格への投資」、ブロックチェーンへの投資は「イノベーションへの投資」、そしてPolkadotへの投資はそのイノベーションの多くを担う「鉄道システムへの投資」であるということにきっと同意してくれることでしょう。

— Jean Philippe Tissot
Arauca Capital 創業者兼ポートフォリオ・マネージャー



序 章

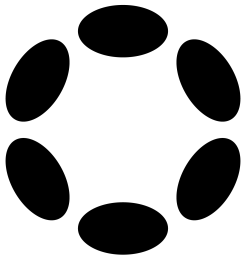
2020年5月26日の登場以来、Polkadotは人間組織の未来について同じような価値観を持つ、多様な人々の想像力を掻き立ててきました。Polkadotは他のブロックチェーンと接続することを主な目的としたブロックチェーンです。ブロックチェーンが何であるかを理解している人が少ないことを考えると、他のブロックチェーンと繋がるというPolkadotの客観的なアイデアを難解なものと捉えるのも無理はありません。このように、Polkadotが何であり、どのように機能するのかを理解しようとするのは大変な知的努力です。
少なくとも、かつてはそうでした。

本書は、ブロックチェーンやコンピューターネットワークの技術的な予備知識がなくても一般の読者がこのエコシステムを理解できるように、Polkadotの膨大な複雑さをなるべく単純に紐解くことだけを目的に書かれたものです。そのために、多くの概念的な表現から技術的な部分を大幅に削ぎ落としています。それだけでも本書は平均的な読者には理想的ですが、技術面に精通した人にはそうではないかもしれません。とはいえ、ガバナンス、クラウドローン、パラチェーンオークションなど、技術的な範囲に収まらない分野でもPolkadotについて学ぶべきことはたくさんあるのです。

筆者の願いは、ブロックチェーン技術と非中央集権型Web（別名Web3.0）の大胆なビジョンを示し、スケーラビリティ（最大限の普及）、共有セキュリティ（最大限の多様化）、相互運用性（最大限の革新と利用性）の問題解決を提案した文書「Polkadot ホワイトペーパー」を初めて読んだときのように、読者が魅了され、インスピレーションを受けてくれることにあります。

Polkadotホワイトペーパーでは革命を必要とする異なる産業に特化した、できるだけ多くの種類のブロックチェーンを構築することで、デジタル化された所有のあり方と個人の自由を実現することが目標であると明言されています。

しかし、物事の順序を誤ってはいけません。ここでは「Polkadotが何であり、どのように描いた世界を実現するのか」の説明は後回しにします。まず、「なぜPolkadotが必要なのか」ということから始めましょう。私は新しい技術を理解する最も簡単な方法は、その技術を生み出す原動力となった哲学について学ぶことだと考えています。そこで、まずは「非中央集権化」の哲学から始めましょう。



非中央集権化の哲学

この章では、なぜブロックチェーンにおいて非中央集権化がこれほど重要なのかについて説明します。というのも、非中央集権的な世界へ訪れた人たちの間で誤解があるようなのです。多くの人がここに利益を求めてやってきては、お金を得ることだけがこの業界のすべてだと思い込んでいます。

もちろん、生涯において資産を増やすことだけに集中している方もたくさんいますし、これはまったく悪いことではありません。誰もが自由に選択していいのです。しかし、6000億ドル以上の高額な時価総額に鎮座するBitcoinは、金融エリートの専横や冷淡さに対する反動から生まれたことを忘れてはいけません。ちなみに、Ethereumの発案者であるVitalik Buterin氏は、財閥の横暴が原因でEthereumの創設に駆り立てられたという逸話をご存知ですか？著名なゲームである「World of Warcraft」がゲーム内の全財産を一方的に差し押さえたとき、彼は泣き寝入りしたという有名な逸話があります。

これはどちらも個人の自由を追求した事例です。お金が絡んでいたのですか？-もちろんです。金銭的な利益を得ることが最終目的だったのでしょうか？-いいえ。ポイントは常に、人類をより良い場所、つまりより大きな個人の自由へと導くことだったのです。もし非中央集権化がこの最終目標を見失ったら、制御不能に陥り、無敵なヒドラのような存在になってしまうでしょう。

先人からの教訓：中央集権の必要性

中央集権と非中央集権という言葉は「権力、所有権、権威」の管理方法の違いを指しています。それらがセキュリティに直接関係するのは、次のような理由からです。

1). 所有者は、所有物のセキュリティに責任がある。
2). 所有者は、所有物に対して権力と権威を持っている。

中央集権的なシステムでは、3つの属性（権力、所有権、権威）はすべて、王、議会、政府、CEO、経営者など中心から発せられます。政府は国政を司る中心的な存在であり、一方で企業はビジネス業務を司る中心的な存在です。このような中央集権的な組織形態は、何世紀にもわたって私たちに役立ってきました。なぜなら、中央集権は私たちが文明を築くためにもっとも効果的な方法だったからです。しかし常にそうだったわけではありません。中央集権は、農耕の発明とともに始まったのです。

農耕以前の狩猟採集民の祖先は一箇所に定住することもなく、多くのものを所有することもなかったので、現在のようなセキュリティに悩まされることはありませんでした。そのため、当然ながら現在のような治安の心配はありません。統治形態も非中央集権型で、何をするか、どこに行くかを部族ごとに決めていました。しかし、狩猟採集民の祖先は農耕の利点を見出すと、遊牧民としての生活を捨て、定住するようになったのです。

それ以来、人々は農地を持ち、家を持ち、村を持ち、明確な境界線が引かれるようになりました。しかし、食糧の安定供給と同時に人口は爆発的に増加し、新たな問題が表面化します。それは私たちの祖先が多くの決断を迫られたことです。土地をどのように共有するのか？誰が争いを解決するのか？自衛のため、あるいは征服のため、戦争になったら誰が指揮をとるのか。例えば、人口5,000人の王国を、敵対する国の兵士たちが征服にやってきたとします。もし侵略された王国が分権的な組織モデルを採用するならば、結論を出すまでに長い間熟考する必要があるでしょう。その間に、王国は間違いなく侵略者に捕らえられてしまいます。
そこで新たな繁栄と生活に見合った新しい組織形態が必要となり、事実上の組織原理として中央集権化が普及し始めました。

職業の専門化により部族全員が農民である必要はなくなったため、中央集権が可能になりました。つまり、安定した食糧供給のおかげで人々は自分の才能と可能な仕事に応じて専門化を進め、先人たちはある人がリーダーとして正しい道筋を議論し、決断することでコミュニティがより効率的に資源を活用し問題を解決できることを理解したのです。
ここで何が起こっていたのか、一度考えてみましょう。当時のコミュニティはより効率的になるために、権力、所有権、権威をコミュニティの中心部（王、評議会など）へ譲ることにしたのです。この進化をトーマス・ホッブズは『リヴァイアサン』（1651年）の中でこう表現しています。ホッブズによれば「全能の組織は、個々の構成員が自然の法則によって生きる権利を放棄し（別名「各自のために」）、その行為の結果として生まれる君主（中央の代理人）にすべての権限を渡し、以後君主が作った法律に従うことを約束したときに誕生するのである。」

このような組織形態は何世紀にもわたって私たちの中心であり、文明を発展し、世界を形作るうえで大いに役立ちもしました。

恐慌、検閲、抗議行動：中央集権化の負の側面

> 2007年の米国住宅市場の崩壊は、規制当局の誰も予測できなかった。その原因は、ほとんど誰も理解していなかった抽象的な投資に対する安全性の幻想が広まったことにあり、それを理解していた人はほとんどいなかった。このシステムは現在も当時と同様に複雑であり、同様の危機が再び起こる可能性がある。もしかしたら明日かもしれない。
>
> —ハンス・ロスリング著「FACTFULLNESS」

ご存知のように、すべてのものには負の側面があります。中央集権化の場合、私たちはその影響にさらされ、その都度、事態は決してこれ以上悪くならないと思い込んできました。しかし、残念ですが現実はこの考えが間違っていることを証明しています。
2008年、米国の一部の銀行家の行為によって、世界経済は大金融危機に引きずり込まれました。そのことを少し考えてみてください。一部の人間のために、全世界が苦痛と心痛を味わったのです。

この危機の本当の問題は銀行家たちがこのゲームに参加しなかったことであり、彼らは他人のお金で遊んでいたのです。そしてゲームが終わりを迎えたとき、自身に大きな影響はありませんでしたが、世界の残りの人々は大きな代償を支払わなければならなかったのです。これは従来の金融の世界におけるインセンティブ・デザインの失敗であり、新しいWeb3.0の動きが歓迎すべき進化である理由でもあります。もし、非中央集権型金融プロトコルが何らかの理由で損失を出したとしても、それを救済する政府は存在しないのです。

私はナイジェリアのEndSARSデモで、中央集権化の負の側面を個人的に経験しました。ナイジェリア政府は権力を乱用し、平和的な抗議活動を支援・促進する人々の口座を凍結するよう銀行に強制したのです（私は当時の状況を追っていたので、このデモが平和的な抗議活動であったことを証言できます）。当時、政府が想像を絶する方法でデモを弾圧する前にBitcoinとEthereumを用いて1週間余分に運動を維持できましたが、その後ラゴスの政府はレッキトールゲートに軍隊を送り込みました。そして、兵士がデモ隊に実弾を撃ち込み、より良い生活を求めていた市民を負傷させ、殺してしまったのです。今日もなお、この出来事を考えると涙が出てきます。政府が罪のない市民に軍隊を放つことは、中央集権的な権力の最高の乱用です。皮肉なことに、この抗議はSARSと呼ばれる悪徳警察部隊によるナイジェリアの若者たちに対して振るわれる警察の残虐行為をやめさせることを目的としていたのです。参考資料として、この悲劇に関するCNNの報道を添付します。

また他の例として、FacebookやGoogleなど、私たちが利用しているWeb製品やサービスを中央集権化がうまくいかなかった例として挙げることもできます。現在のWebは、時間が経つにつれ、より中央集権化を促すような構造になっています。Googleが広告主にとって非常に価値があるのは、Google自身はアクセスできるが、実際には所有をしていないデータがあるからです。
Instagramをはじめ、私たちが使っているソーシャルメディアアプリも同じです。ユーザーデータがなければ、それらの価値は現在よりもはるかに低くなってしまうでしょう。これらの企業は私たちのデータを利用しつつも、所有者である私たちに一銭も支払うことなく、10億ドル規模の帝国を築くことに専念しているのです。さらに悪いことに、彼らはいつでも好きなときに私たちを検閲することが可能です（そして実際に検閲しています）。これは私たちが生きている世界の現実であり、Bitcoinが登場するまでは代替手段がなかったため、受け入れざるを得ない事実でした。では、Bitcoinはこの状況をどのように変えうるのでしょうか？

中央集権化の負の側面をさらに理解するためには、「所有権」「権力」「権威」ついてもう少し詳しく見ていく必要があります。

所有権とは、ある「もの」を誰が所有しているかということです。国の場合、土地は政府に属しますが、国民がその土地を取得した場合は例外です。しかし、その場合でも、最終的に政府はその土地を没収する権利を持っています。

権力とは、行動を起こす能力のことです。本来権力は社会全体に分散していますが、政府がより大きな割合を占め、階層的に分散されています。したがって、大統領は副大統領よりも多くの能力を持つので副大統領よりも権力を持つという事になりますし、市民は投票や抗議ができるため権力を有すると言えます。

権威とは、支配する能力を指します。当然、所有権と権力を持つものは、併せて権威も持ち合わせています。現在のソーシャルメディア空間では、あなたは何も「所有」しておらず、自分のアカウントさえも所有しているとは言えません。そのため、ある日突然ブロックされたり、アカウントが停止されたりすることがあるのです。また、このやり方が気に入らなければ、あなたに残された選択肢はその場を去ることしかないのです。多くのコミュニティメンバーがあなたに同意した場合を除き、あなたはこの管理会社に要望を伝える権限すら持っていません（なぜなら一般的に企業は大多数の意思に従うことを好むからです）。これは、あなたの銀行口座でさえも、現状では同様です。銀行はどんな理由であれ、特に政府が要請すれば、あなたの口座を凍結することができます。政府や銀行がこのような力を持つことが悪いと言っているのではありません。しかし、多くの場合、権力は乱用されます。権力の性質として、あまりに大きすぎると腐敗を招きます。これが中央集権の一つの大きな問題点です。中央集権は、少数の人間に大きな力を蓄積することを助長します。当然ながらこれは一部の人間をまるで神のように振る

舞わせ、彼らを暴君に変えるという事態を招きます（ここでいう暴君とは、悪徳な首長だけのことではありません）。

このように、中央集権から離れる必要性は多岐にわたります。

1). 強すぎる権力が腐敗することは、歴史がある程度証明している。

2). 中央集権は単一障害点を生み出し、システムを乗っ取ることを容易にする。その典型が、下記に紹介するAtahuallpa（アタワルパ）の物語である。

> アタワルパは新世界で最大かつもっとも進んだインカ帝国の絶対君主であり、相対するピサロはヨーロッパでもっとも強力な国家の主である神聖ローマ皇帝カレル5世（別名スペイン王カレル1世）に仕えていた。ピサロは168人のスペイン兵を率いて未知の土地へ訪れた。現地の住民についても知らず、近隣のスペイン人（1000マイル北のパナマ）とも全く連絡がつかず、適時に援軍が来ることもない状況だった。
> アタワルパは何百万人もの臣民を抱える自分の帝国の中にいて、他のインディアンとの戦争に勝ったばかりの8万の兵士に守られていたが、それにもかかわらずピサロはアタワルパを捕らえた。その後ピサロはアタワルパを8ヵ月間拘束し、解放の約束と引き換えに史上最大の身代金を要求した。身代金は縦22フィート、横17フィート、高さ8フィート以上の部屋を満たすほどの金塊だったが、ピサロは約束を破りアタワルパを処刑した。この事はヨーロッパによるインカ帝国の征服にとって、決定的なものであった。
> スペイン人の持つ兵器のおかげで、最終的にスペインの勝利は確実なものとなったが、アタワルパの捕獲はスペインの征服をより迅速かつ容易にした。アタワルパはインカの人々から太陽神として崇められ、臣下に対して絶対的な権威を持ち、彼らは囚われの身でありながらなおその命令に従順であった。彼が死ぬまでの数ヶ月の期間に、ピサロはインカ帝国の他の地域に探検隊を派遣し、パナマから援軍を送る時間を手にしたのだった。アタワルパの処刑後、スペイン人とインカ人の戦闘が始まると、インカ帝国にとってスペイン軍はより手強い存在となった。
>
> —ジャレド・ダイアモンド著「銃・病原菌・鉄」

3). 中央集権化は人々が権力と責任を放棄することを促し、必然的にコミュニティの多くの人々を疎外するような意思決定につながる。

4). 中央集権は所有権、権力、権威に非対称性をもたらし、多くの人々の運命を少数の人々の手に委ねることになる。

唯一の解決策？

　中央集権化の落とし穴に対する解決策のひとつが、非中央集権化です。
おそらく唯一の解決策ではありませんが、現在私たちが持っている最良の選択肢です。非中央集権化の核心は、権力と権威を中央の少数者からコミュニティ全体に再分配することにあります。このようなシステムでは、一人の人間や集団がシステムを支配するのではなく、リスク、責任、報酬を皆で共有することになります。

そして、非中央集権化の最大の魅力は「公平性」にあります。一部の人の行動ではなく私たちの集団的な行動によって事態が悪化したということを知ることははるかに良いことであり、不正、残酷、腐敗、偏見などに対して発言しても誰も黙らされることはないと知っているほうがいいのです。誰もが、誰とでも、どこでも、いつでも、経済的に自由に取引できるのだと知るべきなのです。

非中央集権化の哲学は、中央集権的な権力構造を解体することにあります。このような哲学の帰結は当然、より大きな自由を目指しています。しかし、どのような自由が得られるかは、どの非中央集権化システムについて話しているかに依存します。Bitcoinは経済的自由を目的として作られ、人々が不満を持つ経済機構から自らを解放するための選択肢を提供するものでした。Ethereumは開発者に世界を変えるようなアプリを作る自由を提供しようとし、非中央集権型金融であるDeFi（銀行員がやっていることを多くの人が自ら、自由に行えるもの）やNFT（クリエイターにここ数十年でアート業界が見たことのない芸術的自由への道を与えた）の台頭に拍車をかけたのです。これらは、最初の2つの主要な使用例に過ぎません。今後10年以内に、より多くの非中央型型プロダクトが市場に登場し、現在のシステムに代わるものを提供することが十分に予想されます。

要約すると、非中央集権化の利点は以下の通りです。

1). 中央からシステムを乗っ取ることができないため、セキュリティが高い

例えばGoogleがハッキングされた場合、ハッカーはGoogleの持つ全ての情報にアクセスできる。仮に大統領の頭脳が闇のエージェント（あるいは宇宙人）に乗っ取られたとしても、システムには多くの頭脳があるので、彼/彼女の愚行により国家が陥落することはない。

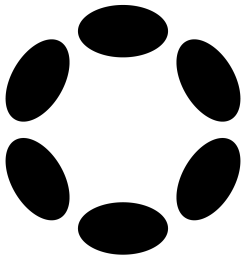
2). より多くの人が意思決定に関与するため、より公平になる

重要な問題に対して大多数が賛成したときだけ行動するコミュニティは、「誰もが平等である」という理想に即している。もし少数の人だけがコミュニティのために意思決定するのであれば、その少数の人たちが自分たちの利益を優先し、コミュニティを利用することになるまでそう長くはかからないだろう。

3). より良い所有権の分配を行う仕組み

少数の人がすべてを所有することは、生命の仕組みに反するからである。ライオンは、ジャングルにいるほとんどすべての動物を殺すことができるにもかかわらず、ジャングルを所有していない。所有権が共有されなければ、成長や進歩は一部の人にしか利益をもたらさないことになり、それはより大きな不平等を助長する嘆かわしい現状となる。

次の章では非中央集権化をどの様に実現するのかについて、一緒に具体的な方法を学んでいきましょう。



どのように非中央集権化するのか

> 私たちは毎時間何千もの神経細胞を失っていますが、私たちの精神的なプロセスはすべて高度に分散しているため、実質的に何の影響も及ぼしません。私たちの個々の脳細胞はどれもそれほど重要ではなく、最高経営責任者（CEO）の神経細胞は存在しない。
>
> ―レイ・カーツワイル著「スピリチュアル・マシーンの時代」

これまで非中央集権化の必要性、目的、利点を理解したうえで、ここからはどのようにそれを実現できるかを探っていくことにします。
かつて、多くの人間がより大きな目標に向かって非中央集権的に働くことは、比較的不可能でした。そして先の説明の通り、大きな目標に向けた組織の試みは、いずれも中央集権によって促進されてきました。しかし、なぜなのでしょうか。

多くの人が一緒に仕事をしようとするときに直面する最大の課題は「信頼の問題」だと言えます。このため、過去数世紀にわたって中央集権化が支配的な組織モデルとなってきました。中央集権は誰もが信頼できる中心的な存在を与えることにより、信頼の問題を回避してきたのです。銀行の主な目的は誰が何を持ち、誰が何を送れるのかを追跡することです。これはまた、政府が存在する理由の一部でもあります。誰が何をすることができ、何をすべきか決定するのを助けるためです。銀行は私たちのお金を安全に保つために、政府は私たちの安全を守り繁栄を促進するために、そしてソーシャルメディア企業は私たちにサービスを提供するために、お互いを信頼しています。したがって、非中央集権化に関しては「どうすればできるだけ多くの人々がお互いを信頼できるようになるか」ということが問題になります。

ですがこの問いに対する答えは、誤解を恐れずに言うと「できない」のです。信頼とは、誰もその正当性を疑うことができないように、安全な方法で情報を追跡することを意味し

ます。中央集権的な解決策は、権力、権限、所有権のいずれかを介して、信頼を1つの組織に委ねることでした。しかし、これにはいくつかのリスクがあります。

1). 中央集権化は情報の非対称性（偏り）を生み出し、一部の中央集権的な支配者が多くの利害関係者を犠牲にして自分たちに有利になるように利用する。

例えば、あるビジネスマンが数人の上院議員と友人でその立場を利用できるため、政府の決定を他の誰よりも早く知ることができる場合がそうである。銀行家と企業が常に結託しているのは、政府と銀行が連携しているのと同じことである。要するに、権力のある立場にある個人は集団よりも自分の利益を優先させ、企てるように仕向けられている。

2). 中央集権的な情報収集と検証は、単一障害点をもたらす。

これは様々な形で現れ、例えば集中管理されたサーバー（銀行記録、政府記録、ユーザーデータなど、情報が保存されているコンピューター）がハッキングされる可能性がある。ハッカーは1つの攻撃ベクトルに集中すればよいのだから、ハッカーからすると合理的な選択肢となる。そして、この管理された情.報に万が一の事態があれば、それは永遠に失われることを意味する。

では、どうすれば信頼の問題を克服し、非中央集権化を実現できるのでしょうか。

Skin in the Game

まず、真の問題は参加者間のリスクと報酬の不均衡にあることを認識する必要があります。民主主義を含む現在の諸制度は、利害関係のない人々が自分たちの利益と他人を害するような決定を下すことを許しています。したがって、2008年の銀行危機が起こったとき、それは銀行エリートが意図的に残酷なことをしたからではなくむしろシステムが彼らの無神経さと欲深さを世界経済に影響を及ぼすことを許したのです。

しかし、もし彼らのミスがエリートたち自身の資金に不利益をもたらすものであったなら、胡散臭い住宅市場に参入する前に専門家による問題点の調査を行ったかもしれません。"Skin in the Game "とは、自分自身の行動とその結果に対する責任、つまり、お金の扱いを誤った結果として損失を出したのなら、自らその損失を償わなければならないということです。さらに、間違った判断で他人の資金を使い果たしながら政府の救済措置で支援を受けるようなことはあってはならないでしょう。それは何重にも不公平なことです。

では、どのような方法を用いれば参加者間のリスクと報酬が公平であり、かつ社会全体を対象とした、大規模なシステムを確立できるのでしょうか？そこで登場したのが、ブロックチェーンとその周辺技術です。

ブロックチェーンとは何か？

ブロックチェーンはデータベース（データの組織化された集合体）です。しかし、私たちがWeb2アプリケーション（Facebook、Instagram、Googleなど）で慣れ親しんでいるデータベースとは異なります。それらの大半は単一の権威によって制御される許可制の中央集権型データベースです。ブロックチェーン上のデータは、それら従来のデータベースとは異なる、いくつかのユニークな特性を持っています。

1). 公共の分散型ピア・ツー・ピアコンピューターネットワークによってホストされている。

2). 暗号とコンセンサス（合意形成）プロトコルによって保護されており、乗っ取りは困難だがコンピューターの同期を取り続けることは容易であるように設計されている。

3). 不変である。つまり、ネットワーク上のノードから過半数の承認を得なければ、既存のデータ情報を更新したり削除することはできない。したがって、ブロックチェーン上のデータを削除したり操作することはできるが、それは多数決で合意された場合にのみ可能となる。

このようなユニークな特性を持つブロックチェーンのデータベースは、ガバナンスや通貨など、社会的な合意が有効であることが求められるアプリケーションにおいてとても有用です。

ブロックチェーンとは、中央集権的な機関が存在しないノード（コンピューター、サーバーなど）のネットワークで、データの記録と検証を行うものであるとも言えます。このデータは取引、口座残高、ネットワークの状態など、どんなものでも台帳に記録され、ネットワークのすべてのメンバーが自由にアクセスできるようになっています。

この「ブロックチェーン」と呼ばれる非中央集権型データベースを構築するためには、さまざまな「仮名」の関係者が協力する必要があります。しかし、中央の権威の監視なしに、お互いを知らない人たちにどうやって信頼してもらえばいいのでしょうか？それは、ネットワーク参加者がお互いを信頼するわけではなく、むしろプロトコルを信頼するような形で「信頼を自動化」するのです。

プロトコルとは何か？

　プロトコルはコンピューターのソフトウェアが動作するための手順の集まりです。HTTPやTCP/UDP、IPを思い浮かべてください。十戒やハムラビ法典のようなものです。プロトコルはネットワークに参加するすべての人のためのルールを設定し、新規参加者が自由にネットワークの一部になるか、離れるかを選択できるようにするものです。最も重要な点は、プロトコルは一人の参加者や特定のグループによって変更されない、ということです。ネットワーク参加者の大多数がこの変更に同意した場合にのみ、あらゆる情報の更新が可能となります。これは、トップダウン方式で変更が行われる国や企業とは明らかに異なります。

このように、ブロックチェーンはネットワーク参加者全員にネットワークへの参加・離脱の選択の自由と、ネットワークを管理する責任を与えているのです。集団的所有とリーダーシップこそが主題なのです。しかし、すべてのブロックチェーンがこの倫理観に則っているわけではありません。
プロトコルのルールが最初から明確であるからこそ、信頼することができるのです。例えばBitcoinの場合、プロトコルではネットワーク上の大多数のノード（コンピューター）が暗号パズルを解いて検証した場合にのみ、ブロック（詳しくは後述）が生成（鋳造）されます。

もっと簡単に言うと、大多数のノードが取引が有効であると同意しない限り、新しい取引は台帳に追加されません。この新しいブロックの生成時に、報酬として新しいBTCが生成されます。要約すると、それこそがBitcoinのプロトコルです。

実際にブロックチェーンはどのように機能するのか？

　ブロックチェーンは常にグローバルな「台帳」であると言われていますが、これは事実です。しかし、「ブロックチェーンは台帳である」と言ってしまうと、技術者でない人が見ても台帳のような表がないため、イメージとして誤解を招くことがあります。ここでは台帳という言葉はあくまでコンピューターの処理と人間の処理の類似性を描くために使われているのです。したがって、ブロックチェーンは情報を保存するから台帳なのであって、実際に帳簿をつけるから台帳なのではありません。しかし、この比較はブロックチェーンが何をするものかを完璧に表現しているので、このような表現は有用と言えるでしょう。
ここからは、この台帳がどのように構築されているのか、より分かりやすい説明を提案することに重点を置いていきたいと思います。

ここではブロックチェーンをより理解するために、「ブロックチェーン」という言葉を構成要素に分解して、それぞれの単語が持つ意味を考えてみましょう。

ブロックチェーン＝チェーン上のブロック
または
ブロックチェーン＝ブロック＋チェーン

ブロックとは何か？

　ブロックとは検証された情報の集まりで、グローバルな台帳に追加できるようにパッケージ化されたものです。ブロックは単一の取引で構成されることはほとんどなく、多くの取引が束になって構成されています。ブロックを生成するには、ネットワーク上で行われた有効な取引（トークンの送信、非中央集権型ソーシャルメディアサイトでの名前の変更、トークンの交換、コメントの投稿など）を暗号技術を使ってまとめ、記録します。暗号学は、生物学、化学、物理学などと同様に、証明可能な数学に基づく解読困難なパズルを使用して強力なセキュリティを作成することに焦点を当てた学問分野です。ここで暗号技術を使ってブロックを形成する目的は、将来的な改ざんを避けるためです。

ブロックはバケツのようなものだと考えてください。どのブロックも最初は空のバケツで、ユーザーがネットワークを利用するたびに、その取引結果（トランザクション）でバケツが満たされていきます。バケツが一杯になると、その後情報を参照される時に備えて封を閉じ、保管されます。ここで重要なのは、ブロックに封をするのはそのブロック内の取引が有効であることに多くの人（ノード）が合意した場合にのみ、可能であることを意味するのです。つまり、誰も所有していないトークンを送ろうとしたり、その他の不正な行為をしていないことが確認されたときです。一度封印されたブロックは再度開いて取引を変更することはできませんが、データ記録を検証するための参考資料として使用することができます。

ブロックチェーンはどのように関わるのか？

ここで、複数のブロックが存在するという事に焦点を当てましょう。各ブロックが格納できる取引結果の情報は有限だからです。したがって、取引の順序、つまりどのブロックが最初に来たかを解読し追跡するために、ブロックを連鎖させることが必要になります。ブロックを連鎖させるプロセスは、ブロックの生成そのものとそれほど変わりはありません。私は、このプロセスをよりよく理解してもらうために、あえて説明を分けただけなの

です。実際には、新しいブロックが増えるごとにチェーンは成長し、後述するProof-of-Work型ブロックチェーンの場合はよりセキュリティが高まります。

では、より深いレベル（技術的な面）においてブロックチェーンはどのようにしてこのような非中央集権型セキュリティを実現するのでしょうか。ブロックチェーンと言えど、その方法はさまざまです。そのような手法の違いはあありつつも、ブロックチェーンを分析する上で考慮すべき主な問題は2つあります。
まず、ブロックチェーンがその機能を発揮するためには、多くのコンピューターが常に互いに通信を取り合っている必要があります。これがネットワークと呼ばれ、より人間的な表現をするなら機械同士が会話を行なっている、とも言えるでしょう。このように、コンピューターはネットワーク上でデータの伝達を行なっています。要するに、ネットワーク上のすべてのコンピューターが対象のデータを持つまで、あるコンピューターから次のコンピューターにデータが次々とコピーされるのです。もしネットワークがなければ、私たちが知っているブロックチェーンは存在しないでしょう。

ブロックチェーンの2つ目の主な構成要素は、コンセンサスメカニズム（合意形成の仕組）、つまり異なるネットワーク参加者（ノード、コンピューター、サーバー）がどのデータが有効で、どれが偽のデータであるか？という結論を出す方法についてです。コンセンサスメカニズムには、主に2つの側面があります。

・コンセンサス - データ（ブロック）をあるノードから別のノードにコピーし、検証するプロセス

・ファイナリティ（最終決定） - 新しいブロックをチェーンに追加するプロセス。（両者の違いについては後述）

当然ながら、他のブロックチェーンのコード（プロトコル）を使って新しいブロックチェーンが作られた場合を除き、どのブロックチェーンも独自のコンセンサスメカニズムを持っています。しかし、どのようなコンセンサスメカニズムであれ、大きく分けて下記の3つに分類ができます。

Proof-of-Work (PoW)

Proof-of-Workは、電子メールスパムを避けるために作られたアルゴリズムで、基本的にコンピューターが悪意を持って電子メールサーバーに負荷をかけることを困難にする仕組みです。これを実現するために、メールサーバーは送信側のIPに、任意の計算量を必要とする小さなパズルを与えます。その解答作業が終わると、コンピューターは作業の証明

となる解答をメール本文と一緒に提示します。このプロセスは過去にBitcoinクライアントに採用され、コンセンサスメカニズムとして再利用されるようになったのです。

PoWではコンピューターは作業（この場合は暗号パズルを解くこと）が行われたときにのみコンセンサスを得ることができ、暗号パズルの解を最初に提供した者がブロックの生成者となり、報酬を得ます。このコンセンサス方式は、エネルギーを大量に消費するため、最近になって環境問題の観点から非難を浴びています。このようなネットワークでは、システムのセキュリティが暗号パズルの難易度とある程度結びついているため、時間経過とともにより多くのエネルギーが必要となるのです。

Proof-of-Stake (PoS)

PoWのエネルギー消費の欠点を克服するために考案されたコンセンサスの方法です。コンピューターの作業と暗号パズルを経済的利益と引き換え、システムのセキュリティをネットワーク内のトークンのステーク数（預けられたトークンの数量）に関連付けます。ステーク（staking）という考え方はここから来ています（詳細は後述）。つまり、あるシステムが大きな経済力に支えられていればそのシステムを乗っ取ることは不可能に近く、乗っ取ろうとする者はさらに大きなコストを負担することになるという論理です。例えば、200万ドルしか出資されていないPoSブロックチェーンは、10億ドル出資されているものよりはるかに容易に乗っ取ることが可能です。

Hybrid Consensus（ハイブリッド・コンセンサス）

最近のブロックチェーンはPoWとPoSを組み合わせたハイブリッド・コンセンサスを採用しており、両者の長所を生かして、より安全でエネルギー効率の高いネットワークを構築しています。ハイブリッド・コンセンサス・システムでは、コンセンサスとファイナリティにおいて若干の違いがあります。
通常、ブロックがチェーンに追加される前に多くのマイナー（またはバリデーター）によって検証される必要があり、あるノードから別のノードへデータをコピーするなど、この継続的な検証のプロセスの事をコンセンサスと呼びます。プロトコルのルールに従って十分な検証が行われると、最も「支持」されたブロックが確定され、ブロックチェーンに追加されます。この2つのプロセスを分離することで、開発者はスピード、セキュリティ、スケーラビリティの面でブロックチェーンをより最適化できるのです。

ここまでコンセンサスメカニズムについて学んできましたが、続いてブロックチェーンに関わる人たちについて、その役割を見ていきましょう。

ブロックチェーン参加者の名称

・フルノード

ネットワークのセキュリティに責任を持つ人たちです。セキュリティ担当者と考えてもよいでしょう。ブロックチェーンによってはマイナー（BitcoinやEthereum）や、バリデーター（Polkadot、Cosmos）など、異なる名前で呼ばれることもあります。どのような名前であっても彼らの目的は同じで、ネットワークを安全にすることです。彼らは非中央集権化された方法で取引を記録し、検証することによってこれを行います。

・ビルダーズ（非中央集権型アプリとブロックチェーン）

ビルダーは、現在のWeb2.0の世界における設立者に似ています。彼らは主にプログラマーで、非中央集権的なアプリケーションや新しいブロックチェーンを作成し、作業を行います。

・ライトノード（エンドユーザー、ウォレット、クライアント）

このカテゴリの多くの人々は、ブロックチェーンを使うためにその仕組みについて知る必要はないでしょう。実際、現在のブロックチェーンのイノベーションのゴールは、エンドユーザーがブロックチェーンに気づかないうちに接するようになることです。また、ビルダーズが作成した「Dapps」といったサービスを利用する人たちの事も指します。

ここまでの説明でブロックチェーンの概念についての理解がまだ不足していると感じていても、心配は無用です。これからブロックチェーンの歴史に飛び込んで、より多くの文脈を紐解き、理解を深めていきましょう。

ブロックチェーンの進化

Bitcoin（ビットコイン）の誕生

旧来のシステムでは、例えばあなたが友人に送金する場合、銀行に行って担当者に送金の代行を依頼する必要がありました。もしあなたが世界的に見ても田舎と呼ばれる地域に住んでいたなら、立ちはだかる課題は金銭的なものだけでなく、物理的なものも含まれるでしょう。

つまり、あなたは自分のお金を完全にコントロールすることができず、銀行はあなたに何の報酬も与えることなく、あなたのお金を自由に貸し出して利息を得ることができるのです。さらに、銀行は無謀な投機によってこの資金を失う可能性があり、その責任を負うことはない。おかしな話でしょう？これは、Bitcoinが予想外の方法でゲームを変えるまで、長い間続いていた事実です。

Bitcoinによって人々は初めて世界中のどこにいる誰とでも、仲介者に書類や高い手数料を要求されることなく、デジタルを用いて価値を送ることができるようになったのです。Bitcoinでは、送金のためにプロトコルにわずかな取引手数料を支払うだけでいいのです。もし送金に失敗しても返金されるため、もはや仲介者は不要なのです。このネットワークは成長し、従来の銀行システムに取って代わる可能性があります。

ここで、Bitcoinについて考えた場合、3つの特徴があります。

1). デジタル価値を転送するためのシステム/プロトコル。

2). デジタルゴールド

3). 投資対象

Bitcoinはここ最近で最もパフォーマンスの高い資産の一つとなっているため、本来の目的である「デジタルキャッシュ」ではなく、「投資」として捉える方が多いようです。

Ethereum（イーサリアム）の登場

長年にわたってネットワークの機能性を拡張するために、Bitcoinのコミュニティは「カラーコイン」を作ろうとしました。これはBitcoin上や、その周辺、またはコピーとして作られたトークンであり、さまざまな資産やアイデアを表現するためのものでした。しかし、これらのプラットフォームは意図したとおりに機能せず、Bitcoinにおけるコードの限界を超えることができませんでした。

数年間Bitcoinを研究し、"この技術をもっと一般化したらどうだろうか？"と考えたVitalik Buterin氏はこのアイデアに駆り立てられ、2014年にEthereumのホワイトペーパー（設計書）を書き、開発者がカスタムトークンを構築・設計できる汎用ブロックチェーンの枠組みを構築しました。開発者はコードを実行するために必要な計算の対価として、イーサ（ETH）と呼ばれるネイティブトークンを使用します。

Ethereumはブロックチェーンをデータベースとするグローバルなスーパーコンピューターとして構想され、ブロックチェーンの基本構造を利用し、より柔軟なユースケースを可能にするプラットフォームを構築しました。Bitcoinが単一のWebサイト/アプリで完全に占められているオープンインターネットプラットフォームであるのに対し、Ethereumはどんな種類のWebサイト/アプリでも作ることができるオープンインターネットプラットフォームだと考えてみてください。

このように、Ethereumの台頭によりブロックチェーンエコシステムの新しい構成要素である非中央集権型アプリケーション（Dapps）が生まれました。
次のテーマはクロスチェーンですが、この話題に移る前に、Ethereumにおける特徴的な機能である「スマートコントラクト」について少し調べてみましょう。

スマートコントラクトの概略

　スマートコントラクトは1994年にNick Szaboによって発明され、Ethereumによって普及しました。ブロックチェーンが様々なネットワーク参加者にお互いを信頼することなく協力するための必要なツールを提供するように、スマートコントラクトは様々な経済主体間の信頼を促進する仕組みを提供します。では、ブロックチェーンとはどう違うのでしょうか。ブロックチェーンは「ネットワークがどのように運用されるか」というルールの集合体であり、スマートコントラクトは「取引がどのように実行されるか」というルールの集合体です。

スマートコントラクトをよりよく理解するために、例として保険契約について考えてみましょう。典型的な保険契約の設定では、保険金請求者は保険会社に自分の請求が有効であることの証明を提出する必要があり、これが時に摩擦を生むことがあります。
自動車保険に加入していたのに、自分の過失で車が全損になったとします。保険会社は合意したとおりに保険金を支払うか、あるいは調査するという名目で対応を遅延させることができます。調査には数ヶ月を要することもあり、請求者はその間公共交通機関に頼らざるを得ません。調査が必要でないとは言いませんが、スマートコントラクトのポイントを理解するために、保険会社が不誠実に行動していると仮定しています。スマートコントラクトであれば、そのようなことはありません。

スマートコントラクトはあらかじめ定義されたパラメータが満たされたときに実行される自己実行型プログラムです。したがって、今回の保険の例ではスマートコントラクトに基づく契約では、次のような流れになるでしょう。まず、車が故障すると車に搭載されたセンサーがその情報をスマートコントラクトに送ります。スマートコントラクトがそのデータを確認すると、その地域のニュース報道とデータを対応付けることで、保険会社からの追加許可を待たずに自動的に保険金が支払われることになります。

このプロセスを金融における業務に当てはめてみましょう。参加者は他の参加者を信用することなく、「契約」そのものを信用することができるので、スマートコントラクトの力によって非中央集権型の貸し借りプラットフォームを独自に運営することが可能です。ここで、流動性提供者（他の人が借りるためにお金を提供する貸し手）は、他のユーザーがトークンを借りるために自分のトークンを預けることが奨励されます。なぜなら貸し手が提供しているトークンを引き出そうと思えば、スマートコントラクトが貸し手に支払われるべき報酬と合わせて預け金を全て返却することが保証されているからです。同様に借り手はスマートコントラクトが取引条件（金利や違約金）を変更しないこと、そして借りたトークンを返済すれば預けている担保が返却されることを信頼できているからです。

ここで、一つ大きな注意点があります。スマートコントラクトはそれを構成するコードと同じくらい安全でなければなりません。Web 3.0空間では欠陥のあるスマートコントラクトが原因で、資金喪失につながるハッキングが多数発生しています。したがって、スマートコントラクトとやり取りする前に、技術的な知識があればコードを見直すか、スマートコントラクトのコードが監査済みであることを確認することをお勧めします。

もう一つ覚えておいていただきたいのは、スマートコントラクトは「止まる事なく稼働する」という事実を通じて、異なる経済主体間の信頼を促進することを最終目的としている限り、さまざまな業界や目的で使用できるということです。例えば、サプライヤーと小売業者間のスマートコントラクトは小売業者の倉庫や店舗に商品が供給されたことが確認された場合にのみ、サプライヤーに資金が支払われるという仕組みです。

長期的に見るとスマートコントラクトの開発は今後、優れたコード開発（開発者）、経済学に基づいたインセンティブ設計（経済学者）、法律を遵守する機能性（弁護士）の役割が非常に重要になります。したがって、スマートコントラクトを開発し、よりスマートなものにするためには学際的なアプローチが必要になるのです。
この点を検討した上で、今度はクロスチェーンに目を向けます。

クロスチェーンの台頭

Ethereumの大成功を受け、より多くの人々に採用されるようになり、複数のレイヤー1ブロックチェーンが誕生しました。しかし、このレイヤー1ブロックチェーンとは何を意味するのでしょうか？これまではこの区別を明確にすることは重要ではありませんでしたが、Polkadotについて詳しく学ぶにあたりレイヤーが何を表しているかを理解することは重要です。

レイヤー1ブロックチェーンは国境が封鎖された国に似ています。この国の中では信頼関係を必要とせず、すべての参加者の間で情報の行き来が可能です。なぜでしょうか？それ

は誤解を与える余地を持たず、即座に処理される法のような仕組みを用いてすでに運用されているからです。Ethereumのスマートコントラクトの導入によりレイヤー1ブロックチェーン（国）は複数のサブプロトコル（国家）を持つことができ、それぞれが途切れることなく通信できるようになりました。しかし、国境が封鎖されているため、このレイヤー1ブロックチェーンは外部との直接接続はできません。

初期のブロックチェーン採用者の一部によくある誤解は、ブロックチェーン業界がその使命を果たすためには単独のレイヤー1ブロックチェーンがあればよいというものです。このような見方はブロックチェーン導入に対して最大公約数的なアプローチをとる人々によって広められていることが多々あります。そのため「Bitcoin以外は真に非中央集権化されていない詐欺だ」という意見を持つ人も珍しくないでしょう。また、EthereumはBitcoinよりはるかに優れており、他のブロックチェーンは冗長であると言ってEthereumを賞賛する人もいます。このような人たちのほとんどは誤った情報を知っているか、自分が持っているトークンで儲けることだけに関心があるかのどちらかです。

実はブロックチェーン業界はマルチチェーン（複数のチェーンが相互通信可能）の未来に向けて準備されており、新しいブロックチェーンはそれぞれ既存のブロックチェーンが活用できる新しいアイデアを持ち寄っています。したがって、金融の非中央集権化に特化したブロックチェーンと、アイデンティティの非中央集権化に特化したブロックチェーンがあれば、汎用ブロックチェーンよりも連携しながらより効果を発揮することになるのです。この考え方を詳しく説明すると技術的な説明に飛び込むことになるので、今回は割愛します。要はインターネットを支配する単一のオンライン企業が存在しないのと同じく、「すべてを支配する単一のブロックチェーンなど存在しない」ということです。

現実には多数のレイヤー１ブロックチェーンがあり、それらが絶縁された国だとしたら、その絶縁された国同士をどうつなげばいいのでしょうか？この問題に対しては多くの解決策が考えられます。
例えば、Cosmos（コスモス）が追求する第一の方法は、すべてのレイヤー1ブロックチェーンに同じネットワーク環境を持たせ、チェーン間の情報交換を専用のブリッジを介して容易にするという方法です。ここでいうブリッジとは文字通り「他国への入り口」です。この方法は確かにチェーン間の問題については解決してくれますが、Ethereumと比較してみても最適な回答とは言えません。

Ethereumではスマートコントラクトは2つの異なる方法で、互いに作用できます。

1). トークンの送受信 ：スマートコントラクトはトークンを交換できる。
2). 指示を与える ：スマートコントラクトは他のスマートコントラクトにトランザクションの実行を依頼することができる。
これがコンポーザビリティの魔法とも呼ぶべき機能である。

このように、1つの取引やアプリケーションで異なるスマートコントラクトを使用でき、人間の介入なしに通信することができます。

Cosmosのチェーン間通信プロトコル内では、転送できる情報はトークンのみです。そのため、ブロックチェーン同士が特定の行動をとるような指示を出すことはできません。なので、このレベルの通信はやや原始的なもの（低レベルコンポーザビリティ）と見なしていいでしょう。スマートコントラクトが享受するような、より高いレベルのコンポーザビリティに到達するためには、レイヤー１より更に低いレイヤーが必要なのです。
そこで、いよいよPolkadotの登場です。

Polkadotは高いレベルのコンポーザビリティを損なうことなく、複数のレイヤー1ブロックチェーンを接続しようとする「レイヤー0」ブロックチェーンです。この仕組みを用いると、ブロックチェーンは互いに接続し、トークンを送信したり、互いの状態を変更することが可能になります。
またPolkadotは接続されたレイヤー1ブロックチェーンの独自の状態遷移機能を尊重します。それらのプロトコルはリレーチェーンの状態遷移に準拠する必要はありません。ただ、レイヤー1ブロックチェーンが実行しようとしている状態遷移の正当性を証明してもらうだけです。つまり、レイヤー0ブロックチェーンのPolkadotを（地球）と例えるなら、それに接続するレイヤー1ブロックチェーン（国）はその国の法律によって運営されます。必要なのは、これらの法律や変更が有効なものであることの証明の確認だけです。これが、リレーチェーンに接続されたパラチェーンに、独自のコンセンサスとファイナリティのメカニズムを開発する自由を与える設定となっています。

では状態の変更とは、実際にはどのような意味なのでしょうか？DeFIに特化したパラチェーンは分散型ID(DID)に特化したパラチェーンに保存されているユーザーのID情報を要求でき、そのDIDチェーン（パラチェーン）の状態を変更できます。DIDチェーンはこの要求を満たすために新しいトランザクションを実行する必要があり、その結果として状態が変更されます。トークンの交換は行われなくても、DIDチェーンが提供した情報はDeFiチェーンがユーザーへの支払いを行う際に使用できるため、より大きな価値が提供されたことになるのです。これは、ブロックチェーン技術がもたらす革新の中核をなす多くの例のうちの1つに過ぎません。

以上が状態の変更についての簡単な説明です。ここで、ブロックチェーンの革新について取り上げる前に、マルチチェーンの世界におけるもう1つの層、レイヤー2ブロックチェーンについて説明しましょう。レイヤー2ブロックチェーンは、レイヤー1ブロックチェーンを拡張するために作られました。具体的には、ブロックチェーンの速度を上げたり、容量を拡大すること等が挙げられます。例えば、Ethereumには少なくとも3つのレイヤー2ブロックチェーンがあり、Polygon、Arbitrum、Optimismの3つのプロトコルがEthereumを

拡張するために稼働しています。このような仕組みは、ブロックチェーンを理解するうえで必ずしも重要ではありません。しかし、レイヤー2ブロックチェーンがレイヤー1ブロックチェーン上で動作している、という事は重要なので覚えておいてください。

トークンこぼれ話

　なぜブロックチェーンにトークンが必要なのか、そしてその種類はどれくらいあるのでしょうか。
まず、すべてのブロックチェーンプロジェクトにトークンが必要なわけではありません。企業や法人が所有するプライベートブロックチェーンのほとんどは、トークンを用いずとも問題なく機能しています。ですが、パブリックブロックチェーンではトークンはオンチェーン上での取引の開始や取引手数料の支払いに必要で、これがなければスパム攻撃によってチェーンが停止してしまう可能性があるのです。このような理由から、Bitcoinブロックチェーンを使用するにはBTC、Ethereumを使用するにはETH、Polkadotネットワークを使用するにはDOTを手数料として支払います。また、PoS（プルーフ・オブ・ステーク）ネットワークでは、セキュリティのためにトークンが必要です。

重要なのは、すべてのトークンがユーティリティ・トークン（取引に使用されるトークン）ではないことです。一部のトークンには、プロジェクトの将来に影響を与える決定についての投票に使用できる「ガバナンストークン」があります。レイヤー1ブロックチェーンで運用されているほとんどのDappsは投票以外には実用性のないガバナンストークンを発行していますが、一部のガバナンストークンは（プロジェクトによって正確な仕組みは異なりますが）配当を得るために使用可能です。

なお、これら上記のトークンは、すべてfungible（代替可能）なトークンです。1つ1つのトークンには差がなく、どれも等しく同じように扱うことができ、このトークンは代替可能と言えます。つまり、常に何の支障もなく互いに交換ができます。しかし、ブロックチェーン技術における全てのトークンが代替可能であるとは限りません。中には代替不可能なものもあります。ここで「代替可能」が似たような性質を持つものと交換可能である、という性質を持つとすれば、「non-fungibility（代替不可能）」はアイデンティティを持ち、唯一の性質を有していることを意味します。したがって、NFT（Non-fungible token）とはブロックチェーンに追加される際に、1つのアイテム／オブジェクトが生成（鋳造）された際にユニークであるトークンのことを指します。ですから、通常は「NFT」はユニークなトークン／作品の集まりを意味します。

では続いて、ブロックチェーン技術の革新に注目してみましょう。

ブロックチェーンとWeb3.0：現在のWeb2.0を打破する

ブロックチェーンはその前に登場した多くのテクノロジーと同様に、現状の打破に挑戦することを望んでいます。知らぬ間に革新を進めた以前のテクノロジーとは異なり、ブロックチェーンは意図的かつ公然と革命を起こし、「信頼」に対する認識を変え、それを自動化しようとしているのです。人間中心の産業で、信頼を必要としないものはないでしょう。仲介者がいるところには、必ず信頼の問題があります。このように、多くの分野がブロックチェーンの利用によるイノベーションの機運にあります。以下に、現在ブロックチェーンによって再構築されつつある業界をいくつか紹介しましょう。

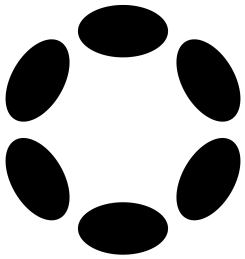
・金融
・ガバナンス
・プロパティ
・アイデンティティ
・データ
・サプライチェーン

この現状の打破の核心は既存のデジタル世界と新しいデジタル世界、つまりWeb2.0とWeb3.0の間の理念の違いにあります。まず、ユーザーが情報を画面越しに読むことしかできなかった時期はインターネットの段階で「Web 1.0」と呼ばれます。これは、電子メール、ニュースレター、**静的なWebサイト**が主体でした。

その後、エンドユーザーが**データを読み書きできる**ようになったWeb 2.0が登場しました。Web 2.0はソーシャルネットワークを拡大し、私たちのつながりを深めることで世の中に多くの恩恵をもたらしました。しかし、意図しない搾取が多く横行し、エンドユーザーに対する不平等や、ひいては虐待をさらに生む怪物にまで成長したのです。データ流出、ユーザー検閲、ユーザーデータの搾取など、挙げればきりがないほどです。

Web 3.0はWeb 2.0の欠点から生まれ、ユーザーが**データを読み、書き、所有できる**段階をもたらしました。Web3.0の「デジタル所有権」は、完全に定義されるまでに数十年はかかるであろう、まったく新しいパラダイムをもたらします。理想的には、Web 2.0とWeb 3.0のユーザーエクスペリエンスはエンドユーザーにとっては非常に似ていますが、開発者やプロジェクトの創設者は新しいトレンドに追いつくために鋭意努力しなければならないでしょう。エンドユーザーにとっては革命を支える理想を理解し、デジタル資産のセルフカストディ（資産を自身で管理する仕組み）のメリットとデメリットを理解することが真のチャレンジとなるのです。これについては、後ほど詳しく説明します。

ここで注目すべきは、Web3.0によってもたらされる再編成の規模です。理論的には思いつく限りのWeb2.0企業はWeb3.0の観点から再編成が可能です。Web2.0とWeb3.0の主な違いは所有権と自由にあることを忘れてはいけません。より公正で多様性を受け入れた組織に作り変えることができない業界はあるのでしょうか？このまま最適化されたものを見つけるのは不可能に近く、これこそがブロックチェーンによる革新が加速し続ける理由です。今のところ、すべてのブロックチェーンは上記に例えた国よりもまだ小さい「島」程度であるため、この前進は限られた範囲にとどまっています。
ありがたいことにPolkadotは最大限の力を発揮するための手段を提供しており、本書の残りの部分はそれが何であり、どのように最終目標を達成しようと計画しているかを説明することに専念します。



第一章

Polkadot入門

Polkadotは一見すると理解するのが難しいかもしれません。「他のブロックチェーンに接続する、スマートコントラクトを持たないブロックチェーン」という見慣れない概念に、即座に躊躇してしまう人もいます。最初の戸惑いを乗り越えた数人はオンチェーンガバナンス、フォークレスアップグレード、パラチェーン、クラウドローン、オークション、クロスチェーンメッセージングなど、他の複雑な要素とも向き合わなければなりません。Gavin WoodがYouTubeでエコシステムの設計を説明しているビデオ、ホワイトペーパー、Polkadot wiki、その他の役に立つリソースに助けられながら、一部の人々はこれを乗り越えようと決意しています。この知的探求の果てに彼らは皆、Polkadotが単純なブロックチェーン以上のものであることを知るのです。

Polkadotの特徴について学ぶために、まずセキュリティの観点から出発してみましょう。すべてのブロックチェーンネットワークは本質的に高いセキュリティを必要としますが、実現は容易ではありません。ここで言う「セキュリティ」とはネットワークのセキュリティと経済的なセキュリティの両方を指しており、以下の特徴が挙げられます。

- ブロックチェーンはリターンが大きい攻撃の標的（機密情報を保存する中央コンピューターなど）がほとんどないか、あるいは全くない、高度に分散化されたものである。これはネットワーク上の取引を検証するために、多くのマイナーやバリデーターが参加することにつながる。これらの数が少なすぎると、結託してネットワークに害を及ぼす可能性がある。

- ブロックチェーンは、ネットワークを攻撃することが経済的に困難なほど、大きな時価総額を持っている。

  例えば、あるブロックチェーンの時価総額（トークン1個あたりの価格に流通するトークンの総数を掛けたもの）が1500万ドルであれば、1500万ドルを預ける

> 余裕のある人なら誰でもネットワークを掌握できる可能性がある。また、ある人が大量のトークンを所有している場合、その人が持っているトークンを一度にすべて売り、安くなったところで買い戻すことで当該トークンの価格を暴落させることも可能である。これによって、ネットワークの時価総額が操作されてしまう。ネットワークに預けられたトークンの時価総額が、そのネットワークを攻撃するコストと等しいPoSネットワークでは、このような操作は難しいかもしれない。1500万ドルを持っていても、1500万ドル分のトークンを売ってくれる人を見つけるのは非常に難しいからである。

まとめると、新しいブロックチェーンを一から立ち上げるのは容易ではありません。どうすればさまざまなブロックチェーンを運用しながら、全体として同じレベルのセキュリティを確保できるのか？それが、Polkadotが解決しようとする最初の問題です。「他のブロックチェーンが接続できるマルチチェーン環境」を構築することで、すでに確立されたセキュリティの恩恵を受けることができます。言い換えれば、Polkadotは、すべての惑星（パラチェーン）が太陽（Polkadotのリレーチェーン）のエネルギー（セキュリティ）の恩恵を受ける太陽系を作り上げているのです。

2つ目の問題は相互運用性に関わるものです。前章で説明したように、DeFi（非中央集権型金融システム）はEthereumがスマートコントラクト間のシームレスな相互作用を可能にしたため、指数関数的に成長し（15ヶ月未満で総額500億ドルが預けられました）、魅力的な新しいユースケースと「好調なマーケットサイクル」を導きました。このように考えると、各スマートコントラクトは、国内であれば他の家の人でも自由にアクセスできる家とも言えます。例えるなら、パン屋がバターを必要とする場合、その使用人は許可を求めることなく料理人の家に駆け込んでバターを手に入れることができるのです。現実世界ではこれは窃盗と呼ばれる行為ですが、家自体がスマートコントラクトによって接続されたデバイスとみなすと、バターがパン屋の使用人に借用されていること、そしていずれは返却されることを把握できるのです。これは少々単純化しすぎた説明ですが、基本的なプロセスを上手く表しています。

個人の力は大したものではなくても団結することで大きな力となるように、ブロックチェーンもお互いに繋がり合うことでより高い性能を発揮します。各ブロックチェーンをインターネット・サービス・プロバイダーと考えれば、何故あるブロックチェーンがアイデンティティを扱い、別のブロックチェーンがコンテンツを扱い、他のブロックチェーンが銀行、ゲーム、プライバシーなどを扱いたいと考えるのか、想像に難くないでしょう。かつてのWeb1.0がそうであったように、ブロックチェーンの可能性は無限大です。特化した、異なるブロックチェーン間でより豊かな相互作用を生み出す機会を利用しないのは無責任であり、ここでPolkadotの出番となるわけです。TCP/IPが異なるノードを接続してインターネットを作ったのと同様に、Polkadotはそれぞれのブロックチェーンに接続することで、「ブロックチェーンのネットワーク」となるのです。

では、Polkadotとは何か？

Polkadotの中核は、他のブロックチェーンを接続するプルーフ・オブ・ステークのレイヤー0ブロックチェーンです。Polkadotの目標は、その接続されたすべてのネットワークに対して**スケーラビリティ、相互運用性、共有されたセキュリティ**を最適化することです。
ここからは各機能を順番に検討し、核となる問題が何であるか、そしてPolkadotがその課題をどのように解決するのかについて説明します。

セキュリティ共有の仕組み

複数の独立したチェーンのセキュリティ問題に対処するために、Polkadotは各チェーンがPolkadotとセキュリティを共有できる仕組みを提供します。各レイヤー1ブロックチェーンはPolkadotに接続することで、そのネットワークを保護するために自らバリデーターのセットと、十分に大きな時価総額を持つトークンを用意する代わりに、レイヤー0ブロックチェーンであるPolkadotのセキュリティを利用できるのです。実際にはPolkadotが100億ドルの時価総額を持つ場合、Polkadotに接続しているそれぞれのレイヤー1ブロックチェーンでも100億ドルの時価総額で担保されたセキュリティの恩恵を受けることができます。経済的なセキュリティに加えて、各チェーンはPolkadotの大規模なバリデーターセットからセキュリティを得ることになります。これはブロックチェーンにおいて初めての仕組みであり、これまでにない偉業であると言えます。

Interoperability：相互運用性

これがPolkadotのレイヤー0ブロックチェーンの最も注目すべき特徴です。ここまで、Dapps同士が自由に通信することで何が起きるかを説明しましたが、今度は異なるブロックチェーン同士が効率的に連携して、それを運用するとどうなるかという話です。今の時点ではイメージしにくいかもしれませんが、第5章やパラチェーンについての解説に進めばきっとイメージしやすくなるはずです。Polkadotの設計の大部分は、異なるブロックチェーン間の相互運用性を確保することにあるということだけは覚えておいてください。

Scalability：スケーラビリティ

ブロックチェーンは世界レベルの利用が推進できなければ、より高い公平性と包括性をもたらすことはできません。この問題に対するPolkadotの解決策は、ネットワークが異なるトランザクションを並行して実行できるようにする「シャーディング」（データベース

の負荷分散の手法の一つ）を使用することです。例えば、2021年時点でのEthereumはシングルシャードネットワークで、トランザクションが次々と処理され、すべてのノードがブロックチェーン全体のデータを保存する必要があります。シングルシャードネットワークでは性質は大きく異なるものの、すべてのトランザクションが同じシャードで実行され、Polkadotが採用しているマルチシャードネットワークではトランザクションはそれぞれのシャード内で並行して実行されます。この場合、各シャードは異なるブロックチェーンに対応し、DeFi取引はDeFiシャードで実行され、NFT取引はNFTシャードで実行されます。改めて、これは単純化した説明ですが、スケーラビリティのプロセスを理解するのに役立つはずです。

Polkadotでは、各レイヤー1ブロックチェーンが異なる用途に合わせてネットワークをカスタマイズできるため、効率的な並列計算(ネットワークが異なるノードで異なる種類の取引を処理する)を用いて、オープンな環境でスケーラビリティの問題に取り組むことができます。例えば、DIDに特化したパラチェーンは、DeFiに特化したパラチェーンと同じシステム設計を必要とすることはないでしょう。下記の方法によってネットワークはよりスケーラブル(より多くの処理を一度に行える)になるのです。

1). 各ネットワーク（パラチェーン）がその用途に最適化されていることを確認する。

2). 異なるトランザクションを並行して実行する。

例えば、ネットワーク上でトランザクションの有効性を検証するノードが1,000台あるとしましょう。1シャードモデルでは、1,000台すべてのノードが同じトランザクションを処理することになります。4シャードモデルの場合、ノードは250台ずつの4つのグループに分けられ、各グループのノードは異なる種類のトランザクションを処理します。グループAはDIDチェーン、グループBはDeFiチェーン、グループCはガバナンスチェーン、グループDはデータチェーンからのトランザクションを処理を行います。このように1,000台のコンピューターであっても、配置の方法次第でより多くのことを行うことが可能なのです。

フォークが不要なアップグレード

正直に言うと、私は嘘をつきました。チェーン間の相互運用性はPolkadotの特筆すべき点ですが、それだけではありません。
EthereumとEthereum Classicの問題を覚えていますか？あるいは、BitcoinとBitcoin Cashの過去の軋轢はいかがでしょうか？
これらは初期の、あるいは正規のチェーンがハードフォークによって核となるプロトコルをアップグレードする必要があったために起こったものです。フォークとはその名の通り

ある時点のステークホルダーに異なる道を提供するものです（詳細は第四章で解説）。フォークはネットワークにとって望ましい機能のように思えるかもしれませんが、「国民が投票内容について大きな議論をする度に、分断される国」というものを想像してみてください。この国はフォークのたびに人が去っていき、国はどんどん小さくなり、その度に国を支えるのに必要な人的資本が失われることになります。ここで、ブロックチェーンがデジタル国家に類似していることを考えると、長期的な成長にとってフォークはあまり理想的ではありません。ネットワークの長期的な繁栄のためには、コミュニティが自らを危険にさらすことなく課題を解決し、プロトコルをアップグレードする方法を見出すことが不可欠です。Polkadotはフォークを使わないアップデートを可能にしており、これがどのように行われるかについては第4章で説明します。

次の章でPolkadotの技術的な設計について説明をします。今のところ、Polkadotを特別なものにしている、いくつかの重要な機能を理解していただくだけで十分でしょう。その前に、Polkadotのエコシステムの「Chaos=カオス」なメンバーについて少しだけお話しします。

カオスなメンバー：Kusamaについて

本書ではPolkadotのみ言及し、Kusamaについては一切触れてきませんでしたが、この2つのブロックチェーンは技術的にも概念的にも深く結びついていることを理解することが重要です。
KusamaはPolkadotの試験的なネットワークだとみなされることが度々ありますが、実際はそうではありません。Kusamaは独自のオークションスケジュール、パラチェーン候補、ガバナンス、コミュニティを持つ、実際に稼働している独立したリレーチェーンです。また、KusamaはPolkadotエコシステムの開発を先導しています。そのためPolkadotに展開されているすべての機能は、何よりもまず先にKusamaに展開されます。KusamaはPolkadotの荒削りなバージョンであり、主にPolkadotが予期せぬ混乱や現実の行動を経験しないように保護するために存在します。

そしてKusamaのガバナンスシステムがPolkadotの4倍のスピードで稼働し、またDOTと比べてKSMの発行数は小規模であることを踏まえると、両者の主な違いはコミュニティの新陳代謝とトークノミクス（経済学的側面から見たトークンの設計）にあると言えます。このため、Kusamaのキャッチフレーズは「Expect Chaos =カオスを期待する」というユニークな表現になっています。なぜならKusamaのワイルドで実験的な世界では、次に何が起こるかわからないからです。

本書ではKusamaについてはそれほど言及していませんが、Polkadotについて述べる際には同様にKusamaについての説明でもあると思ってください。なお、本書の内容をPolkadotに絞ったのは、Kusamaを併記することによる読者の混乱を避けるためです。PolkadotとKusamaの両者を、エコシステムも含めを一言で言い表す際には、「DotSama」という言葉が用いられます。

第二章

Polkadotのネットワーク

「Polkadotは複雑だ」とよく批判されますが、この指摘はそれほど的外れではありません。しかし、この複雑さはリレーチェーンとパラチェーンという2つの主要な部分だけで構成される、シンプルな技術的構造の上に成り立っているのです。リレーチェーンはすべてのパラチェーンが接続する中心的なハブです。この短い章では、リレーチェーンだけに焦点を当てます。パラチェーンについては第5章で説明します。

写真イメージ：Polkadotのリレーチェーン

リレーチェーンとは

　リレーチェーンの目的を視覚化するために、円形のパイプ(リレーチェーン)があり、そこに他の多くのパイプ（パラチェーン）が接続されている様子を想像してください。これらの接続パイプはメインパイプと同じルールを持つ限り、どんな形でも、どんな機能でも提供できます。

リレーチェーンの主な機能は「接続するすべてのパラチェーンにセキュリティを共有し、相互運用性を提供すること」です。しかし、そのためにはまずリレーチェーン自体が可能な限り安全である必要があります。どうやってセキュリティを貸し出すか、つまり自分自身の安全を担保しながら、どのようにしてパラチェーンとセキュリティを共有すれば良いのでしょうか。リレーチェーンが自身のセキュリティを維持する方法を理解するためには、ブロックチェーンネットワークの2つの重要な側面を考慮する必要があります。

パブリックブロックチェーンは、その上でやり取りされる情報の流れ（検証であれ検索であれ）を誰もコントロールできないからこそ、重宝されるべき仕組みと言えます。つまり、新しいブロックが生成され、チェーンに接続される前に、ネットワークノードの過半数がその有効性に合意する必要があります。しかし、どの取引（データ）が有効であるのかについて、ノードはどのように合意するのでしょうか。これは「コンセンサス」と呼ばれるプロセスを経て行われます。

リレーチェーンのコンセンサスメカニズムの詳細については本書では専門的になりすぎるため、ここではある程度単純化した説明に留めておきます。Polkadotリレーチェーンの現在の機能では、「ハイブリッドコンセンサスメカニズム」を使用しています。つまり、プルーフ・オブ・ステークとプルーフ・オブ・ワークを組み合わせて、両者の長所を生かしているのです（第三章に詳細）。

一般論として、ブロックチェーンのコンセンサスには、ブロック生成とファイナリティという二つのプロセスがあります。ブロック生成とは新しいブロックを生成するプロセスを指し、ファイナリティとはブロックを検証してチェーンに封をするプロセスを指します。リレーチェーンであるPolkadotはすべての非中央集権型ブロックチェーンネットワークと同様に、そのコンセンサスを通じていくつかの問題を解決しようと試みています。

・悪質なノードにより共謀が行われた場合でも、少数の善良なノードによりチェーンのセキュリティが維持されるような堅牢性

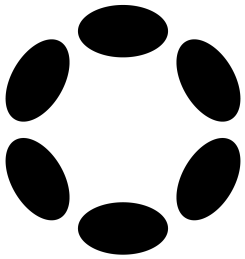
　つまり、悪質なノードによってチェーンが改ざんされた場合や、善良なノードが50%未満しか存在しない場合においてもチェーンの完全性が保たれることを意味

する。

・スケーラビリティのためのトランザクションの取り込みと検証のスピード
・ネットワークの回復力
ネットワークが頻繁にダウンしない、あるいは全くダウンしないこと。

・ネットワーク参加者のどのグループもネットワークを完全にコントロールできないような、より高度な非中央集権化。

これらのソリューションを全面的に成功させるために、リレーチェーンはBABEとGRANDPAを使用しています。両プロトコルの詳細な説明はPolkadotの入門書には必要ないと判断したため、詳細は巻末の技術的な付録をご覧ください。
次章では、リレーチェーンがバリデーター、ノミネーター、コレーターからどのようにセキュリティを得ているかについて見ていきましょう。



第三章

Polkadotネットワークのセキュリティ

Polkadotの技術的なセキュリティを理解した上で、次は「経済的」なセキュリティに目を向けましょう。Polkadotはどのようにして経済的なセキュリティを担保しているのでしょうか？この質問に答えるために、キーワードとなる「ステーキング」とネットワーク内の様々な役割について掘り下げていきます。

ステーキング（ステーク）とは何か

非中央集権型ネットワークはゲーム理論の概念を用いて、ネットワーク参加者全員の行動を一致させるための役割、責任、インセンティブが存在するシステムを設計することにより、多くの参加者の協調を実現します。これは、多くの非中央集権型システムでトークンが必要とされる主な理由の1つで、経済的報酬が究極のインセンティブメカニズムとなるのです。Bitcoinの場合はBTC、Ethereumの場合はETHがそれにあたります。このように、ブロックチェーンのセキュリティの強さはプログラムされたコードの品質だけで決まるわけではありません。インセンティブとトークンの設計の質によって定義されるのであり、その核心はゲーム理論にあります。例えば、Bitcoinではすべてのマイナーが BTCの報酬を得るためにブロックを生成し、検証します。Bitcoinのようなプルーフ・オブ・ワーク(PoW)方式ではネットワーク参加者の役割は少なく、マイナーに限定されます。この場合、ネットワークに必要なのはノードとBitcoin、そしてユーザーだけだからです。

プルーフ・オブ・ステーク(PoS)方式では大抵の場合、ノードに加えてネットワークを保護するために一定額以上のステーキング（資金を預ける）ユーザーが必要です。また、最低額が決まっていないチェーンも存在します。いずれにせよPoS方式ブロックチェーンは技術的セキュリティと経済的セキュリティの両方に依存しているため、経済が外部要因となりこのセキュリティに影響を及ぼす、ということを覚えておいてください。PoW方式ブロックチェーンのセキュリティはそれを確保するノードの数だけ強固になりますが、PoS

方式ブロックチェーンのセキュリティはそのノード数とステーク（預けられた資産）の価値に依存します。このように、PoSブロックチェーンでネットワークのセキュリティを高めるプロセスをステーキングと呼びます。PoSがPoWに勝る主な利点は2つありますので、以下に見ていきましょう。

・PoSはPoWに比べ、エネルギー消費量が圧倒的に少ない

これは私たちのテクノロジーが気候変動に与える影響が大きくなっているため、非常に重要なポイントです。PoWが実際にどの程度環境に影響を与えているかについては議論の余地がありますが、例えば米国海洋大気庁のデータによると、近年温暖化の傾向が見られます。(注)

・PoSはネットワークセキュリティにコミュニティがより深く関与することで、より大きな非中央集権化を実現する

これはPoWがネットワークセキュリティの責任を、ノードを運営する手段や技術に精通した人々に移行させているからです。このため、時間の経過とともに必然的に中央集権化の度合いが高まっていきます。

Polkadotネットワークの場合には「バリデーター」「ノミネーター」「コレーター」の3種類のネットワーク参加者がいます。

バリデーター

PolkadotのバリデーターはBitcoinのマイナーのようなものです。彼らはトランザクションの処理と検証、ブロックの生成、ブロックチェーンの履歴の保存を行うノードを運営しています。彼らがいなければ、ネットワークは成り立ちません。注目すべきポイントは、以下の通りです。

・ネットワークが稼働する物理的なインフラを提供する。
・バリデーターは常にオンライン状態である必要がある（特に、新しいブロックを生成するのがバリデーターの場合）

バリデーターの作業は関連するコンピューター機器を入手し、Polkadotのコードを実行するだけという簡単なものです。ノードが設置されると、ほとんどの作業が自動化され、バ

リデーターはトラブルシューティングと接続性の維持に専念できるようになります。また、バリデーターは経済的・物理的な貢献に対して、DOTトークンで報酬を得ることができます。ネットワーク上のバリデーターの総数はネットワークの需要に応じて調整でき、最初は数名から始まります。現在は297名に達しており（2022年1月現在）、目標はバリデーター数が1,000人に到達することです。

この数字を見てBitcoinが2万人以上、Ethereumが1万人以上のマイナーを抱えていることを考えると、非中央集権化を支えるのに十分な数字なのだろうか？と思う人もいるかもしれません。なぜ1,000人のバリデーターで十分なのかを理解するためには、Polkadotのコンセンサスの仕組みを念頭に置く必要があります。Polkadotでは、ノミネーターがPhragmén方式を通じて候補からバリデーターを選出することで、バリデーター間による共謀の可能性を制限しています。
また、Polkadotは1,000人のバリデーターを対象にしていますが、これはバリデーターになる資格を持つ人が1,000人しかいない、ということを意味しているのではありません。むしろ、ブロックの生成と検証を1,000人のバリデーターが同時に行い、それ以外のバリデーターはバリデーター候補として活動するという意図も含まれています。
多くのバリデーターを必要としないことは二酸化炭素排出量を減らすだけでなく、スケーラビリティを実現する上でも有効なのです。もし13,000人のバリデーターがいて、アクティブセット（現在ネットワークコンセンサスに参加しているバリデーター）の2/3のバリデーターが同意しなければならないとすると、各取引は処理される前におよそ7,500人のバリデーターを待つ必要があり、これは必然的にネットワークの速度を低下させることにつながります。

非中央集権化の目標はできるだけ多くのバリデーターを持つことではなく、できるだけ多くのネットワーク参加者を持つことであり、所有権、権力、権威の分散化が重要なのです。大半のユーザーはノードを運営する手段も技術も持っていないため、PoSがより望ましいシステムであるのはこのためです。もしネットワークのセキュリティがバリデーターやマイナーによってのみ提供されるのであれば、コミュニティの大部分が取り残されることになります。PoSではコンピューターやコーディングについて何も知らない一般人でもネットワークのセキュリティにおいて中心的な役割を果たすことができ、さらに報酬も得ることが可能です。これに対し、PoW方式ブロックチェーンでは技術者やマイナーを中心に所有権と権力、権威が集中する傾向があります。PoSにおいてはステーキングの仕組みを用いてより強力な非中央集権化を促進することが目的となっているのです。

続いて、Polkadotがどのようにしてこの目的を達成しているかを理解するために、ノミネーターの役割を探ってみましょう。

ノミネーター

本書をお読みになっている方は既にノミネーターであるか、あるいはなろうとされている可能性が高いと思われます。ネットワークセキュリティを高める上で、ノミネーターの役割はバリデーターに比べると技術的な面でははるかに容易です。
なぜなら、バリデーターはノードを動かすという重要な仕事がある一方で、ノミネーターはバリデーターをサポートするためにトークンを一定期間預けるだけで良いのです（バリデーターのウォレットに資金を送金するわけではありません）。

バリデーターに選出されるために必要な資産は高額で（現在140万DOT）、バリデーターは他の多数のノミネーターからの委任、つまりトークンの継続的なサポートを確保して初めてその役割を担う資格を得ます。バリデーターに対する報酬はバリデーターとノミネーター間で分配されますが、この分配率はバリデーターが設定するものとなっています。報酬からバリデーターへの報酬分を差し引いた額が各ノミネーターに支払われますが、これは該当のバリデーターに対するステーク比率に応じて分配されます。

他のPoSシステムではノミネーターが選択できるのは1人のバリデーターのみですが、Polkadotではノミネーターが最大16人のバリデーターを選択できる高度なメカニズムが採用されています。この中から1eraという単位（Polkadotではおよそ1日）毎に行われる選挙で、アクティブセットに入ることができるのは数人のバリデーターだけです。
16人の有効候補者を選ぶことで、ノミネーターは最大の報酬を得るチャンスを得ることができます。これはトークンをステークするリレーチェーンが最大限のセキュリティを確保するために、すべてのノミネーターとバリデーターに対してステーキングプロセスを最適化するプロトコルを備えているためです。この詳細はあまりに専門的なので、その中核的な機能性の基本的な要約のみを以下に記述します。

＜ノミネーターの参加を最大化する＞

このアルゴリズム（プロトコル）は各eraにおいてノミネーターがバリデーターを少なくとも一人選択することにより、ノミネーターのコンセンサスへの参加を最大化します。eraとはブロックチェーンにおける時間の尺度であり、私たち人間の一日のようなもので、生成されたブロックの数で表されKusamaでは約6時間、Polkadotでは約24時間です。ノミネーターが16人のバリデーターを選択した場合、このメカニズムにより16人のうち少なくとも1人がアクティブセットに含まれることが保証されます。

＜一元化のリスクを最小化する＞

　これはゲーム理論によって証明されていますが、人間は最も確実なものを求める傾向にあり、すべての選択肢の中で最も人気のあるものを選びがちです。たとえば、多くのノミネーターがあるバリデーターを選択すると、他のノミネーターも同じバリデーターを選択するでしょう。そして、このようにバリデーターが本来求めていた以上の力をネットワークに対して持つことになり、中央集権化が起こるのです。このリスクを軽減するために、ステーキングプロトコルではステーク（預け金）の量やノミネーターの数に関係なく、すべてのバリデーターに等しい報酬が支払われます。

しかし、多くのノミネーターを持つバリデーターは、全体としてステークされたDOTあたりの報酬が少なくなります。結局、これらの人気バリデーターに対して最も多くのDOTを預けているノミネーターのみが最大の報酬を得ることができ、仮にあなたがこのバリデーターに少額のDOTしか預けていないノミネーターだとすれば、報酬はかなり少なくなります（または全く報酬がない場合もありますが、そのバリデーターがどれほど委任されているのかによって結果は異なります）。そのため十分な報酬を得られように各自がノミネート先を最適化しようとすることに繋がり、ノミネートは時間の経過とともに変化していきます。これは、すべてのノミネーターが常に自分のノミネート先を見直し、ネットワーク参加に対して最大の報酬を得られるよう強制する仕組みとして設計されています。

＜ノミネート（委任）の方法＞

　ノミネートの最初のステップは、DOTトークンを取得することです。そのためには、アカウントとウォレットが必要です。ウォレットはPolkadot-JS、Fearless、Talisman、Nova、Polkawallet、その他多くのエコシステムウォレットを使用することができます。一つ覚えておいてほしいのは、資金を預けると約28日間の強制的な "unbonding “期間に該当することです。つまり、ステークして預けた資産のロックを解除して、トークンを引き出すことを選択した瞬間から、実際にトークンを取り戻すのに約28日間かかるということです。

この不便さを避けるために、中央集権的な取引所の中には出資金を即座に引き出すことができるところもあるので、より自由度の高い手段で参加することができます（ノミネートの代理店の様なもの）。より望ましい解決策は、DOTをステークする際にデリバティブトークンを与えてくれる「非中央集権型プラットフォーム」を利用することです。例えば、Acala（詳細は後述）のプロトコルを使用すれば、DOTをステークし「liquid DOT」の略であるLDOTを受け取ることができます。DOTと債権トークンであるLDOTの違いについてですが、LDOTはエコシステム全体のDeFiプロトコルで使用可能であり、LDOTを用いたステーク報酬を得る事ができます。そのためLDOTを運用後にDOTに交換し直した場合、以前よりも多くのDOTを保有することが可能です（あくまでも資産運用の一例です

ので、必ずしも利益を得るだけでなく、損失を被る可能性もあります）。このような機能を持つトークンはLDOTだけではありません。同じく「リキッドステーキングサービス」を提供するパラチェーンは他にもありますが、その場合のトークンの名前は異なります（BifrostのvDOTとParallel FinanceのxDOT等がその例です）。

ノミネートの実際の作業は、16人のバリデーターを選択することにあります。前述の取引所などのプラットフォームを通じてステークを行っている場合はこのプロセスを経る必要はありませんが、もしあなたが自分でステークをしているのであれば、正しいバリデーターを選択する方法を学ぶ必要があります。

・正しいバリデーターを選択する

適切なバリデーターを選択することは非常に重要なプロセスです。もし悪意のあるバリデーターを選んでしまったら、せっかく稼いだトークンを失うという悲劇的な事態に直面するでしょう。正しいバリデーターを選択すべきもう一つの理由は、ステーク報酬を最大化するためです。バリデーターによっては、選択次第で他のバリデーターよりも多くの報酬を得ることができるものもあり、自分の報酬を最大化することがあなたのすべき事です。ではどうすれば正しいバリデーターを選択できるのでしょうか？

・バリデーターの「Skin in the Game」

もし何かを選択する事で失うものがあるならば、誰しも悪意を持った選択や不注意な状態での選択は避けらるはずです。この考えは「Skin in the Game」とも呼ばれ、バリデーター選択の際にも当てはまります。裏を返せば、もしバリデーターが自分の手元にトークンを持っていないなら、失うものは何もないということです。一方で、もしバリデーターとしての活動が報われた場合、彼は多額の報酬を手にすることができるのです。したがって、自身によるステークがない、あるいはステークが少ないバリデーターを選ぶのは得策ではありません。 ただし、そのバリデーターが悪意や不注意で行動することはないと信用する（信用できる）場合はこの限りではありません。

・バリデーターの身元を確かめる

仮にネットワーク上の誰もがあなたの身元を知っている場合、きっと、悪意ある行動を取る事は困難なはずです。もちろん、この方法ですべてのバリデーターの過ちを防げるわけではありませんが、信頼できる経験則として有効と言えるでしょう。自分のアイデンティティをオンチェーンで表示する人は、そうでない人よりも信頼できます。なぜなら、その人の評判がかかっているからです。また、オンチェーンのIDを持つ人に対して取引に不安がある場合、その人に連絡を取って状況を確認することができます。しかしこの方法

も万能では無く、一部の怪しいバリデーターは古いIDから新しいIDへ乗り換え、新しいバリデーターアカウントを立ち上げることがありますので、一筋縄ではいきません。その場合、おそらく元のIDと同じ情報が記載されており、いくつかの詳細が変更されているだけでしょうから、情報の精査が必要です。

・バリデーターの手数料に注目する

　より大きな利益を得るためには、手数料が最も低いバリデーターを選択することが賢明な判断です。手数料が50％に設定されているバリデーターは報酬の50％を受け取り、50％をノミネーターに分配することになります。手数料が10%の場合、バリデーターは10%の手数料しか取らないので、後者の方がノミネーターにとってより収益性が高くなります。

・バリデーターの過去の行為を参照する

　過去の実績に基づいて、その人物や団体を判断するのは自然なことです。バリデーターの場合、過去に何度も悪意ある行為をしたことのあるバリデーターを指名することは避けましょう。しかし、時にはバリデーターが、自己の過失ではなくとも知らぬ間にその様な行為の被害者になることがあります。ネットワークは時として、誠実で勤勉なバリデーターがペナルティを受けるような問題に遭遇することがあるため、何が起こっているのかを注意深く観察しなければなりません。

その他、バリデーターを安全に指名する方法については、こちらのガイドをご覧ください。

コレーター

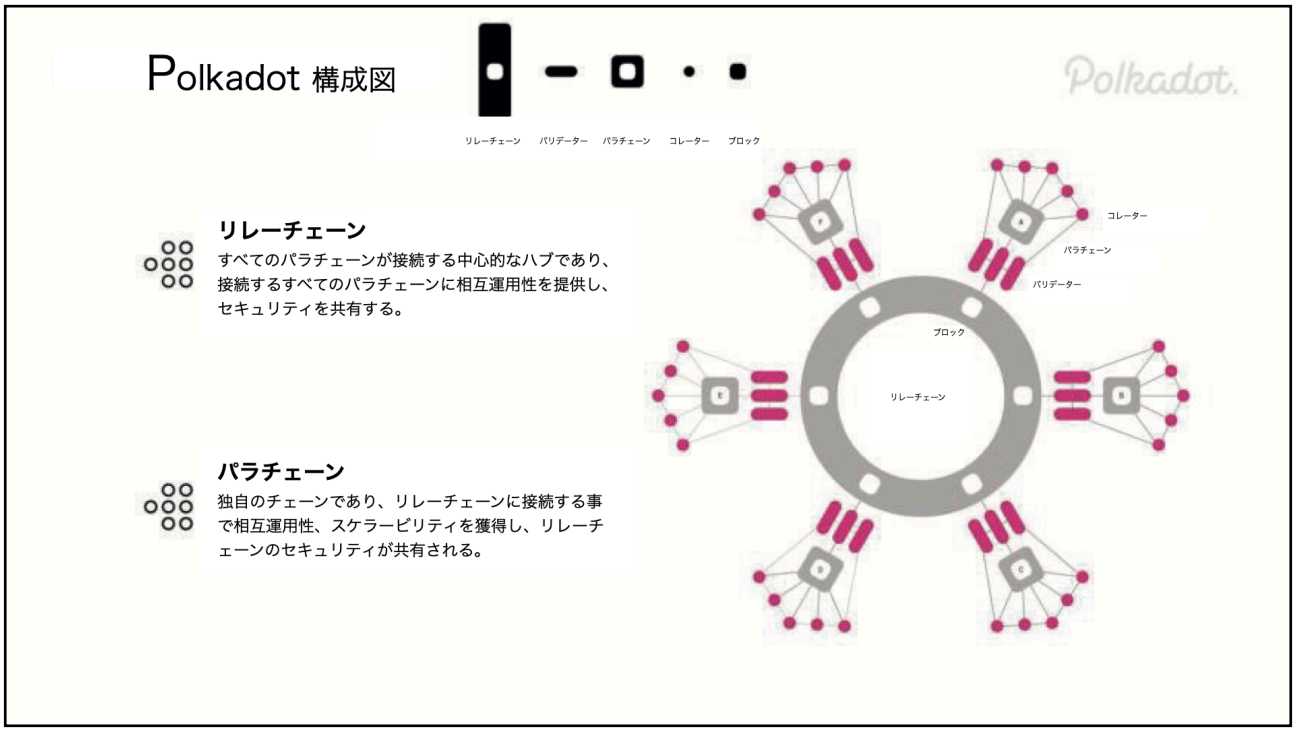
　バリデーターがリレーチェーンのブロックを生成・確認するのに対し、コレーターはパラチェーンのブロックを生成・確認する役割を持ちます。パラチェーンでもリレーチェーンと同様のメカニズム(BABEとGRANDPA)が用いられていることに留意して下さい。

コレーターはリレーチェーンと同様にパラチェーンのフルノードを実行しなければならないので、コレーターをパラチェーンのバリデーターと考えることができます。パラチェーン上のコレーターが新しいパラチェーンブロックの生成に合意すると、そのブロックをリレーチェーンのバリデーターに転送し、リレーチェーンに組み入れるようにします。このようにして、コレーターが送信した検証済みの取引ブロックはバリデーターによってさら

に検証され、リレーチェーンに追加されます。リレーチェーンのバリデーターはパラチェーンにランダムに割り当てらます。

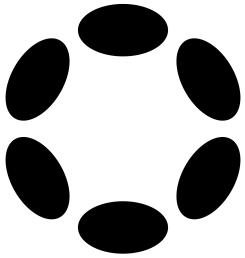
例えば、x番目のブロックにおいて最初の期間（epochと表記され、約 4 時間）ではバリデーター V1、V2、V3 はパラチェーン A に割り当てられているとしましょう。これは、パラチェーンAのコレーターがトランザクションをV1、V2、V3に転送することを意味し、その他のバリデーターは他のパラチェーンからのトランザクションを検証することができます。

これらのバリデーターは検証が終わると、検証済みの取引をリレーチェーン上の他のバリデーターに提案し、さらなる検証を受けてから、その取引をリレーチェーンに追加します。実際にはこの作業はほとんど自動的に行われています。バリデーターは、自分がどのパラチェーンで作業を行うかを事前に知ることはできません。epochの終わりには、バリデーターV1、V2、V3はパラチェーンAから移動し、新しいバリデーターが次のepochでパラチェーンAの取引の検証を行うことになります。このプロセスは、コレーターとバリデーター間の共謀のリスクを最小化し、封じ込めることで、ネットワークセキュリティを強化することが目的です。例えば、あるeraまたはepochで悪意ある攻撃があった場合、この攻撃は次のeraの初めに誠実なバリデーターによって対抗されることになります。



イメージ図：バリデーター、ノミネーター、コレーターの構成図

(注). 出典：米国海洋大気庁(National Oceanic and Atmospheric Administration 2021年1月)。2020年は2016年に次いで地球で2番目に暑い年だった。https://www.noaa.gov/news/2020-was-earth-s-2nd-hottest-year-just-behind-2016. アクセス日：2021-08-31.



第四章

Polkadotのガバナンス

ハッキングがもたらしたもの

　2016年、今でいう「DAOハッキング」により6000万ドルものETHが盗まれるという驚くべき事件が発生しました。下記にその経緯を簡単にまとめます。

2016年4月、多くの人々がETHトークンをスマートコントラクトに預け入れ、暗号資産エコシステム初期の非中央集権型自律組織（DAO）に資金を提供しました。このクラウドファンディングでは、1億5000万ドルが調達されましたが、それから3カ月も経たないうちにスマートコントラクトがハッキングされ、悪質なハッカーが資金を流出させ始めたのです。コミュニティはパニックに陥りました。ほどなくして、ホワイトハット（善意で集まったハッカーの集団）が出現し、共同で犯人の行為を止めさせようとしました。ハッキングの詳細については、本書では専門的になりすぎるため割愛しますが、ブラックハット（同じく悪意あるハッカー集団）がスマートコントラクトのコードの欠陥を利用したことは明らかです。設計上、攻撃を行なっているハッカーは非常にゆっくりとしかトークンを引き出せないため、ホワイトハットハッカーの集団は最終的にこの悪用を阻止する方法を見つけ出すことができましたが、この救助隊は、最終的に泥棒がお金を持ち逃げできるような失態を犯してしまったため、コミュニティに残された唯一の解決策はチェーンの状態を攻撃前に戻して、今回の出来事をなかった事にするという方法だけでした。

Ethereumコミュニティの目と鼻の先でこの様な盗難事件が起こったことを考えると、正しい選択を決めるのは簡単な結論だと思われるでしょう。しかし、事態はそう安易なものではありませんでした。
まず、コミュニティはEthereumのユーザーが次に何をすべきかについて投票する方法を考えなければなりませんでした。というのも、当時、ブロックチェーンのデータは暗号に

よって封印された不変のものであり、チェーン上で起きたことは決して元に戻せないというのが一般的な認識だったのです。しかし、今回は6,000万ドルが盗まれたため、描いた理想も結局は現実と向き合わなければなりません。そして、その現実とは、Ethereumのブロックチェーンに保存されている情報を変更するという事を意味しました。

結果、2つの陣営が生まれました。一方は、チェーンを攻撃前のブロックに戻すことで、盗難の履歴を消そうとするもので、こちらが多数派。一方、非中央集権を掲げる純粋主義者はEthereumのブロックチェーンの不変性に手を加えることに反対します。遂にはコミュニティ内で投票が実施され、ユーザーの80％がEthereumのブロックチェーンの歴史からハッキングを抹消することに票を投じました。しかし、そのためにはブロックチェーンを更新し、元のコードを書き換える「フォーク」を作成する必要があり、フォークを実行するにはネットワーク上のすべてのノードが新しい状態に書き換えられ、新しい方向に進むことができるようにアップデートを受け入れる必要がありました。こうしてアップデートが実行されると、ハッキングの痕跡はすべて消え、ほとんどのコミュニティメンバーは「善行こそが勝ち、泥棒の手元には何も残らないだろう」と喜んだのです。

しかし、Ethereumネットワークが新しいチェーンに分岐し、日々新しい歴史を刻んでいるにもかかわらず、アップグレードに従わないノードが存在することがすぐに明らかになりました。基本的に、彼らは古いEthereumの正規（彼らから見て）のチェーンに留まることを選択し、そこには盗難の記録も残っていたのです。するとすぐに、新たなパニックが起こりました。ノードオペレータは意図的にこれをやっているのだろうか？ハッカーの仕業なのだろうか？マイナーに接触する試みがなされ、結局理由は不明だが意図的な行為である、ということが明らかになり、フォークを拒否した古いチェーンは、Ethereum Classicとして知られるようになりました。この話は、2020年8月に発売されたマシュー・ライジング氏の著書『Out of the Ether』で詳しく知ることができます。ここではPolkadotのオンチェーンガバナンス設計とフォークレスアップグレードの重要性を強調するために、このちょっとした歴史を掘り下げることが必要なので触れました。

EthereumがEthereum Classicにフォークすることの何が大きな問題なのだろうか？と思うかもしれません。非中央集権化の観点からは、すべてのネットワーク参加者にフォークが適切かどうかを選択する自由を与えることは理にかなっており、それによってチェーンの整合性が保たれます。しかし、それはコミュニティにとって他の重要なリスクももたらします。少数のマイナーがEthereumネットワークとのコンセンサスを破棄し、古いチェーンに留まることを選択したとき、3つのレベルでEthereumのセキュリティは損なわれました。

1). ネットワーク上のマイナーが減少した
2). ETHの価格が暴落し、その価値が影響を受けた
3). ハッキングと予期せぬフォークにより、コミュニティの信頼が揺らいだ。

悲しいことに、ブロックチェーンネットワークの歴史の中で起こった論争的なフォークはこれだけではありません。Bitcoinでも起こりました。BitcoinのコミュニティがBitcoinのブロックチェーンの速度について議論になり、ネットワークを拡張し、1ブロックに収まるトランザクションの数を増やすためのさまざまな方法を提案したことが始まりです。ある陣営は、ブロックサイズを8倍にして、1秒間に処理できるトランザクションを8倍多くすることを望んでいましたが、この場合ネットワークはより大きなブロックが埋まるのを待つことになるため、ブロックの検証時間が10分を超える事になります。また、そもそもBitcoinのプロトコルを改ざんすることは異端である、と考える者もいました。
そこで、結果的にBitcoinネットワークの一部がフォークして、Bitcoin Cashという新しいネットワークになり、既存のコードを更新してブロックサイズの増加を可能にしたのです。長年にわたり、Bitcoinは他の多くのネットワークにフォークされてきましたが、これらのフォークを保証するマイニングパワーは、ますます少数の、大規模なマイニングプールの担い手に集中しています。

そのため、これらのフォークされたネットワークはBitcoinと同じ価値を提供できず、十分なネットワーク参加者を集めることができないため、容易に攻撃される可能性があります。なぜなら、非中央集権型ネットワークのパワーは、そのコミュニティの強さ（人数と参加レベル）にあるからです。

現在のBitcoinとEthereumを見ると、これらのフォークはネットワークに何の影響も与えていないように見えますが、実際はそうではありません。このような論争的なエピソードがあるにもかかわらず、両ネットワークがここまで発展してきたのは、その設計がベストなものであることの証明にはならないのです。むしろ、すべてのブロックチェーンネットワークに内在する問題点を指摘しているとも言えます。もし、コードを誰でも見ることができ、コピーすることができるのであれば、簡単にフォークすることができます。そして、何度もフォークすれば、そのネットワークのセキュリティに度重なるダメージを与えることができます。なぜなら、フォークするたびにマイナーやコミュニティのメンバーが引き離され、ネットワークの価値やコンセンサスパワーが失われることになるからです。

では、どうすればネットワークとそのコミュニティを弱体化させないようにできるのでしょうか？Polkadotの答えは、すべての参加者が信頼できるオンチェーンガバナンスプロセスを提供することです。フォークレスアップグレードと組み合わせることで、壊滅的な影響を受けることなく、簡単にアップグレードできるブロックチェーンになるのです。その方法を理解するために、まずはPolkadotのガバナンスメカニズムを学んでみましょう。このセクションでは、Q&A形式で進めます。

Polkadotのガバナンス

1.ガバナンスは何のためにあるのですか？

　どのようなシステムにおいても、ガバナンスの主な目的は、システムのパラメータを変更することです。国に例えるなら、新しい法案や憲法の改正がこれにあたります。Polkadotの場合、これらはオンチェーンデータになります（以下例）。

・ユーザー残高の更新（キーの盗難や紛失の場合など）
・ランタイムの更新
・パラチェーンやパラスレッドの接続・切断

2.ガバナンス体制はどうなっているのですか？

　Polkadotのオンチェーンガバナンス構造は評議会、技術委員会、コミュニティ（投票可能なDOTを保有している人々の総称、「referendum chamber」とも呼ばれる）の三者から構成されています。それぞれについて詳しく見ていきましょう。

i.評議会

　すべてのDOTホルダーを代表する6〜24人のメンバーで構成されるグループです。主な目的は、Polkadotネットワークに新しい方向性を与えることを目的とした提案を検討することです。

＜評議会の執行範囲＞

・技術委員会メンバーの選出

・評議会の提案に対する投票 - すべての提案（referendum:レファレンダム＝国民投票、Treasury:財務、bounty:報奨金、tips:チップ）は、次の段階に移る前に、評議会によって明確に可決/否決される必要がある。ただし、コミュニティ主導の提案だけは例外となる。

・提案がエコシステムにとって相応しく無いと判断された場合、レファレンダムの拒否権を行使する。但しその拒否権は別の一般投票によって覆すことができる。

・技術的な緊急事態が発生した場合、レファレンダム（全DOTホルダーが参加できる投票）が迅速に行われる。

＜評議会メンバーの選考方法＞

　DOTを保有していれば誰でも立候補は可能です。評議会に参加したいDOTホルダーは、自らを推薦し、十分な票を集める事で選出され、評議会メンバーになることができます。DOT所有者はバリデーターを選ぶのと同じように、トークンを預ける事で自分たちに代わってネットワークを統治するメンバーを選出することができます。このように、評議会メンバーは投票者の支持によって選ばれるため、希望者は、DOT保有者に対して宣伝キャンペーンを積極的に行う必要があります。

2週間ごとに選挙が行われ、縁故採用を防ぐために評議会の構成が入れ替わります。これは受動的な参加者が自分のDOTの投票権を、管理する意思のある他のメンバーに委譲するよう促すことで、コミュニティのガバナンスへの参加を促すためのものです。しかし、これはあくまで理想的なシナリオです。現実には、議員の候補者が少ないことと、有権者が希望する候補者のリストを変更することがほとんどないため、同じ議員が何ヶ月もその席に留まることが度々見受けられます。

＜投票の仕組み＞

　評議会メンバーの選出は、ステーキングで実装されているのと同じメカニズムで行われます。しかし、預けられたトークンの比重に依存するため、時間の経過とともに、ネットワークが「クジラ」と呼ばれるDOT数の多いユーザーを優遇する可能性があります。この問題に対する完璧な解決策は今のところありませんが、Polkadotで使用されているPhragmén方式は興味深い解決策を提供しています。というのも、そのアルゴリズムは各候補の背後にあるトークンウェイトを考慮しつつも、その情報だけでは判断を下さないからです。その代わり、次のような理想的なシナリオを想定して結果を最適化します。

1). 経済的な安全が最大限保証されるように、預けられた総額を最大にする。

2). 最小限のステークを持つバリデーターの背後にあるステークを最大化し、すべての候補がアクティブセットへのアクセスを許可するバッカーを獲得するために競い続けるようにする。

3). 報酬の分散を最小限にし、最高額のバリデーターと最低額のバリデーターの間にあまり大きな差が生じないようにする。

Phragmén方式はあらゆることを考慮した上で、一定の公平性を作り出すために適切な働きをしています。その内部構造を理解するためには、このWikiの記事をご覧ください。

ii.技術委員会

技術委員会は、Polkadotのコードベースに貢献した開発者で構成されています。彼らは、ネットワークが円滑に動作するようにすることを任務としています。

＜技術委員会の役割＞

・評議会への提案
・技術的な緊急事態が発生した場合、提案を迅速に行うことができる
・レファレンダムがPolkadotのセキュリティに危険を及ぼす場合、評議会に勧告し、レファレンダムを拒否する。

＜技術委員会の参加者＞

技術委員会へのチームの追加や削除は、評議会の多数決によって行われます。

iii.コミュニティ

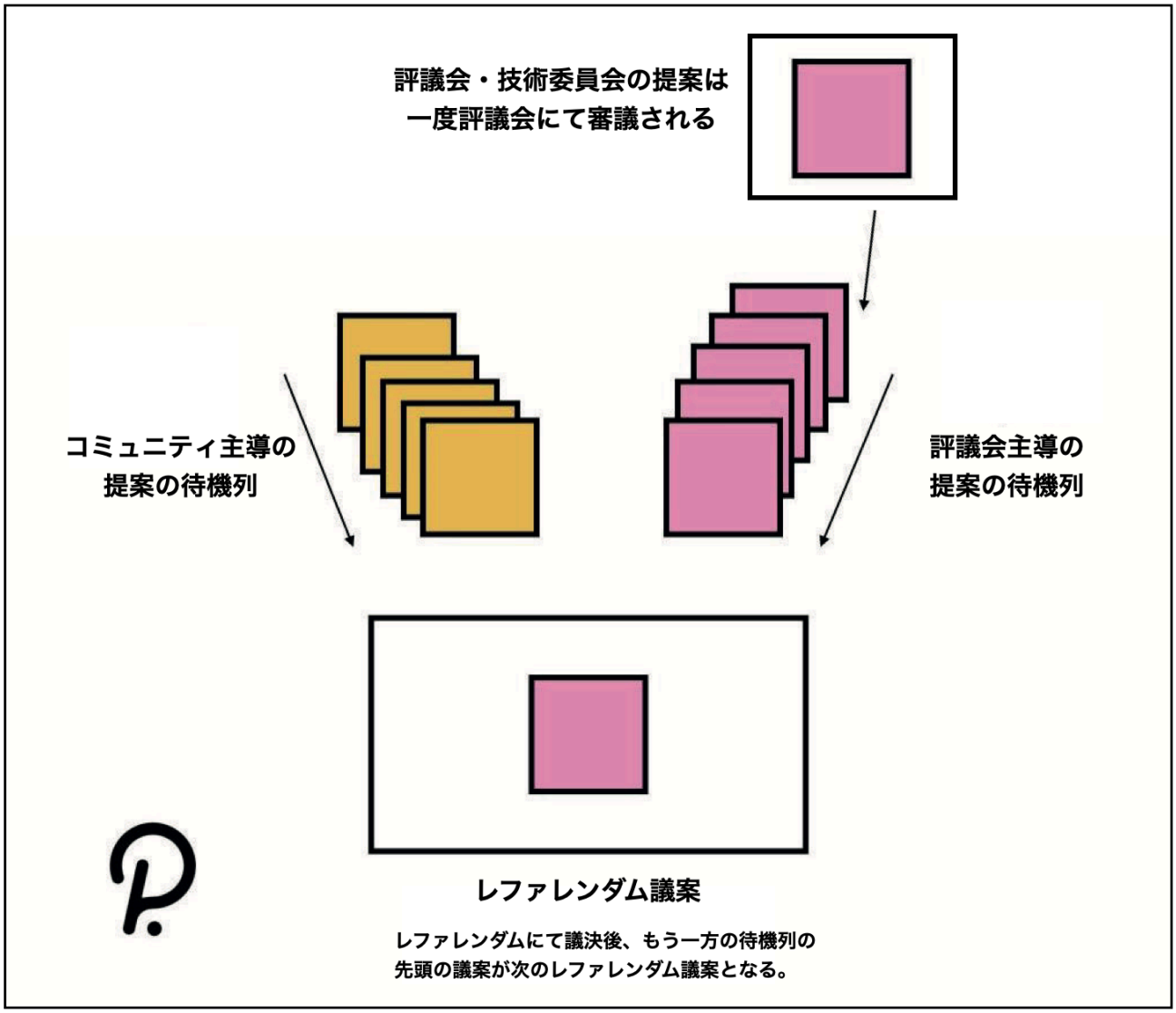
DOT所有者で構成されており、以下の活動に参加できます。

1). 評議会メンバーの推薦
2). 議案の提出
3). レファレンダムの実施

3. 意思決定はどのように行われるのですか？

Polkadotの方向性についてなされるすべての決定は、「Proposal=提案」から始まります。提案は、3つのガバナンス機関のいずれによっても行うことができますが、技術委員会の提案は、評議会に提出され、評議会はそれについて投票します。その提案が可決されると、レファレンダムへ移行します。一方、コミュニティからの提案は全ての投票サイクル（Polkadotでは約28日間）ごとに、最も多くのトークンに支持された案がレファレンダムへと進みます。このように、提案はコミュニティ主導の提案と評議会主導の提案の2種類があります。
ただし、技術委員会が補足的な提案を迅速に行う必要がある緊急事態を除いて、レファレンダム1回につき1つの提案しか行うことができません。

２種類の提案は別々のキューで管理され、少なくともいずれかのキューに1つの提案がある前提で、交互に投票が行われていきます。もし前回の投票サイクルでコミュニティからの提案投票が行われた場合、次の投票サイクルでは評議会の提案投票を行います。このように順番を決めることで、コミュニティ、評議会、技術委員会がタイムリーな意思決定に積極的に参加できるようになります。投票サイクルが回ってきた時点で、キューに提案がない場合はもう一方の提案投票が行われます。（例、コミュニティ提案投票のサイクルで提案がない場合、評議会からの提案投票を実施。）



イメージ図：レファレンダムのプロセス

4. 提案された議案はどのように進行しますか？

チェーン上のガバナンスを通じて提出されたすべての提案は、以下のいずれかのステータスに該当する可能性があります。

＜Seconded:賛成＞

コミュニティメンバーが提案を行う場合、いくつかのDOTを預けなければなりません。もしその提案が他のコミュニティメンバーにとっても価値のあるものであれば、彼らはより多くのDOTをロックすることでその提案を支持することができます。より多くのDOTが提案に賛同すればするほど、その提案は速やかにレファレンダムによる議決を待つ待機列の先頭に引き上げられ、その時点でステータスが変更されます。同様のプロセスは評議会主導の提案にも適用されます。

＜Pending:保留＞

提案が議決待ちに達した場合、その提案は間もなく公式なレファレンダムにかけられます。重要なのは、提案がタイムテーブル化されると、提案時に預けられたDOTは提案者/支持者に返却されることです。

＜Canceled:取り消し＞

提案がPolkadotチェーンにとって危険であると考えられる場合、キャンセルすることも可能です。具体的には、技術委員会が満場一致で賛成した場合や、Sudoキーなどがこの機能を使った場合が該当します。そのような提案が、その脅威の本質が明らかになる前にレファレンダムの状態になった場合、評議会の3分の2の賛成があればレファレンダムを中止することができます。仮にレファレンダムの中止が争点となった場合、その意思決定はコミュニティに委ねられることになります。提案やレファレンダムがキャンセルされると、その保証金として預けられたトークンはすべて焼却されます。

＜Blacklisted:ブラックリスト＞

システムに対して重大なリスクをもたらす提案、例えばコーディングエラーなどは、プロトコルによってブラックリストに登録されることがあります。ブラックリストに載った提案は修正されない限り、審議の対象に戻されることはありません。

5. 票数はどのように計算されますか？

レファレンダムの結果を計算するには主に2つのメカニズムを考慮する必要があります。

＜Conviction Multiplier＞

　これはゲーム理論を最大限に活用したガバナンスの重要な分野です。というのも、PoSに大きく依存するシステムでは、トークン保有者の効力を平準化するために効果的なプロセスを導入する必要があるからです。Polkadotでは、conviction multiplierという手法を用いて実践されています。
例えば、あるレファレンダムの投票者が、GさんとBさんの2人だけだったとしましょう。

Gさんは20DOTを投票に用いて、Bさんは90DOTで投票しました。

当然、Bさんの投票先の意見が勝つと予想されます。しかし、conviction multiplierを導入すると、トークンの数と、トークンがロックされる期間の両方が最終的な結果に影響するため、そうはならないのです。
GさんとBさんが設定したconviction multiplierについて、もう少し詳しく見てみましょう。

Gさんは20DOTを投票に用いてレベル 6 のロック期間を選択し、Bさんは90DOTを用いてレベル1のロック期間を選択して、投票しました。

Polkadotの仕様に従うと、レベル 1 のロック期間は4週間で、レベルが1つ上がる毎にロック期間は倍になります。 したがって、上記の例では、最終的な投票の持つ効果は以下のような結果になります。

Gさん = 20 x 6 = 120 DOTS
Bさん = 90 x 1 = 90 DOTS

このようにGさんの投票の効力は、結果的に預けるDOTが少なくとも、ロック期間の倍率が高いので、Bさんよりも大きな影響を与えることになります。この興味深いメカニズムについてもっと知りたい方は、こちらのWiki記事をご覧ください。

conviction multiplierが、少数のDOTを持つコミュニティメンバーと、より大きな資産を持つコミュニティメンバーとの投票力をどの程度まで調整するかはまだ分かっていませんので、この方法は将来的にさらなる調整が必要になるかもしれません。
最後に、レファレンダムや評議員の指名に使用されたトークンは、一時的にロックされ、他のアカウントに移動することができないため、このシステムを利用しようとすると、コストがかかります。ただし、これらのDOTはロックされた状態であってもブロック生成報酬を得るためのステークに利用することが可能であることは覚えておいて下さい。

＜投票へのバイアス効果＞

　これもオンチェーンガバナンスの重要な仕組みで、その設計にはゲーム理論が用いられています。どのガバナンス組織が提案を開始したかによって、レファレンダムの結果を決定する3つの異なる方法があります。

1). 通常の多数決

　評議会で過半数の賛成を得て提出された提案は、投票率に関係なく「賛成」または「反対」の多数決で可決または否決されます。この場合、投票バイアスは機能しません。

2). 正の投票率バイアス

　コミュニティ主導の提案に基づくレファレンダムの場合は、少し事情が異なります。この場合、投票メカニズムには提案された変更に対して、コミュニティからの圧倒的な肯定的支持がある場合にのみ失効するバイアスが組み込まれています。というのも、投票者が少なければアップグレードを進めるために必要な「賛成」の数は単純な過半数よりも多く必要な設計になっています。例えば、コミュニティの19％のみが投票した場合、20％の「反対」で80％の「賛成」を覆すことも可能です。
この仕組みはレファレンダムの投票率が低ければ自分たちの望む結果が得られると考え提案をする、悪意あるユーザーからエコシステムを守る事を目的としています。

3).負の投票率バイアス

　このメカニズムは評議会内で全員から賛成を獲得した提案を、レファレンダムで投票する場合に適応されます。このシナリオではレファレンダムの投票者数が少ない場合、提案を可決するために必要な賛成票の割合が低くなるように、提案の否決に対して「ある仕掛け」が配置されています。例えば、投票率が30％であれば、70％の「反対」を覆すのは30％の「賛成」で足りるのです。ここでの最大の目的は、ネットワークの技術的な更新を早め

ることにあります。評議会が提案の利点に満場一致で同意しているので、レファレンダムで提案された内容はよほどのことがない限りエコシステムに付加価値を与えるものである、と想定されているのです。

6. レファレンダム後の進行は？

レファレンダムが否決された場合、オンチェーンでは何も起こりません。レファレンダムが可決された場合、約28日間の待機期間の後、オンチェーンでの変更がシステムによって自動的に実行されます。これは、Polkadotでコード化されたオンチェーンガバナンスの利点の1つであり、提案を取り消したりブラックリスト化したりする選択肢を持つことが重要である理由です。

これまでご紹介した主要な投票の仕組みを踏まえ、もう1つのトピックに移りたいと思います。

Polkadotのガバナンスに対する批判

Polkadotのオンチェーンガバナンスプロセスは、多くの批判を集めています。しかしほとんどの場合、これらの否定的なコメントは特定の問題についての強い意見というよりも、むしろ無知から生まれています。ここでは最も一般的な批判を取り上げ、それに答えていきましょう。

1. 中央集権化の一形態である／今後中央集権化することになる

目に見える形で活発なガバナンスプロセスは中央集権化の一形態に過ぎないと考える人がいます。実のところ、私もこのような危惧を抱いています。とはいえ、ガバナンスプロセスが中央集権化を促すわけではなく、それを実際に行うのはユーザーです。現在、多くの人がEthereumは意思決定に関して完全に非中央集権化されていると考えていますが、それは完全な真実ではありません。しかし、Ethereum Foundationの予算はどうなっているのでしょうか？具体的にどのように支出が管理され、コミュニティによって追跡されているのでしょうか。何も、裏で何か怪しげなことが行われていると言っているのではありません。そうではなく私が言いたいのは、Ethereumコミュニティの誰も、資金がどのように使われ、誰がこれらの支出提案に賛成しているのか、その全容を知らないということです。これはEthereumのプロセスを批判するものではなく、むしろその仕組みの一部に関する情報が曖昧なままであるという事実に注意を喚起するためのものです。したがって、Ethereumが用いている手法より透明性の高い方法を持つことに本当に問題があるので

しょうか？私は、私たちが見落としたり、当たり前だと思ったりするような点を指摘しているに過ぎないのです。

ネットワーク関連の開発に関しては、Vitalik Buterin氏のアイデアがEthereumエコシステムのロードマップを牽引していることが広く知られ、コミュニティも受け入れています。他の参加者は、彼のアイデアを新しいプロジェクトに取り入れることがよくあります。一方、少数派の批評家は変更がマイナーによって最終的に実装される前までに欠陥を指摘します。これは実際には良いプロセスなのですが、非常に時間がかかり、透明性に欠けていることがあります。Polkadotについても当初は同じことを批判されたでしょうが、現在はすべてがオンチェーン化されているため、あらゆる変更を検証することができます。

もしTreasury（プロジェクトが持つ財源）があるなら、それがどのように使われているのか、コミュニティは知る必要があります。また、ないのであれば、あったほうがコミュニティにとってメリットがあるのではないでしょうか？今のところ、エコシステムの開発をサポートするためにTreasuryが利用できる、オープンで検証可能な方法でコミュニティのメンバーに資金を提供できる公式のTreasuryはEthereumやBitcoinにはありません。資金調達にとどまらず、意思決定プロセスが各財団の手に一元化されていることは明らかです。個人的には、システムを構築した人々がそれを破壊しようと企むとは考えにくいので、これには何の落ち度もありません。
これは、私たちがプロジェクトの創設者を暗黙のうちに信頼している理由でもあります。しかし、持続可能な非中央集権型ネットワーク関連の意思決定を行う方法として、私はやはりオンチェーンプロセスを採用する事に賛成です。

結局のところ、より良い社会、つまり現在の社会を反映しつつもより公平なルールの社会を望むのであれば、ブロックチェーンが必要なのです。なぜなら、ブロックチェーンは私たちのガバナンスシステムを修正したり、より良くしたりするために使えるツールだからです。多くの間違いが起こり、多くの教訓が得られるでしょうが、何も行動しないよりは実験する方がはるかに良いと考えます。

2. 悪質なユーザー（または初心者）にネットワークに害を及ぼす機会を与えることになる

　これは正当な懸念であり、ありがたいことにPolkadotのガバナンスの設計において既に考慮されています。対応策のひとつとして、ガバナンスによってネットワークを破壊しようとする悪意あるユーザーは、多額のDOTを使わなければなりません。つまり、ネガティブな結果になるように票を動かしたい人は以下のことをしなければならないのです。

1). 多数のDOT保有者にDOTを用いて悪意ある行為をするように説得する。
2). 悪意ある行為をするための資金を自分で用意する。

いずれのシナリオも資金やリソースの面で非常に大きな負担となります。しかし、もし初心者が誤ってエコシステムに危機をもたらす提案をしたとしても、ガバナンスシステムには訂正や取り消しを可能にするチェックポイントが存在するため、実現することは難しいでしょう。

3. 一般人には複雑すぎる

　この点については十分に共感できます。既存の組織のガバナンスの仕組みというのは、これを特別に教える学問分野が存在するほどに、複雑です。そのため、(Polkadotのように)完全な非中央集権化を目指すガバナンスのプロセスには政治学や歴史学、ゲーム理論から学んだ多くの教訓を設計に取り込まなければならず、複雑になってしまうことが予想されます。
とはいえ、ブログの連載を読むだけで自国の憲法をしっかり理解することはできず、それなりの努力が必要なのと同じように、Polkadotのガバナンスへの理解もまた努力が必要です。
Polkadotの場合、必要なのは特定の役割とプロセスがあるということだけで、それに関する情報は300ページの文書よりはるかに少ないのです。どんな技術でもそうですが、何かを理解するということは、それを使いこなし、最大限に活用できるようになるということです。普通の人が普通の町議会について学ぶことができるように、オンチェーンの評議会が何をするのか理解することは、さほど難しいことではないでしょう。つまり、ガバナンスのプロセスや現在利用可能なインターフェースについての説明を簡素化することは、実現可能なのです。

4. EthereumとBitcoinはガバナンス機能がなくても非中央集権化されています

　Ethereum ClassicとBitcoin Cashが元のチェーンから分岐したのと同じように、テクノロジーは異なる方向に進化するので、この批判は妥当とは言い難いです。現在、オンチェーンガバナンスは極端なことをせず、検証可能な手段を提供することで対立を解決する方法を提供しています。Bitcoinを除き、ほとんどの非中央集権型プロジェクトには資金援助団体や財団（foundation）が存在します。しかし、この文脈における財団とは、ネットワークの長期的な成功を管理する際に信頼できる人々のグループではないのでしょうか？

しかし、私たちは彼らによってどのように決定がなされ、その決定にどのような手順が取られるのかを実際に目にすることはできません。漠然とした説明のブログ記事があちこちにありますが、投票数は見られません。これは意思決定のために投票が必要だと言ってい

るのではなく、私たちはその正当性を証明する実際のデータなしに、私たちのために行われる意思決定に多くの信頼を置いているということを示しているに過ぎないのです。
一方、非中央集権型ブロックチェーンシステムでは、信頼とはオンチェーンに記録された検証可能なデータによってのみ成り立つものなのです。

5. DOTに依存しすぎているため、ネットワークが常にDOTの大量保有者の言いなりになってしまう

　これも私が過去に一生懸命向き合い、考えた正当な懸念です。まず、考えなければならない点がいくつかあります。

1). より多くのDOTを保有する者はガバナンスの決定がエコシステムに悪影響を与えた場合、より多くのものを失うことになる。したがって、この保有者はエコシステムにとって最良の変化を支持するインセンティブがある。

2). Polkadotはトークン・ベースのガバナンスの限界を認識し、これらの問題を回避するためのソリューションを提案している。具体的には少額保有者であっても自分の投票力を高める事を可能にする「Conviction Multiplierメカニズム」を導入している。

3). ネットワークが望ましい方向に進化していない場合、いつでも自由にエコシステムから脱退することができる。

DOTへの過度な依存は、ネットワークのセキュリティを高めるために必要です。Proof-of-stakeは文字通り**ステークによる証明**です。もし私たちがPoS方式を使ってネットワークを安全にすることに問題がないのなら、なぜそれをガバナンスに適応させることを心配する必要があるのでしょうか？本当の問題は、オンチェーンでの運用を維持しながら、ガバナンスの決定についてコンセンサスを得るためのより良い方法があるのかどうか？です。また、コミュニティが後にこのステップが必要だと判断すれば、トークンへの依存度がいずれ変化する可能性もあります。そして、それこそがPolkadotのガバナンスプロセスの素晴らしさなのです。

6. 今後、何かしらの問題が起こるだろう

　私たちは新しいことや未知のものに対して、ネガティブなバイアスをかける傾向があります。私自身あらゆる場面で最悪の結果を想像してしまうので、Polkadotのガバナンスの過程で何か不測の事態が起こる可能性を考えるのは当然のことです。しかし、**ガバナンス**

のプロセスがあることで、何が起こってもDOTホルダーはネットワークにとって望ましい行動を集団で決定することができるのですから、もっと前向きに考えることができるようになりました。そして、もしアップグレードの提案が結果的にコミュニティを二分し、膠着状態に陥った場合には、真の意味でコミュニティによるネットワークの回復力が試されることになります。

全体として、Polkadotのオンチェーンガバナンスはその設計と実装に政治学、人間心理、経済理論が組み込まれているため、この分野で最も堅牢なものの1つです。一つ大きな注意点は、Polkadotのエコシステムでは物事が本当に速く進み、ほとんどすべてのシステムパラメータが参加者によって調整できるため、私がこれまで書いてきたことはすべて変更される可能性があるということです。これは素晴らしいことであり、もし設計段階で間違った仮定がなされていたとしても、次のバージョンのシステムで修正することができます。時間が経つ事で結果的に過ちがあったかどうかが明らかになるので、よく観察し、考察する機会を設けていきましょう。

Treasuryの仕組み

　オンチェーンガバナンスプロセスの利点の1つはコミュニティがプロトコルのTreasuryの資金を最大限に活用できることです。PolkadotではオンチェーンのTreasuryは評議会によって管理されおり、Treasuryに関する提案は評議会の投票によって決定されます（レファレンダムは実施されません）。Treasuryの唯一の目的は、エコシステムの維持と成長を促進することです。ここからは、どの様にしてそのゴールを達成する仕組みになっているのか、詳しく見ていきましょう。

＜Bounties：報奨金制度＞

　Treasuryの提案に関して、評議会メンバーがチェックを行い適切な評価をするのは現実的に限界があります。評議会のメンバーがすべての提案に記載された活動を適切に評価する専門知識を常に持っている可能性は極めて低いので、評議会が提案の監督を専門家に委任する方法が必要となります。

報奨金制度とは特定の仕事（または特定の目的）に対する報酬であり、事前に定義された報酬が支払われる仕組みで、DOT保有者であれば誰でも報奨金の提案を開始することができます。特徴的な点として、提案がなされるとプロジェクトの検証と実行はバウンティキュレーターと呼ばれる人たちが担います。バウンティキュレーターは、特定の目的のために使用されるTreasuryの一部を管理する権限を持つ個人、またはグループと定められています。

これらの人々はバグや脆弱性の修正、戦略の策定、またはPolkadotエコシステムに利益をもたらす一連のタスクの監視を行います。

報奨金の提案が可決された後に評議会によってプログラムの実行者としてキュレーターが選出され、提案内容の実行を行います。この際、評議会に承認される前に、キュレーターは保証金を支払う必要があります。これはプロジェクトの実行時にデータの改ざんなど悪意ある行動を取った場合に備え、場合によっては預けられた資産を没収するための安全措置のためですが、提案者が報奨金の受取に成功した場合には彼らは報酬と同時に保証金も返還されます。

＜Proposal：支出提案＞

報奨金が具体的なタスクに対して支払われるのに対し、支出提案はより自由度の高い仕組みです。提案の内容はインフラの構築、コミュニティの教育、新しいプロジェクトの構築、ツールの作成、エコシステムのマーケティングなど様々です。現在までにこの本の制作を含め100以上の独立した提案がPolkadot Treasuryから資金提供を受けており、報奨金との主な違いは提案された内容がバウンティーキュレーターではなく提案者自身によって実行されることです。

＜Tips：チップ制度＞

これはコミュニティメンバーが、エコシステムの維持と成長のために努力した他のコミュニティメンバーに対して報酬を推薦する仕組みです。DOTホルダーであればコミュニティ内外に対して広報活動を行った他のメンバーへのチップを評議会へ要求することができます。例えば、私は以前Polkadotのガバナンスについて書いた記事について、コミュニティメンバーからチップの対象者として推薦されたことがあります。

Treasuryの資金源

では、これらのTreasuryとして管理される資金はどこから来るのでしょうか？財源は幾つかあり、下記に紹介します。

1). 没収財

バリデーターが何らかの理由（主に悪質な行為により）で除籍された場合、没収された資金はTreasuryに送られ、報酬としてバリデーターの行為を報告した人（多くの場合他のバリデーター）に送られます。
報酬は没収財から支払われ、行為の性質や報告者の数によって異なります。

2). 取引手数料

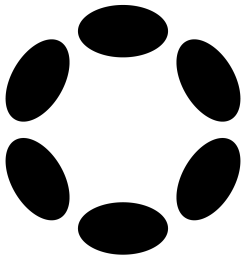
各ブロック生成時にユーザーが支払う取引手数料の一部はブロック生成者に報酬として送られますが、残りはTreasuryに送られます。

3). ステーキング

DOTのインフレ率は最初の1年で10%となるように設計されており、理想的なステーキング率は全供給量の50%に設定されています。つまり、現存する全トークンの半分がステーキングに固定され、インフレ分が報酬としてバリデーターに完全に行き渡ることがPolkadotの理想的でな設計となっており、もしステーキング率が50％を下回ればバリデーターは最高値よりも少ない額を受け取る事となり、残額がTreasuryへと分配されます。

4). パラスレッド

パラスレッドと呼ばれるチェーンは、パラチェーンとは異なりブロック単位のオークションに参加します。この時、入札額の一部は該当のバリデーターに送られ、残りはTreasuryに分配されます。
更なるTreasuryの詳細については、Polkadot wikiの記事をご覧ください。



第五章

Polkadotネットワークの拡張

これまでPolkadotのネットワークがどのように構成されているかを見てきましたが、次にPolkadotの唯一無二の特徴であるパラチェーンによって、ネットワークがどのように拡張されているかを見ていきたいと思います。
パラチェーンがなければ、リレーチェーンはステークとガバナンスの機能に限定された、肉付きのないネットワークに過ぎません。それに対してパラチェーンは、取引手数料の有無、ブロックの大きさ、小ささなど、チームが望むような設計が可能です。つまり、各パラチェーンはそれ自体が正に1つの国なのです。そして、リレーチェーンは、そのさまざまな国をつなぐ道路や海路を整備するネットワークと考えることができます。

また、各パラチェーンは非常にカスタマイズしやすいレイヤー1ブロックチェーンであり、以下のような特筆すべき機能を持ちます。

・パブリックレイヤー１ネットワーク
・プライベートレイヤー１ネットワーク
・レイヤー２スケーリングソリューション
・ブリッジ

これは、リレーチェーンが実際に接続されるチェーンを事前に決めていないからこそ実現できるのです。Substrateがサポートするプログラミング言語を使って構築されたものであれば、どのような機能を持っていてもそのまま受け入れることが可能です。SubstrateはWeb3 Foundation(W3F)からPolkadotの構築を委託されたParity Technologiesが開発した、最新のブロックチェーン構築のためのフレームワークです。したがって、Substrateを使って構築されたブロックチェーンやネットワークは、Polkadotのリレーチェーンと互換性があります。

しかし、実際のところパラチェーンとは何なのでしょうか？
パラチェーンになることにどんな意味があるのでしょうか？パラチェーンはリレーチェーンの強力な経済的セキュリティによって守られ、リレーチェーンのバリデーターのコンピューティングリソースをクロスチェーン操作に使用できるという点で、リレーチェーンの子供のようなものです。

ここで、パラチェーンが標準的なレイヤー1ブロックチェーンと比較した場合の利点は2つあります。

・リレーチェーンから共有された、強固なセキュリティ
・相互運用性

共有セキュリティの概念はもう理解されているはずですから、あとはブロックチェーン技術の「聖域」とされる相互運用性に注目していきましょう。

パラチェーンの相互運用性

私は、相互運用性こそがPolkadotの唯一無二性を表していると考えています。ブロックチェーンに馴染みのない方にはあまりピンとこないでしょうから、ここではなぜパラチェーンの相互運用性がブロックチェーン分野での無限のイノベーションの鍵になるのかについて、説明したいと思います。

DeFiとNFTを用いた非中央集権型デジタル所有権は、異なる自動化システム/ネットワーク間の「信頼」を不要とした相互運用性のおかげで、今日の地位を築きました。
通常、ブロックチェーンプラットフォームは、ブリッジを介して、あるプラットフォームから別のプラットフォームへ、またはその逆へトークンを移動できる場合、相互運用可能である、と言われています。

例えば、BitcoinをEthereumに送りたい場合、必要なのはブリッジのためのアプリケーションにアクセスして、トークンの転送を行うだけです。これは数クリックで完了する、簡単な操作です。注意しなければならないことは、この場合私がBitcoinからEthereumへ移したトークンは、厳密にはまだBitcoinのネットワーク上にあるということです。これは、ブリッジの転送方法が、まず私のBTCトークンをBitcoinネットワーク上の専用アドレスに送信して凍結し、次にEthereumネットワーク上で「ラップされたBTC」という新しい代替トークンセットを生成し、続いて「ラップBTCトークン」を私のEthereumアカウントに送信する、という方法だからです（そのためWBTCとして表記される）。

既に述べた通り、これは非常にシンプルで分かりやすい処理ですが、Polkadotの持つ「相互運用性」は少々異なります。詳しくみていきましょう。

まず、相互運用性には2つの側面があります。

1). トークンやメッセージの送信
2). 関数の呼び出し

1点目はかなり些細なことですが、2点目については比較的聞き慣れないものですので、例を用いてみましょう。
例えば、ブロックチェーンAがブロックチェーンBの関数を実行するには、ブロックチェーンAとブロックチェーンBの間の操作を自動化し、人間の仲介者を不要にする必要があります。その場合、ブロックチェーンAはブロックチェーンBのスマートコントラクトを呼び出し、ブロックチェーンBはブロックチェーンAに応答して、要求された情報を与えたり、何らかの計算を実行する事になりますが、これぞ相互運用性と呼ぶべきものです。

この概念を理解するために、更に別の実用的な例を用いて説明してみましょう。
あるユーザーが、チェーンBに保管されている貴重なNFTを担保に、DeFiに特化したチェーンAで融資を受けたいとリクエストしてきました。しかし、チェーンAがこの融資依頼を受け入れる前に、いくつかの情報を確認しなければなりません。

1). 果たしてこのユーザーは本人か？
2). このユーザーは本当にNFTを所有しているのか？
3). このNFTの価値はいくらなのか？

こういった疑問のほかにも、チェーンAは以下の作業も必要です。

4). ローンポジションを表すNFTを生成する
5). チェーンBにトークンを送信する

更に、これらデータをすべて収集するためにチェーンAは他のチェーンと通信する必要があり、最終的に以下のプロセスを行います。

- ユーザーの本当の身元を知るために、チェーンAはIDチェーンCと通信し、ユーザーが本当に本人であること、融資を受ける資格があることを確認する。

- チェーンAは、このユーザーにローン残高がないことを確認するため、パートナーである他の2つのDeFiチェーンとクロスチェックを行う。

- このユーザーが実際に担保となるNFTを所有していることを確認するため、チェーン A はチェーン B と情報照合を行う。

- このNFTの価値を評価し、担保比率が適切かどうかを確認するために、チェーンAは予測チェーンであるチェーンD上でスマートコントラクトを開始する。この予測チェーンは、予測者と評価者のセットにインセンティブを与え、NFTの真の価値を分析させる。

- すべてが順調であることを確認したチェーンAは、NFTの回収を進め、チェーンB上のNFT保管庫にロックし、ユーザーに要求されたトークンを渡し、利息の回収を開始する。

注）説明をよりわかりやすくするため、本来必要な手順を追加して説明しています。

このように、相互運用性には「強い」面と「弱い」面の2種類があることがわかります。弱い相互運用性では、ユーザーはこれらの操作をすべて単独で行い、異なるチェーン上の複数の取引に署名しなければなりません。強い相互運用性があれば、あるチェーンは他のチェーンのアイデンティティ、予測、保管庫といったチェーン間の機能を活用し、その処理を安全にし、より良いユーザー体験を提供することができます。

さて、パラチェーンが他のレイヤー1ブロックチェーンに比べて強い優位性を持っていることを考えると、パラチェーンのスロットをめぐって激しい競争が起こる理由もわかってきました。Polkadotのホワイトペーパーによると、リレーチェーンは無限にパラチェーンを持つことはできず、そのリソースは有限であり、今後10年ほどで100前後のパラチェーンをサポートすることになるそうです。しかし、このことは、誰がパラチェーンスロットを得るかをどのように決定するかという新たな課題を提起しています。

パラチェーンスロットオークションとクラウドローン

取引を例に考えた場合、貴重なアイテムが売りに出され、それに対して大きな需要がある場合、最も賢明な取引方法はオークションです。

なぜなら、最も高い価格を提示する人々が最終的な買い手となることが保証されているからです。技術的にも経済的にも安全な非中央集権型システムであるPolkadotにとって「貴重なネットワーク資源をいかにして分配するか」が最も重要な課題であり、そこで登場するのがパラチェーンスロットオークション（PSA）です。PSAは、さまざまなプロジェク

トの中で最も高い入札者にパラチェーンスロットを割り当てるのに役立つ堅牢なメカニズムであり、ここからはその仕組みについて学んでいきましょう。

PSA（時にパラチェーンリリースオファリングの略でPLOとも表記されます）は、Polkadot上で1週間開催され、この1週間の間にパラチェーンは入札を行い、オークション期間終了後に落札者を決定されます。しかし、実際の手続きはもう少し込み入っています。

PSAは、1週間を「開始段階」と「選考段階」の2つのフェーズに分けます。この2つのフェーズが必要なのは、Polkadotが「キャンドルオークション」にヒントを得た新しいオンチェーンメカニズムを採用しているからです。伝統的なオークションは、タイマーをセットし、時間が過ぎると最高入札者が決まるというもので、これはeBayで見られるものと似ています。しかし、Polkadotは自らのネットワークの経済的セキュリティを最大化するために設計されている一方、このようなオークション方式では入札者が早期に最高額の入札をするメリットはなく、システムがオークション・スナイピング（終了時間間際になるべく少額で最高価格を獲得しようとする手法）にさらされるという大きな問題をはらんでいます。

例えば、ボブはある絵画に40,000ドルの入札をしたいが、市場の様子を見るために最初は15,000ドルで始めることにしました。しかし、その入札額を上回る入札があったので、500ドル追加して再び入札します。しかし、彼の入札額はまたもや上回られてしまい、彼は延々と入札を続け、タイマーが最後の3秒になると、ボブは最終的に28,000ドルを提示します。残念ながら、最後の1秒で、他の参加者アリスはボブの入札を自分の28,500ドルの入札で上回り、ボブはオークションで負けてしまうのです。しかし、本当の悲劇は別のところにあります。28,500ドルはボブの実際の予算である40,000ドルよりはるかに低いため、この作品の画家がより大きな評価額で損をすることにあります。このような一連の行為を抑制すべく、17〜18世紀頃に「キャンドルオークション」という手法が考案されました。オークション参加者はロウソクにいつ火がつくのかはわかりますが、ロウソクがいつ消えるかはわからないため、なるべく早く自身の最高額を提示し入札を試みようとする、これがキャンドルオークションと通常のオークションの持つ性質の違いです。

ですがこのキャンドルオークションをブロックチェーン上で実装するのは容易なことではありません。ブロックチェーンはランダム性を持った仕組みではないため、幾つかの設定で解決するような問題ではないのです。そこでPolkadotが採用した解決策は、オークションを開始と選考の２段階に分ける事と、オークションの第2段階目で登場する「オークション終了後に、遡って終了時間をランダム設定する」ことです。

2日間続くオープニング・フェーズでは、パラチェーンのスロットを希望するプロジェクト側が入札を行い、その入札はオンチェーンに登録され、オークション終了まで継続され

ます。スロットの座を落札するために必要な額を入札するのは自由ですが、自分のTreasuryの範囲内の入札額であることに注意しなければなりません。5日間続く選考段階では、期間終了後にリレーチェーンが検証可能なランダム関数を使って、オークション終了の瞬間を遡って選択するため、例えば最終日に入札した金額はすべて無効になる可能性もあります。したがって、オークション終了後に後から遡って設定された過去の正確な時刻時点（ブロックで表記）で最も高い入札を行っているパラチェーンの候補者が落札者となるわけです。つまり、リレーチェーンでは、3日目の特定のブロック、ここでは例として#123456ブロック時点でオークションが終了したと判断することが可能なのです。つまり、例えブロック#123456以降に最高値をつけたとしても、その候補者はオークションに勝つことはできません（ブロック#123456以降にどれだけ高額な金額を入札していても）。なお、遡って指定される終了日時に開始段階の期間は含まれることはありませんので、この期間の入札は必ず有効となり、だからこそ開始段階の入札は非常に重要なのです。

パラチェーンスロットは、プロジェクトが選択したスロット期間の数によって、Polkadotの場合であれば3ヶ月から2年（Kusamaの場合は1年）の幅があります。これにより、オークションに別の興味深い力学が導入されます。リレーチェーンが勝者を選択する際に、次の要件を考慮する必要があるからです。

・経済的収入の最大化（できるだけ多くのDOTまたはKSMを入札してもらう）
・スロット期間の最大化（できるだけ多くのスロット期間に入札してもらう）

つまり、全体の入札額が最も高く、利用可能なスロット期間が最も短いパラチェーン候補は、利用可能なスロット期間が最も長く、全体の入札額が2番目に高いパラチェーン候補と比較して、リレーチェーンの目には不利に映るということです。ただし、スロット期間は、プロジェクトが必要とする時点で利用可能なスロット期間に依存するため、この理想的なシナリオが常に実現されるとは限らないことに注意してください。

パラチェーンスロットの取得は、非常にコストがかかります。Kusamaの最初のパラチェーンスロットは50万KSM（当時約9,000万ドル）でしたが、現実的にそれだけのレンタル料を払えるチームはほとんどないため、非中央集権化の観点では理想的ではありません。

Polkadotは、このような状況を改善するために、パラチェーンのチームが自身の資金に加えてコミュニティのメンバーからDOTを調達できるよう、「クラウドローン」と呼ばれる手法を導入しました。これは、いわゆる資金調達に似ていますが、いくつかの顕著な違いがあります。

- コミュニティから集めたトークンは直接パラチェーンチームへは渡らず、代わりにリレーチェーンが保有する。これは報酬の発生しないステークとも言える。

- チームがオークションで落札できなかった場合、トークンは出資者に払い戻される。

- チームがオークションで勝った場合、トークンはレンタル期間中、リレーチェーンに保管される。このレンタル期間が終了すると、トークンはクラウドローンの出資者に返却される。

PSAでコミュニティメンバーにクラウドローンへの貢献を促すため、パラチェーン候補チームはしばしばNFT、デリバティブトークン、ボーナスステーキングレート、特別なコミュニティの役割などの特典とともに、ネイティブトークンの供給のシェアを貢献者に提供します。コミュニティメンバーにとって、これはWin-Winのシナリオであり、パラチェーンのクラウドローンやオークションに使用されるトークンはステーク報酬の対象ではないため、発生する損失は機会損失としてのステーク報酬のみとなります。

キャンドルオークションの仕組みとクラウドローン機能を組み合わせると、Polkadotはかつてないほどのイノベーションと発展の最中にいることがわかります。私が何故このように断言できるかというと、下記の根拠があるからです。

1). パラチェーンのスロットは、コミュニティの力を借りて獲得しなければならないので、「最高のチーム」がまずトップに立つことが保証されている。最高のチームというのは、技術とコミュニティへの参加の両方で成果を出せるチームという意味である。なぜなら、最高の技術チームがしっかりとコミュニティづくりしている弱い技術チームに敗れてしまうこともあり得るからである。

2). パラチェーンのスロットは最終的に期限終了を迎え、再度更新しなければならないので、チームはコミュニティにより良いサービスを提供し、クラウドローンへの依存を克服し、自己資金を増やすことに注力することが予想される。当然、パラチェーンスロットを更新できないプロジェクトも出てくるが、これは良くもあり悪くもある。サービスを縮小したり停止したりするパラチェーンにとっては悪いことだが、エコシステムにとっては継続するために必要な価値を生み出さない限り、永久的なスロットを持つパラチェーンがいないということが保証される。

この設計のもうひとつの面白さは、パラチェーンプロジェクトの多様性です。例えば、3つのDeFiチェーンが競合していたとして、そのすべてが成功する可能性は低いでしょう。例えば、十分な収益とコミュニティの支援を得ることで、2つのプロジェクトはスロット

を獲得できるかもしれません。その場合、残り1つのプロジェクトはパラスレッドを維持し、他の非DeFiプロジェクトがネットワーク上で運営を続けることになります。これはあくまで理論的な推測であることに注意してください。私が言いたいのは、このデザインによってパラチェーン候補の多様化が促進されるということです。

パラスレッドの概略

パラチェーンのスロットは有限であるため、すべての候補者がパラチェーンになれるわけではありません。また、プロジェクトによっては、パラチェーンになることが必ずしも適切でない場合もあります。パラチェーンを希望するのはリレーチェーンへのアクセスが途切れず、いつでも好きなときにブロック生成をできるからであり、そのようなリソースを必要としないプロジェクトはパラスレッドになる方がよいでしょう。パラチェーンはいわゆるサブスクリプションサービスであり、パラスレッドは都度必要なサービスに対して支払いを行う、従量課金制であると考えることができます。
Polkadotにおいて、パラスレッドを選択するメリットは2つあります。

・リレーチェーンとの接続を完全に絶つ必要がないため、プロジェクトは運用の終了を決断しやすい。

・パラチェーンスロットを取得できないプロジェクトでも、Polkadotの共有セキュリティの恩恵を受けることが可能である。

パラスレッドはどの様に機能するのか？

リレーチェーン上のいくつかのパラチェーンスロットは、パラスレッド用に予約されています。この特別なスロットは「パラスレッドプール」と呼ばれ、パラスレッドを希望するプロジェクトが接続されます。リレーチェーンにブロックを追加するために、これらのパラスレッドはブロック候補と取引手数料をパラスレッドプール内のコレーターに送り、コレーターはDOTで指定された入札とともにブロックを伝播します。

リレーチェーンのバリデーターは入札を確認し、どのブロックをリレーチェーンに含めるかを決定します。この時、リレーチェーンバリデーターの主な動機としては最も高い入札額で提出されたブロック候補を受け入れて、自分たちの報酬を最大化することでしょう。Polkadot Wikiによると、パラスレッドの入札によるトークンはおおよそ80対20で分配されます。つまり、80%がPolkadotのTreasuryに入り、20%がブロック生成者に入ることになります。これは取引手数料にも適用される同じ割合であり、Polkadotの他の多くのパラメータと同様に、ガバナンス機構を通じて変更することができます。

パラチェーン候補プロジェクトと提供するサービスの概要（2021年9月時点）

1. Acala - DeFi

AcalaはPolkadotエコシステムのためのクロスチェーンのオープンな金融インフラを提供するビジョンを持つ、初の”非中央集権型金融(DeFi)"コンソーシアムです。そのミッションはPolkadotのDeFiハブとなり、金融アプリケーションの使用や構築を容易にし、取引効率を向上させ、ユーザーの貴重な時間を節約することです。つまり、AcalaはEthereumと同じミッションを持ち、唯一の違いはDeFiユースケースに特化して構築されているため、DeFiサービスにとってはるかに利便性が高いということです。このプラットフォームは、あらゆるDeFi Dappsの開発者とユーザーにとって価値のある目的地となる、一連のコアプロトコルを提供します。

a) Honzonプロトコル(aUSD)

AcalaのaUSDを支えるプロトコルであり、クロスチェーン資産の裏付けがある非中央集権型複合担保型のステーブルコインです。これに対し、時価総額で最大のステーブルコインであるUSDTは、単一の企業の管理下にある中央集権型のステーブルコインです。非中央集権型ステーブルコインとして広く採用されているDAIは、担保としてETHなどの暗号資産を使用していて、USDTと比較して低い時価総額となっています。このようにaUSDは両者の長所を提供し、ステーブルコインの制限を避けようとしています。さらに、DOT、ETH、BTC、KSM、およびAcalaのガバナンスを通じてホワイトリストとして認定された他のトークンなど、さまざまな資産から生成することができます。

b) Homaプロトコル(LDOT)

Homaプロトコルは非中央集権型ステーキングプロトコルで、ユーザーはステーク期間中に資産の流動性を失うことなく、DOTを運用するというメリットを得ることができます。
実際にはユーザーはPolkadotにステークしてDOTを預けるという選択の代わりに、Acala Dappsのhomaプロトコルを使用し（必ずしも1対1の比率ではありませんが）、DOTをステークすることでLDOTを受け取ることができます。LDOTとはliquid DOTの略で、ユーザーはこれを担保にステーブルコインの流動性提供を行ったり、送金やスワップなどに自由に利用することが可能です。
ユーザーはステークしたDOTを換金したい場合、LDOTをプロトコルに返却するだけで、DOTとその間のステーク報酬がすぐにウォレットに返金されるため、Polkadotでステークする場合に必要な約28日間のステーク解除期間を回避することができます。

c) 非中央集権型取引所(DEX)

Uniswap、Sushiswapなどの非中央集権型取引所と同様のプロトコルで、ユーザーがトークンを交換し、流動性を提供し、報酬を得ることを可能にする仕組みです。
Acalaの目標は、非中央集権型プロトコルの複雑さを一切排除し、誰もがDeFiにアクセスできるようにすることです。すでに、米国のフィンテック企業であるCurrentと提携し、「Hybrid Finance」（非中央集権型金融と中央集権型金融の融合）という新しいタイプの金融を実現することを目指しています。つまり、暗号ウォレットを持っていないユーザーが、従来の銀行口座からDeFiで利回りを稼ぐことが可能になる事を意味しています。

2. HydraDX - DeFi

HydraDXもDeFiに特化したレイヤー1ブロックチェーンですが、Acalaとは大きく異なります。HydraDXの提供するサービスの中核は、「Omnipool:オムニプール」と呼ばれる「流動性の井戸」で、市場で取引されるトークンに対応した多様性に富んだ仕組みです。現在、ほとんどのトークン取引はペアで行われています。例えば、DOTとKSMを交換したい場合、あなたはまずDOTとKSMのペアを持つ取引所を見つける必要があり、そうして初めて、DOTからKSMへのスワップが可能になるのです。もし、そのようなプールが取引所になければ、私はDOTとKSMをそれぞれ別のトークンにスワップせざるを得なくなります。例えば、DOT/USDTのペアとKSM/USDTのペアを見つけたとすると、USDTとKSMをスワップする前にDOTをUSDTにスワップしなければならないことになりますが、これでは資金効率が悪いし、ユーザーフレンドリーでもありません。Uniswapのような非中央集権型取引所でさえ、プールでペアになっていない2つのトークン間のスワップを実行する場合には、1つのプールから次のプールへの自動スワップが行われることで最終的に希望する2つのトークンの交換が行われており、実際には多くのスリッページ（手数料）が発生しているのです。

Substrateのパワーと柔軟性のおかげで、HydraDXはすべての資産に対して単一のプール（Omnipool）を構築することで、この制限を克服しています。この詳細は、財務的にも技術的にもかなりテクニカルなものですが、ここでは基本的な要約を述べるに留めておきます。Omnipoolを作るために、HydraDXはLRNAトークンをベーストークンとして、他のすべてのトークンと取引することで、LRNAトークンが価格オラクルとして機能するようにします。HydraDXはレイヤー1ブロックチェーンであるため、そのOmnipoolで全てが運用されるという訳ではありません。むしろ、その上にさらに多くの金融アプリケーションが積み重ねられることになります。

3. KILT - アイデンティティ

長い間、私たちのデータ、特に私たちを識別するデータは、私たちを陥れ、操作し、利用するために使用されてきました。KILTは、ユーザーの「認証情報」を証明・検証するプロセスを非中央集権化することで、このような現状に挑戦しようとしています。
KILTは、自己主権、匿名、検証可能な資格を発行するためのオープンソースのブロックチェーンアイデンティティプロトコルです。KILTは、アイデンティティとプライバシーに関する革新的なビジネスモデルを可能にし、デジタル世界における信頼できるアイデンティティソリューションのニーズに応えます。KILTは、ユーザーが個人の属性を主張し、それを信頼できる機関によって証明させ、その主張を自己主権型の資格として保存することを可能にします。
このモデルの中核にあるのは、ユーザーは自分の資格に対して完全な所有権と権利を持つべきであり、他の当事者とやり取りする際には本人だけが自分のアイデンティティ情報を利用できるようにすべきだという考え方です。このプロトコルでは、資格を発行する必要がある人（求職者など）と、資格を検証する必要がある人（採用企業など）が存在します。

KILTブロックチェーンが本格的に稼働すると、採用したい企業に対して、あなたが本人であることを証明することが可能になります。企業は、あなたが提供した情報をKILTブロックチェーン上で確認するだけでよいからです。さらに検証が必要な場合は、証明者にお金を支払ってあなたの資格を検証してもらうことができます。
繰り返しになりますが、これが基本的な考え方です。しかし、これはレイヤー1ブロックチェーンであり、その上にさらに多くのIDアプリケーションを構築できることを忘れないで下さい。

4. Robonomics - IoT

私見ですが、DotSamaで一番面白いパラチェーン候補です。というのも、彼らは誰も提案したことのない「ロボット経済学」というものを構築しているからです。彼らのアイデアの核心は、自動化（自律型ロボット）の台頭に伴い、ロボット同士のやり取りを管理するための仕組みが必要になっているという認識です。例えば、工場では多くのロボットや機械が連携して製品を製造していますが、ロボット間の操作を円滑にするために人間が必要です。
例えば、あるラインで1サイクルを終えた製品を、次のラインに移動して製造を続けるには、ほとんどの場合人間の手が必要です。このとき人間の関わりが必要なのは、ロボット同士による会話や動作の連携がまだ実現できていないからです。

ここで、ロボット間のやり取りに自動的なコミュニケーションの仕組みを加えることで、全く新しい可能性、つまりロボノミクスの世界が開かれるのです。ロボノミクスによって、工場ロボットが自動運転車に指示を出し、製品の準備ができたら、工場ロボットが自動運転車にピンを刺して集荷に来るようにすることが可能になります。また、セキュリティ面についても考慮されており、ロボットをスパム攻撃から守るため、工場ロボットが輸送ロボットにいくらかのトークンを支払った場合にのみ、輸送ロボットは工場ロボットの呼び出しに反応します。

ここでいう「ロボット」とは、必ずしも人型機械のことを指すのではありません。プリンター、コーヒーメーカー、トラックの中のコンピュータープログラム、トレーディングロボットなど、ある一定の入力を受けて、ある一定の動作を自動的に行うように設計されている機械はすべてロボットと言えます。ロボノミクスは、デジタル世界と現実世界の経済を「ロボット」で結びつけようとするプロジェクトであり、法定通貨と暗号資産が「オラクル」（ブロックチェーン上のスマートコントラクトにオフチェーンのデータを提供するサービス）で結ばれているように、非常に興味深いものです。

5. Phala - プライバシー

Phalaは、クラウドコンピューティングにおける信頼の問題に取り組んでいます。Phalaのレイヤー1ブロックチェーンは、データの機密性を犠牲にすることなく大規模なクラウド処理を可能にする、信頼性の高い計算プラットフォームです。平たく言えば、Phalaはブロックチェーンのコンセンサスによって集められたPCのネットワークを通じて、非中央集権型のプライベートクラウドを構築しているのです。Phalaは、Google Drive、One Drive、Adobe Cloud、Azure、AWSといったパーミッション型/Web2クラウドサービスに代わる新しいモデルを提供したいと考えており、Phalaはスマートコントラクト、非中央集権型ストレージプロトコル、データ索引サービスなどを自由に組み合わせることができる汎用的な非中央集権型コンピューティングネットワークを提供することに取り組んでいます。

Phalaの提供するFat Contractは、Polkadotとそのパラチェーンを構築するために使用されたフレームワークであるSubstrateのパワーと柔軟性によって可能になった、現在のスマートコントラクトモデルのアップグレードを目指した製品です。従来、スマートコントラクトはオンチェーンでコードを実行します。つまり、ブロックチェーンネットワークがコンセンサスとともにスマートコントラクトの計算を実行する責任を負っています。しかし、これでは、ネットワークの計算能力（ブロック生成、最終性など）に縛られるため、スマートコントラクトの力が制限されます。スマートコントラクトの実行をブロックチェーンのコンセンサスから切り離すことで、より強力なスマートコントラクトが生まれます。

Fat Contractとは、その計算をオフチェーンで処理するスマートコントラクトのことです。これは、Phalaのプライバシー保護機能と相まって、計算データがマイナーに見られることはないことを保証します。Fat Contractsの主な魅力は、より幅広いサービス、特にゲーム、メタバース、データ分析など、多くの処理能力と速度を必要とするサービスに対して、よりリッチでパワフルなスマートコントラクトの利用を可能にすることです。

6. Crust - データ

　クラウドサービスは私たちの生活に大きく貢献しています。ディスク容量が限られた個人所有のデバイスにすべてのデジタルファイルを保存する必要はもうありません。しかし、中央集権的なクラウドサーバーに保存されたデータは、完全に自分のものではありませんし、自分のデータが常に安全でアクセス可能であるとは断言できません。これに対し、非中央集権型クラウドには、1つのクラウドやホスティングサービスに依存しないという利点があります。
Crustは、日常的なユーザー、専門家、開発者向けに、わかりやすい非中央集権型クラウドストレージを提供しています。Crustでは、あなたのデータは世界中の複数のノードに保存され、いつでもどこでもこのデータを取り出すことができることを保証します。さらに、保存されたデータはあなただけが所有しており、あなただけがアクセスすることができます。これは、Crustがデータをノードに送信する前に、高度なデータ暗号化を使用しているためです。Crustは、Google、Dropbox、Boxなど、現在運用されているすべての集中型クラウドストレージサービスに挑戦しようとしているのです。

7. Zeitgeist - Futarchy

　Zeitgeistは、Polkadotエコシステムの中で最も独創的なアイデアを提案するレイヤー1ブロックチェーンです。民主主義は理想的な統治形態ですが、意思決定のためのモデルに関しては多くの欠点があります。
現在、国家間の富の差は、天然資源や人間の能力の差に帰することができないほど大きな差があります。その原因は、民主主義国家であるにもかかわらず、非効率的な政策がとられていることにあり、その中でFutarchyは、新しい政府の形として、予測市場の結果を利用して意思決定の方法を変えようとする取り組みです。

Futarchyの主張によると、市場はより合理的であろうとする傾向があり、ガバナンスの独立した形態として使用できる、ということです。Zeitgeistはレイヤー1ブロックチェーンを提供し、誰でもあらゆるトピックに関する人々の意見を測定する予測市場を作ることが

できるため、企業、政府、ブロックチェーン・コミュニティ、DAO、その他の組織の政策決定をサポートすることが可能です。Futarchyでは自由奔放な意見に基づく意思決定ではなく、まるで人々が「自身の発言に対してお金を預ける」ことを強いられるような、重み付けされた仕組みが用いられています。

この様に意見を言うことにコストが伴うと、人々はより慎重に、より正直に意見を言うようになることが期待されます。そして、例えば、国会議員がどのように自身の発言に重み付けをしたかによって、判断に至る未来が想像できます。次の質問を見てみましょう。「税金を減らせば、もっと経済が発展すると思いますか？」民主主義では、議員全員が自分や他人の意見に基づいて投票されますが、Futarchyでは、税金を下げることが経済の進歩につながるかどうか、議員全員が財政的な立場を取ることが求められます。強い信念を持つ者は、自身の発言に対してより多くのお金を預け、間接的に投票結果を左右することになるでしょう。

自分の意見に十分な信頼があり、大きな額の重み付けをするリスクを負っている人と、自分の意見を十分な資金で裏付ける勇気がない人、あなたならどちらについて行きますか？しかし、どの様な理想も絵空事と指摘される通り、Futarchyモデルにはいくつかの潜在的な欠点があります。一部の人々は、Futarchyのある種賭け事の様なゲーム性やリスクテイクの部分に気を取られ、資金や社会的影響力を得るために「Crypto Twitter現象」すなわち「ビッグ」アカウントがその影響力を利用して時価総額に見合わないトークンの価格をつり上げることに、どうしても気を取られてしまうでしょう。また、人々が自分自身の意見を形成することなく、煽りや大きな賭けに従うことになることも予想されます。これは、無関心な人々が「インセンティブ」の欠如のためにわざわざ投票しない民主主義より100倍悪いと言えます。このように、Futarchyはより多くの参加者を集めるために非中央集権化されていますが、賭けの妥当性を損なう「ギャンブル」的な効果も存在するのもまた事実です。実装して初めて展開が見えてくる、それがZeitgeistの未来に期待する理由です。

8. Moonbeam - スマートコントラクト

MoonbeamはPolkadotネットワーク上のEthereum互換のスマートコントラクトプラットフォームで、開発者は既存のSolidityスマートコントラクトやDappsフロントエンドを元のコードに最小限の変更を加えて展開できるようになっています。Kusama（Moonriver）上で同プロジェクトのカナリアネットワークのローンチに成功した後、このプラットフォームを「Ethereum 3.0」と呼ぶ人もいます。
この呼称に伴ってMOVR（Moonriverのネイティブトークン）の価値が上がることは間違いありませんが、このネーミングはまったくふさわしくないというわけではありません。ひとつには、MoonbeamがEthereumのネイティブツールをスムーズに統合しているため、すべてのEthereum Dappsが簡単に利用できる点にあります。こうして開発者は、

Ethereumブロックチェーンの制限（不当なガス料金、モジュール性の欠如など）に苦しまない、より豊かなDappsを作ることが可能です。

　これまで紹介してきたプロジェクトは、Polkadot上に構築されている多くのパラチェーン候補のほんの一部に過ぎません。以下のリンクはエコシステム・プロジェクトに関するいくつかの有用なリソースへのリンクですので、是非ご自身でどの様なプロジェクトがあるのか、その際立つ特徴について調査してください。

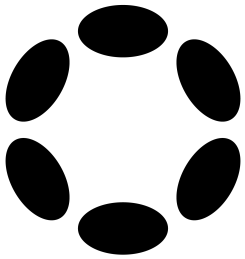
・https://parachains.info/

・https://dotmarketcap.com/

・https://polkaproject.com/

注意すべき点は、これらのプロジェクトのほとんどは、（2021年9月時点では）パラスレッドとしてしか登録されていないことです。パラチェーン枠のオークションを落札してリレーチェーンに接続されるまでは、そのプロジェクトはパラチェーン候補にとどまっています。
本書の冒頭では、なぜさまざまなブロックチェーンが必要なのか、なかなか想像がつかなかったかもしれません。この章で、これからの時代はまさにマルチチェーンであることを納得していただけたのではないでしょうか。どちらかというと、Polkadotのようなレイヤー0ブロックチェーンが、将来のレイヤー1ブロックチェーンの開発が成功するための指数関数的なイノベーションをサポートすることを目的としているため、無限の汎用性があることをより理解していただけたのではないかと思います。

人類と地球全体にとって未解決の問題があまりにも多く、あらゆるテクノロジーの目標は生活をより良くすることであるべきです。ただし、人間だけを対象とした狭義の生命ではありません。そのような考え方が現在の気候危機を招いたのです。ここでいう生命とは、植物や動物、大気など、私たち人間にとって欠かすことのできないすべてのものを指します。非中央集権型ネットワークや組織の願いは、生命を尊重し、自由と平和と公正を促進し、人類の繁栄をもたらすという地球規模の問題に対して、人々が時間をかけてより寛容になることです。もし長期的にこの様な取り組みができなければ、Web2.0での失敗を繰り返す運命にあるでしょう。



第六章

Polkadotネットワークへの参加

この本を読んでいる時点で、あなたはすでにPolkadotについて多くのことを学んでいます。しかし、知識のための知識は何の価値ももたらしません。知識は応用することでその価値を発揮するのです。本書は、Polkadotを親しみやすい形で紹介し、この非中央集権型ネットワークの素晴らしさと可能性をより多くの人に知ってもらうために書かれたものですが、それはまだ物語の半分に過ぎません。この本が書かれたもっと適切な理由は、エコシステムの新しい構築者とアンバサダーを募集するためです。なぜなら、ネットワークはその参加者次第で良いものになるからです。
もしあなたがPolkadotのエコシステム上に出現したチャンスに興奮したり、刺激を受けたりしたなら、この章では、ネットワークに参加することを心からお勧めします。

Polkadotに参加すべき理由は以下の通りです。

- 真に非中央集権化されたネットワークである。
- フォークレスアップグレードとオンチェーンガバナンスにより、将来的にも利用可能なシステムである。
- 活気と情熱にあふれたコミュニティがある。
- スケーラビリティがあり、どんな大胆なアイデアでも受け入れることができる。
- 差別や検閲からの自由といった普遍的な価値観に合致している
- レイヤー1ブロックチェーン、レイヤー2ブロックチェーン、スマートコントラクト、Dapps、ブリッジ、その他多くの斬新なプロトコルの無限な「パラバース」への入り口である。

このように、Polkadotを構築したり参加したりすることで、Web3.0イノベーションの最前線であり、中心に位置づけられるのです。さて、参加することに納得していただいたところで、実際にどのように参加するのかを考えてみましょう。

Polkadotネットワークに参加する方法

この小項目では、ネットワークへの参加にどのような選択肢があるかを説明します。

セキュリティ

非中央集権型ネットワークは安全である限りにおいてのみ価値があり、したがってネットワークに参加する最も明白な方法は、そのセキュリティに貢献することです。幸いなことに、Polkadotはノミネート・プルーフ・オブ・ステーク（NPoS）を採用しているネットワークであり、一般人にもネットワークの保護者として参加する機会を与えてくれています。
ここでは4つの異なる役割が用意されています。

1). バリデーターになる

これにはいくつかの機器と技術的なノウハウが必要だが、バリデーターになることで取引を検証し、ブロック生成に参加できる。

2). コレーターになる

バリデーターがリレーチェーンを保護するのに対し、コレーターはパラチェーンとパラスレッドを保護する。そして自分の好きなパラチェーンのコレーターになることができる。

3). ノミネーターになる

DOTトークンを持っている場合、バリデーターにそれを預けるだけで報酬を得ることができ、使用できるさまざまなウォレットや追加機能がある（詳細は下記のおすすめに紹介）。

4). クラウドローンに参加する

自分のDOTをロックして、パラチェーンがリレーチェーン上のパラチェーンスロットを一定期間確保するのを支援できる。これにより、パラチェーンから報酬としてネイティブトークンを得ることもある。

上記のすべての操作は、ネットワークの公式Webインターフェースであるpolkadot-js extensionやアプリ上で完了することができます。しかし、技術者でないユーザーの多くは、より初心者に優しい代替手段を必要としていますので、下記にご紹介します。

ステーキングとクラウドローンに参加するためのおすすめウォレット

＜PC版＞
1. Talisman wallet (著者個人としてはこちらがお勧めです)
2. SubWallet

＜モバイル版＞
3. Fearless wallet
4. Nova wallet
5. Polka-wallet
6. Mathwallet（PC版も利用可能）

＊中央集権的な取引所に対する簡潔な注意事項

Binance、Kraken、Coinbaseなどの中央集権的な取引所を通じてDOTをステークし、Polkadotクラウドローンに参加することができますが、私は意図的にそれらを推奨ウォレットのリストから除外しています。なぜなら、中央集権的な取引所をオンチェーンでの行為に用いることは、非中央集権化の考え方に反するからです。これらの取引所を通じてステークやクラウドローンに貢献すると、事実上あなたのトークンの所有権は取引所に委ねられており、これは長い目で見ると問題になりかねないからです。

1). 中央集権的な取引所ではあなたのトークンや他のユーザーのトークンを使ってガバナンスに参加したり、あなたが支持しない提案に投票することができる。

2). 中央集権的な取引所はハッキングされたり、そのバリデーターが被害に遭う可能性があり、結果としてネットワーク参加者の大部分を危険にさらすことになる。

私が推奨するウォレットを通じたステークとクラウドローンへの参加は、オンチェーン参加の権利を第三者事業者が管理するアカウントに移すのとは対照的に、あなたのオンチェーンでの行動が常にあなたの管理下にあるアカウントに結びつけられることを保証するものです。

ガバナンス

ガバナンスは残念ながら非中央集権型ネットワークで最も人気のない機能であり、ほとんどのレファレンダムは10%の投票率を得ることができていません。ですから、あなたがガバナンスの活動に参加することは、ネットワークに新しい息吹を与えることになります。以下、いくつかのアイデアを紹介します。

1. 評議会に立候補する
2. 評議会の候補者と次点者に投票する
3. 議案の提案または賛成
4. レファレンダムへの投票
5. エコシステム構築者とアンバサダーのためのヒントを提出する
6. Polkassembly、Element、Discord、およびRedditでの議論に参加する

これらのプロセスの詳細は、Polkadot wikiでご覧いただけます。

エコシステムの成長に貢献する

もし、ネットワークの確保や管理のどちらにも興味がない場合は、ビルダーやアンバサダーになることを検討してください。

＜ビルダー＞

ビルダーとは、パラチェーン、ランタイムパレット、スマートコントラクト、Dapps、開発者ツールの開発に取り組む個人または個人のグループのことを指します。ビルダーとして、Web3 Foundationに助成金を申請したり、オンチェーンTreasuryに支出案を提出したりすることで、資金を得ることができます。また、現在および将来のSubstrate関連プロジェクトを特定し、支援し、指導するプログラムであるSubstrate Builders Programに参加することも可能です。

＜アンバサダー＞

この役割は、Polkadot・アンバサダー・プログラムの一部として提供されるポジションとは異なっており、こちらの応募フォームに記入することで参加できます。アンバサダーの主な責任と義務は、ネットワークの成長と普及を促進することです。これは、最終的な目標を達成するためであればどの様な方法を用いても構いません。例えば、本やブログを書くことはこの目的のためにふさわしい仕事ですが、ウェビナーの録音、作曲、ミートアップの主催、オーディオビジュアル解説の制作なども該当するでしょう。繰り返しにな

りますが、あなたの想像力は無限大です。エコシステムが恩恵を受けると思われるプロジェクトがあれば、ここで紹介する手順でオンチェーンTreasuryからの資金援助を申請することができます。ちなみに、この本はPolkadotのオンチェーンTreasuryから受け取った資金によって実現した、オリジナルのアイデアです。

DotSamaの情報をキャッチアップしよう

ネットワークに参加するための最初のステップは、エコシステムの最新情報を入手することです。以下は、エコシステムの発展を追跡するのに役立ついくつかの重要なリソースへのリンクですので、ぜひ欠かさず情報をご覧ください。

1. DotLeap

これは、私（著者）とBruno Škvorcによって運営されている週刊ニュースレターです。DotSama（Polkadot + Kusama）エコシステムの最も注目に値するアップデートを発行することに焦点を当て、リレーチェーン、パラチェーン、Dapps、パラスレッド、コミュニティ、その他多くのニュースをカバーしています。SubstackとSubsocialで毎週公開される、まさにエコシステムの包括的な概要です。

2. parachains.info

DotSamaに関する情報を網羅したサイトで、クラウドローン、オークション、パラチェーンプロジェクトなどの情報を紹介しています。トークンの供給量と価格、投資家、ロードマップの進捗、Web3 Foundationの助成状況など、クラウドローン、オークション、パラチェーンプロジェクトに関する情報が掲載されています。また、パラチェーン公式プロジェクトのニュースを集約したニュースタブも用意されており、こちらもコミュニティ主導のプロジェクトで、オンチェーンTreasuryから資金提供を受けています。

3. Dotmarketcap

このサイトは、Polkadotエコシステムプロジェクト、パラチェーン候補、オークションに関する情報を集約しているという意味で、parachains.infoと似ています。マーケットキャップによってランク付けされた取引可能なプロジェクトのリストと、いくつかの貴重な洞察を提供しており、その最大の利点は、トークン価格とクラウドローンに関するすべ

ての情報が瞬時に更新され、あなたが興味を持つプロジェクトの選択を追跡するためにこのWebサイトを使用できることです。

4. NFT Review

これもgbaci（私）とBruno Škvorcが運営する週刊誌で、NFTとメタバースに強くフォーカスしています。DotSamaやその他のWeb3.0スペースからのNFTニュースをカバーしています。

5. Polkadot Blog

Web3 Foundationが運営・管理する公式ブログです。更新は頻繁ではないので、ブログをご覧になることをお勧めします。もちろん、DotLeapを購読していれば最新のブログ記事が公開されるたびに、更新情報を受け取ることができます。

6. Polkadot Daily Digest

こちらは、Web3 Foundation の教育・コミュニティ担当ディレクターである Bill Laboon がほぼ毎日書いています。このダイジェストには、リレーチェーン、ガバナンス、コミュニティの議論に関する重要なPolkadotとKusamaの最新情報が含まれています。r/PolkadotとSubsocialで見ることができます。

7.dotTreasury

PolkadotのTreasuryに関する情報を探すのに最適なWebサイトです。Treasuryの積立金、収入、支出、その他の財源に関する情報を提供しています。

8. Polkadot A to Z

Web3 Foundationの技術教育者であるEmre Surmeliによる教育シリーズです。PolkadotとSubstrateの技術に関するコアな技術情報を、1つずつコンセプトごとに紹介しています。コンテンツは短く消化しやすい形式で提供され、現在Redditで公開されています。

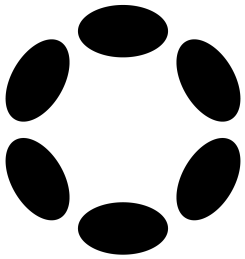
9. Guide to Polkadot-JS

コミュニティメンバーであるAnaelle LTDが作成したPolkadot-JS Apps and Extensionの機能性を非常に分かりやすく紹介しています。ウォレットの操作を初心者にもわかりやすくするために、ステップ・バイ・ステップで説明されています。

10. Ser, Have ya 'Heard?

コミュニティメンバーであるJay Chrawnnaが毎日配信している教育用ビデオシリーズ。DotSamaのエコシステムにおける最新のニュースや開発について、一般視聴者向けに非常に面白いフォーマットで分解して説明しています。現在、YouTubeで公開されています。

以上がPolkadotをより詳しく知るためのニュースソースのご紹介でした。
皆さん、「パラバース」へようこそ！



技術面についての付録

BABEとGRANDPAについて

（このコンセンサスメカニズムは、Polkadotのフォークレスアップグレードによって将来変更される可能性があることにご留意ください）。

　BABEとGRANDPAの話をする前に、コンピューターのプロトコルについて説明する必要があります。
まず、ブロックチェーンはプロトコルであることを常に覚えておいてください。しかし、プロトコルとは何でしょうか。プロトコルとは、コンピューターのソフトウェアが動作するための手順の集まりです。プロトコルは、そのルールが最初から明確であるため、信頼することができます。そしてプロトコルはコンピューターが行う自動化された動作のセットと考えることができます。

さて、プロトコルについて知っておくべき重要なことは、プロトコルはその中に多くのプロトコルと、サブプロトコルを持つことができるということです。つまり、ブロックチェーンがプロトコルであるということは、ブロックチェーンがサブプロトコルのプロトコルであり、各サブプロトコルは他の更にサブとなるサブプロトコルを持つことができることを意味しているのです。各サブプロトコルやサブ・サブプロトコルは、特定のタスクを担当します。
したがって、それ自体がプロトコルであるPolkadot・リレーチェーンの場合、さまざまなサブプロトコルやサブ・サブプロトコルが存在することになります。リレーチェーンプロトコルのサブプロトコルとして、BABEとGRANDPAがあるのはこのためです。
ここまでで、BABEの紹介ができるようになりました。コードの読み方を知っているオタクな方々にとっては、かなりセクシーな存在です。しかし、我々素人にとっては、強力ではあるものの、実態についてはよく分かりませんので、もう少し詳しくみていきましょう。

BABE - ブロック拡張のためのブラインド・アサインメント

BABEはリレーチェーンのサブプロトコルで、ブロック生成を制御します。これを安全かつ非中央集権的に行うために、いくつかの優れた手法を用いています。

ブラインド・アサイン、別名ランダム・セレクション

最初に紹介する仕組みは、ブラインド・アサインというプロセスです。どのノードが次のブロックを作るかを決めるには、ランダムに決める方法と決定論的に決める方法の2つがあります。あるノードが前もってX個のブロックを提供することを知っていた場合、そのノードはこれらのブロックに含める偽の取引を作成することができてしまうので、BABEはランダムに選択を行います。つまり、ノードはどのブロックを生成するか事前に知ることができません。具体的な仕組みは専門的すぎて本書では説明できませんが、BABEはブロックを生成するノードをランダムに選択することだけは覚えておいてください。もうひとつ、本書で詳しく説明しない理由はBABEが近々Polkadotを去るという噂があるからです。BABEの複雑さを解消するために多くの時間を費やしてきたのに、1年も経たずに修正を余儀なくされるのは非常に残念なことです。

複数の割り当て、別名バックアップの作成

BABEでは、より高度な非中央集権化を実現するために、異なるノードに同じブロックを生成するよう割り当てています。その目的は、ブロックの生成に競争力を持たせることで、ブロックの有効性について異なるノード間で対立が発生した場合、すべてのノードがあらかじめ定義されたパラメータに従って、どのブロックが最も有効か投票できるようにするためです。なお、これはプロトコルであることを忘れないでください。
複数割り当てのもう一つの利点は、ブロック生成に選ばれたノードがオフラインになったり、他の問題でブロック生成ができなくなったりすることがあることです。このような場合、ネットワークがフォールバックできるセカンダリーブロックが常に生成されていることになります。このように、ブロック生成待ちのノードには、BABEによって決定されたプライマリーブロックプロデューサーと、複数のセカンダリーブロックプロデューサーが存在するのです。

BABEには他にもサブプロトコルがありますが、今回紹介したものが最も注目されるものです。これ以上の情報は、技術的な領域に深く潜ることを推し進めるだけです。それについては、BABEに関する研究論文を読むことをお勧めします。

GRANDPA（グランパ） - ファイナリティ・ガジェット

BABEと同じく、GRANDPAもサブプロトコルです。しかし、BABEとは異なり、ブロックが有効であることを検証し、元に戻すことができないことを確定するファイナリティに重点を置いています。つまり、BABEはネットワークが非中央集権的にブロックを生成するのを助けるのに対し、GRANDPAは非中央集権的にブロックを確定するのを助けるのです。これは、さまざまなフォークの分岐に対して投票を行うことで実現されます。
BABEは同じブロックを生成するのに異なるノードを選択するため、どのブロックシーケンスが有効であるかという疑問が常に存在します。これは、GRANDPAが登場する前に、BABEがいくつかのブロックとそれに関連するフォークを作成するためです。つまりGRANDPAの仕事は、チェーンのどのフォークが最も有効かを決めることなのです。

“Polkadotにもフォークがあるのか！？”と疑問に思われるかもしれません。この文脈では、これらのフォークは確定されていないため「faux-forks」（偽のフォーク）と呼ぶ方が適切でしょう。一旦フォークが確定すると、他のフォークは放棄され、ネットワーク上のすべてのノードがGRANDPAの決定を受け入れることになります。しかし、GRANDPAはどのように判断し、どのように信用すればいいのでしょうか。ひとつには、GRANDPAはプロトコルなので、指示されたことだけを実行します。この点については、できるだけ専門的な内容を避けながら説明します。

1). 最後の確定したブロックとの関連
GRANDPAによって最後に確定したブロックから来るフォークは選択肢として有効であると見なされる。

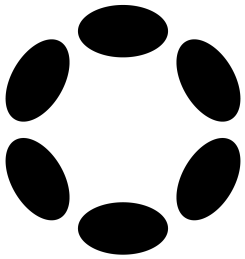
2). プライマリーブロック数 - プライマリーブロック数が最も多く含まれるフォークは、より高いウェイトが与えられる。プライマリーブロックとは、BABEがプライマリノードとみなすノードが生成したブロックのことを指す。BABEは同じブロックを生成するためにノードを選択し、他のノードはセカンダリと呼ばれることに注意が必要。

GRANDPAは、これらの要件を満たすブロックから最も有効であるブロックを選択することができます。

BABEとGRANDPAの主な目的は、リレーチェーンにコンセンサスとファイナリティ、すなわちセキュリティを達成するための非中央集権化された方法を提供することです。

非中央集権化が進むことは虚偽を含む中央集権的な管理ではなく共有された事実に基づいて動作することが保証されるため、今後も支持され続けると予想されます。

もし、あらゆる悪意を持ったユーザーがチェーン上のデータを不正に操作しようとしたとしても、それは不可能に近いと言っていいでしょう。



著者紹介

gbaci

非中央集権化とDotSamaエコシステムに情熱を注ぐライターであり、フィルムメーカー、ミュージシャン。
2020年12月にブロックチェーン技術の深堀りを始めて以来、Polkadot Ambassador、RMRKのHead content writer、NFT ReviewとDotLeap-Polkadotと、Kusamaに関するあらゆる事柄に関する週刊ニュースレターの共同編集者を務める。

「RMRKはすべての人に使われる唯一のNFT標準になる」という強い信念を持つ。
また、Gillian Baciという名前でプロとして音楽を制作しており、作曲可能なマルチメディアコレクションという形でSingularからリリースしている。

暗号資産の話や作曲をしていない時は、小説や脚本を書き、映画を撮影し、本を読み、永続的なインパクトを生み出すための斬新なアイデアで遊んでいる。
地球市民として彼はすべてにつながっており、私たちは社会と宇宙全体でひとつであると信じている。

Twitterでは、@gbaciXというハンドルネームで彼を見つけることができる。