

## 第7回：イーサリアムの今後



## 注意点

### ▼Not Investment Advice

資産運用はリスクが伴うものです。クジラの管理人は投資対象の展望を伝えることもあります。投資は一切推奨しません。自己責任でお願いします。

### ▼Do Your Own Reserch

闇雲に情報を信頼せず、自分で学んで考える姿勢を持ちましょう。  
資金を失うことも珍しくはありません。

### ▼No Promotion

くじらの管理人で紹介するサービスには原則プロモーションを含むことはありません。仮にプロモーションを含む場合は開示します。

An aerial view of a city skyline, likely New York City, with a strong blue color cast. The image shows numerous skyscrapers of varying heights and architectural styles. In the foreground, several buildings are visible, including one with a prominent circular feature on its roof. The background is filled with more buildings, some partially obscured by a layer of white fog or smoke that rises from the city. The sky is a uniform blue, and the overall atmosphere is hazy and monochromatic. The text 'イーサリアムの課題' is centered in the middle of the image in a white, sans-serif font.

# イーサリアムの課題

## ■ イーサリアムとは



### イーサリアム(Ethereum)

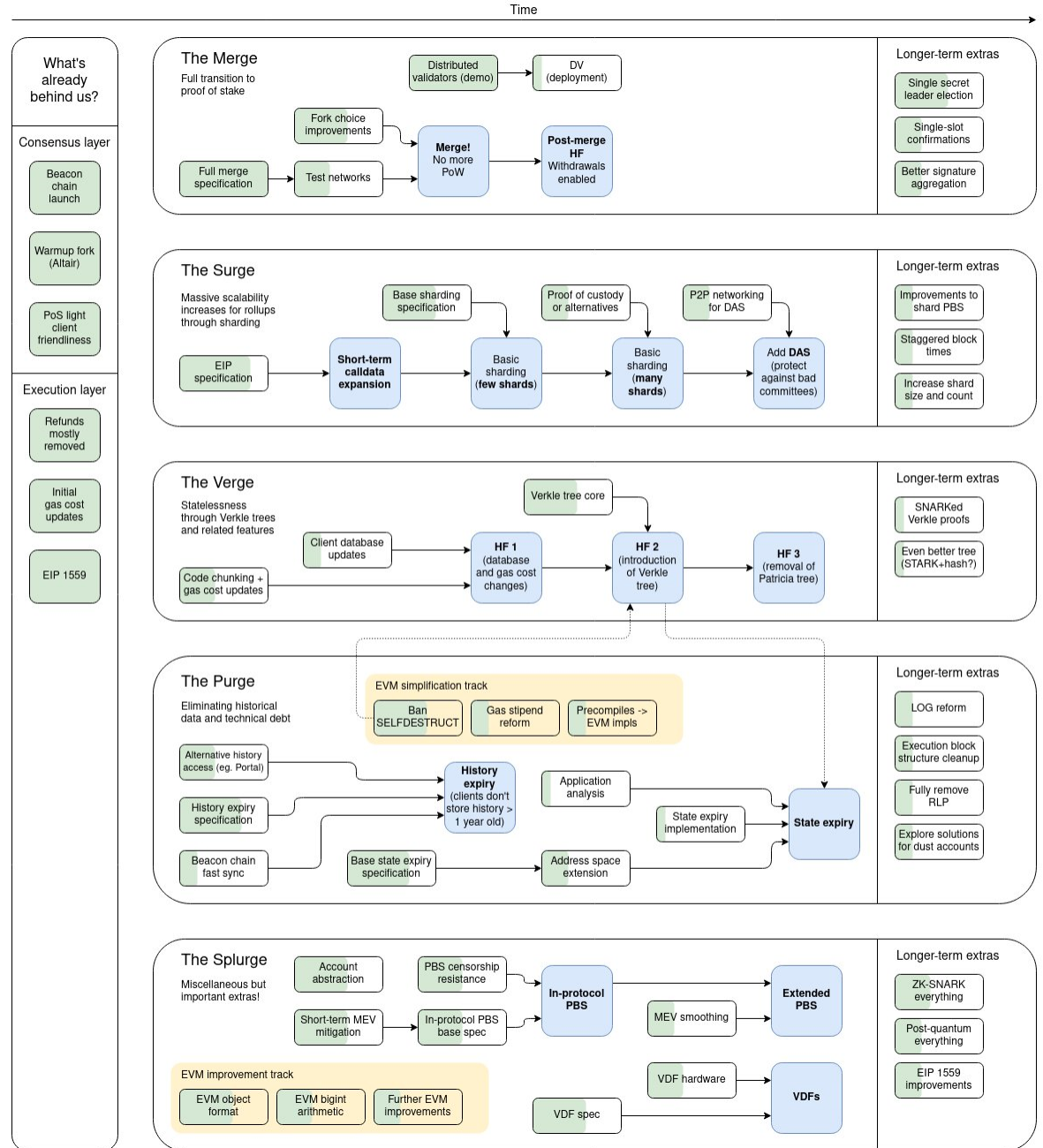
分散型アプリケーション開発用の  
プラットフォーム

アプリの開発ができるコンピュータのようなもの



# ■ イーサリアムのアップデート

イーサリアムのプラットフォームの課題を解決するための数多くのアップデートが予定されています。



# イーサリアムの課題

現状イーサリアムの最も大きい課題はスケーラビリティ問題です。

## スケーラビリティ

コンピュータやシステムが負荷の増大に対して破綻することなく機能を拡張できる能力のこと。

1つのブロックが生成される時間、1つのブロックに記録できる取引の量は決まっている。

赤が青に1ETHを支払った

取引：●が●に●をあげた

取引：●が●に●をあげた

取引のブロック

取引のブロック

最後尾



赤が青に  
1ETHを支払う



ブロックチェーンの利用者が増加すると、記録待ちの長蛇の列ができる。



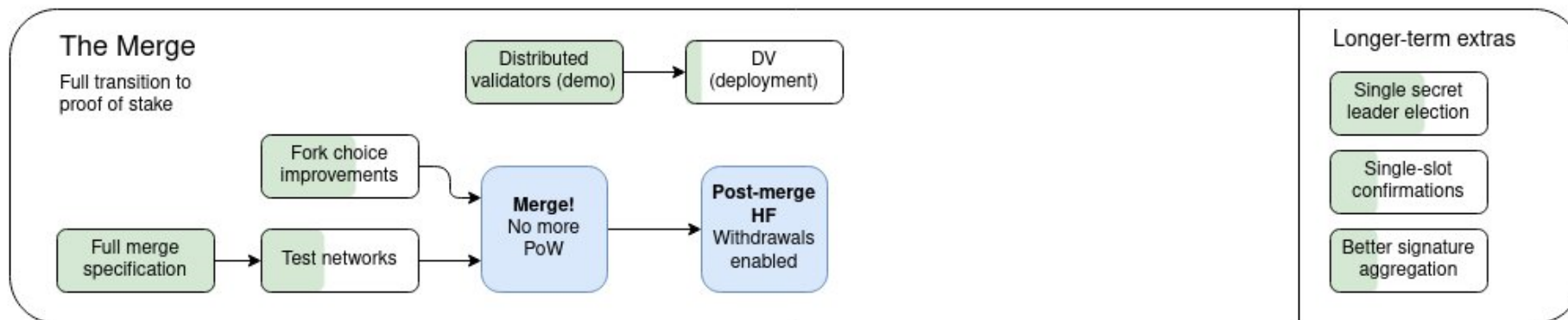
取引を早く記録してもらうために、マイナーに支払う取引手数料を引き上げる。結果、取引手数料の水準が上昇する。

参考：2022年の4月現在  
1回の取引で3000円程度の  
取引手数料がかかっている。

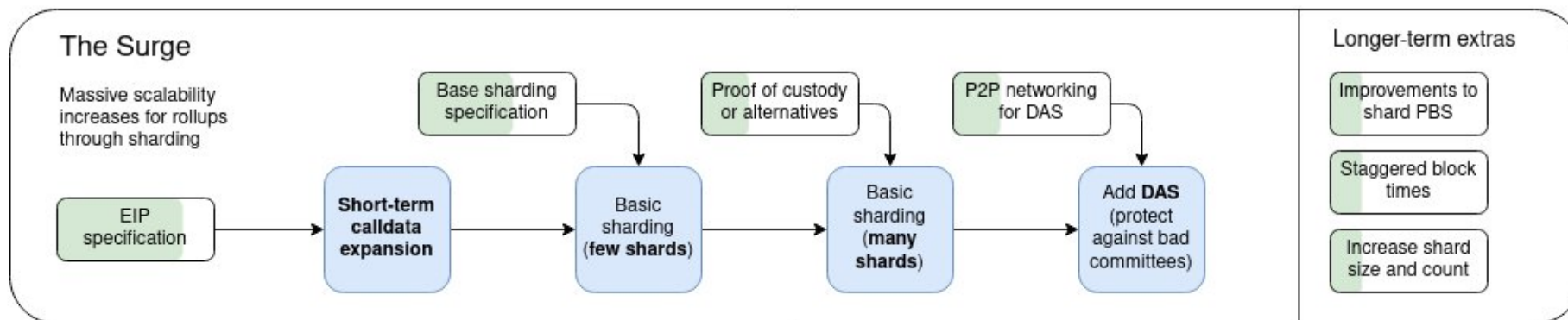
# ■ 直近予定されているアップデート

2022年～2024年の直近1～2年においてはThe MergeとThe Surgeという2つの大型アップデートが予定されています。

Proof of Stakeへの完全な移行



シャーディングによる  
スケーラビリティの向上





An aerial view of a city skyline, likely New York City, with a strong blue color cast. The image is hazy, with fog or low clouds partially obscuring the buildings. The text 'レイヤー2とサイドチェーン' is centered in white. 

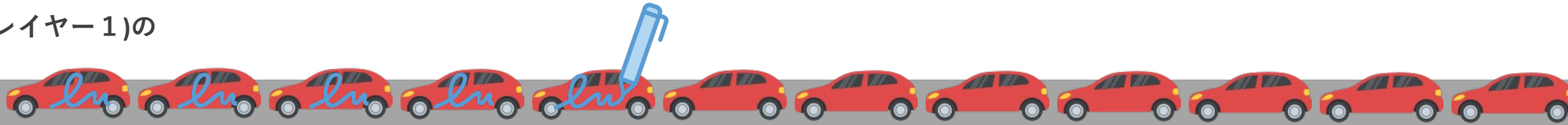
# レイヤー2とサイドチェーン



## ■ レイヤー 2

レイヤー 2 とは、イーサリアム本体（レイヤー 1）のセキュリティを活用しながら、レイヤー 1 とは別の場所で行う取引の処理を行い、スケーラビリティ問題を解決するための方法です。

イーサリアム本体(レイヤー 1)の  
ブロックチェーン



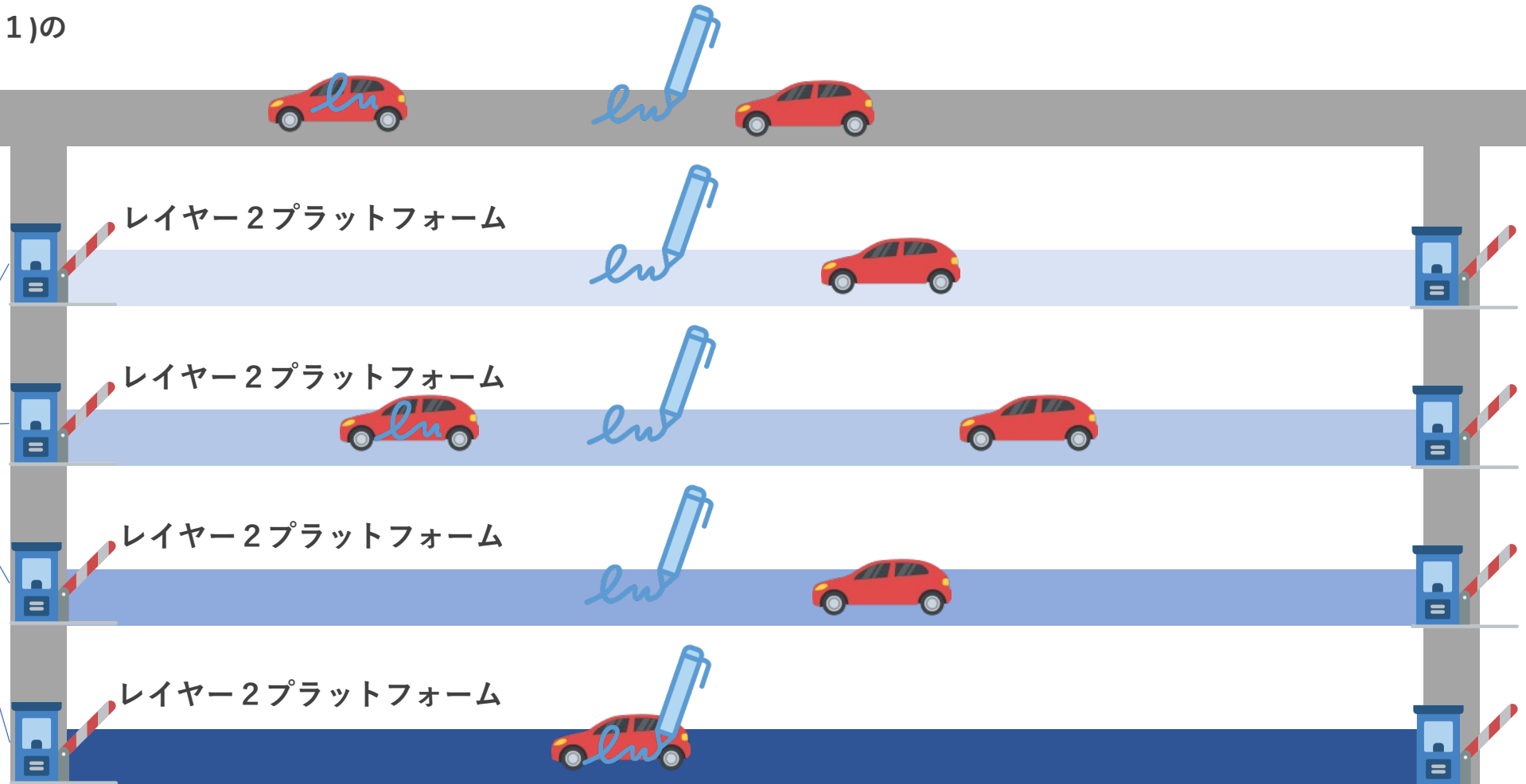
現状は渋滞して込み合っている。

## ■ レイヤー 2

レイヤー 2 では Rollup という技術が用いられており、レイヤー 1 の外側で取引の処理を行い、そこで処理した取引データをレイヤー 1 に戻すことで処理を分散させます。取引データはレイヤー 1 に戻る、つまり、結果的にレイヤー 1 に存在することになるため、レイヤー 1 と同じセキュリティが実現できます。

イーサリアム本体(レイヤー 1)の  
ブロックチェーン

レイヤー 1 は  
レイヤー 2 の  
処理が正しいか  
どうか検証する  
だけの作業に  
集中できる。



レイヤー 2 に処理が分散することで渋滞が緩和できる。

## ■ レイヤー2の代表プロジェクト

レイヤー2のネットワークを開発しているプロジェクトは数多くありますが、以下の3つは特に注目されているプロジェクトです。



**Arbitrum**

レイヤー2で  
最もシェアが大きい。



**Optimism**

レイヤー2で  
2番目にシェアが大きい。





















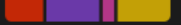













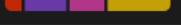




**zkSync**

Rollupにゼロ知識証明という  
技術が使われている。

## ■ レイヤー2のマーケットシェア

レイヤー2のマーケットシェアは「L2BEAT」というサイトで確認することができます。

No.	Name	TVL	Breakdown	7d Change	Market share	Purpose	Technology
1.	 Arbitrum	\$1.98B		-1.60%	50.32%	Universal	Optimistic Rollup
2.	 Optimism <sup>OP</sup>	\$770M 		+11.02%	19.50%	Universal	Optimistic Rollup
3.	 dYdX <sup>◆</sup>	\$708M		-13.50%	17.95%	Exchange	ZK Rollup
4.	 Loopring	\$166M 		+13.85%	4.21%	Tokens, NFTs, AMM	ZK Rollup
5.	 Metis Andromeda <sup>OP</sup>	\$93.14M 		-7.62%	2.36%	Universal	Optimistic Chain
6.	 zkSync	\$58.84M		-2.44%	1.49%	Tokens, NFTs	ZK Rollup
7.	 Boba Network <sup>OP</sup>	\$51.40M 		-11.24%	1.30%	Universal	Optimistic Rollup
8.	 ZKSpace	\$35.51M 		-6.52%	0.90%	Tokens, NFTs, AMM	ZK Rollup
9.	 Immutable X <sup>◆</sup>	\$25.83M 		+2.00%	0.65%	NFT, Exchange	Validium
10.	 DeversiFi <sup>◆</sup>	\$23.07M 		+0.13%	0.58%	Exchange	Validium
11.	 Sorare <sup>◆</sup>	\$17.04M		+8.34%	0.43%	NFT, Exchange	Validium
12.	 Aztec	\$4.99M		-15.56%	0.13%	Private payments	ZK Rollup
13.	 OMG Network	\$3.02M		-0.13%	0.08%	Payments	Plasma
14.	 ZKSwap 1.0	\$1.65M		-4.95%	0.04%	Payments, AMM	ZK Rollup
15.	 StarkNet	\$542K		+3.40%	0.01%	Universal	ZK Rollup



## ■ サイドチェーンとは

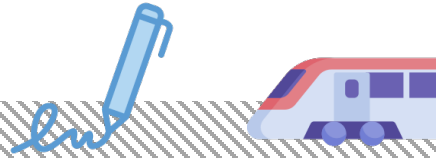
イーサリアムのスケーラビリティ問題を解決するための現状の解決策としてサイドチェーンがあります。  
サイドチェーンとはレイヤー1とは異なるブロックチェーンで取引を処理する技術のことです。

イーサリアム本体(レイヤー1)の  
ブロックチェーン



ブロックチェーンが  
別物

乗り換え(ブリッジ)が必要

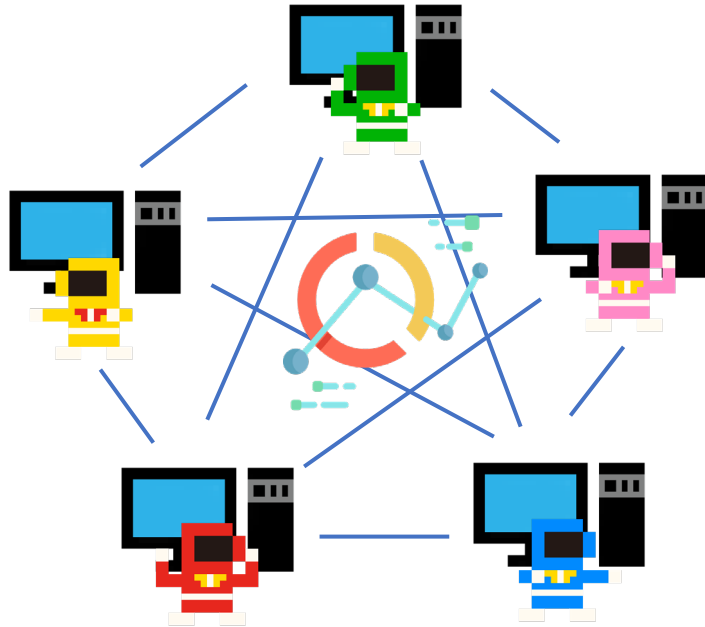


サイドチェーンの  
ブロックチェーン

# ■ サイドチェーンの代表プロジェクト

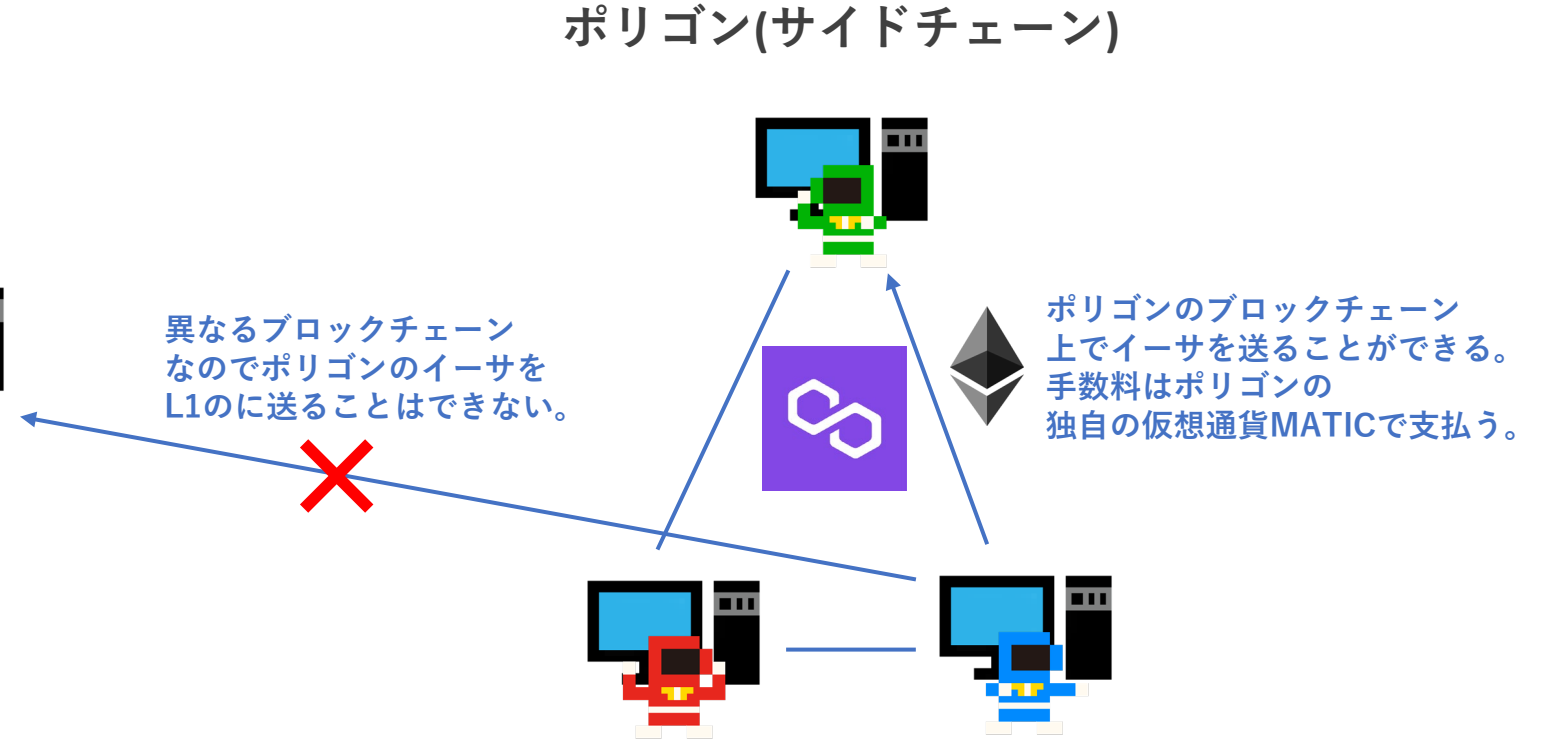
イーサリアムのサイドチェーンのプロジェクトとして代表的なのがポリゴンです。  
セキュリティを犠牲にする代わりに高速で安価な取引が実現できています。

イーサリアム(L1)



イーサリアムのノード数は5663程度と  
ポリゴンよりはるかに多い。  
分散により高いセキュリティを実現している。

ポリゴン(サイドチェーン)



ポリゴンのノード数は100程度のため  
高速で安価な手数料で取引が可能。  
その分セキュリティを犠牲にしている。

取引手数料は1円程度

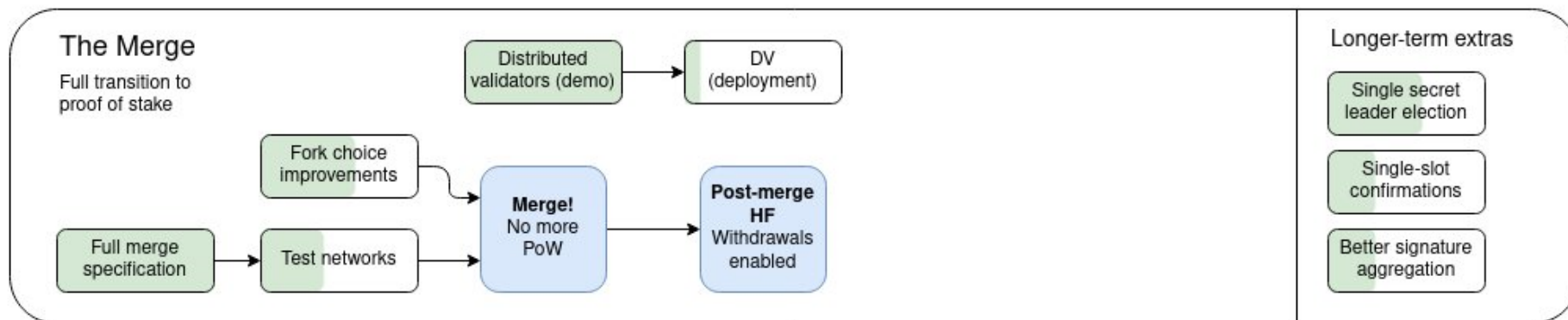
An aerial photograph of a city skyline, likely New York City, with a heavy blue color overlay. The image shows numerous skyscrapers of varying heights and architectural styles. In the center, the text 'PoSへの移行' is written in white. The background is slightly hazy, suggesting a misty or overcast day. The overall mood is professional and modern.

PoSへの移行

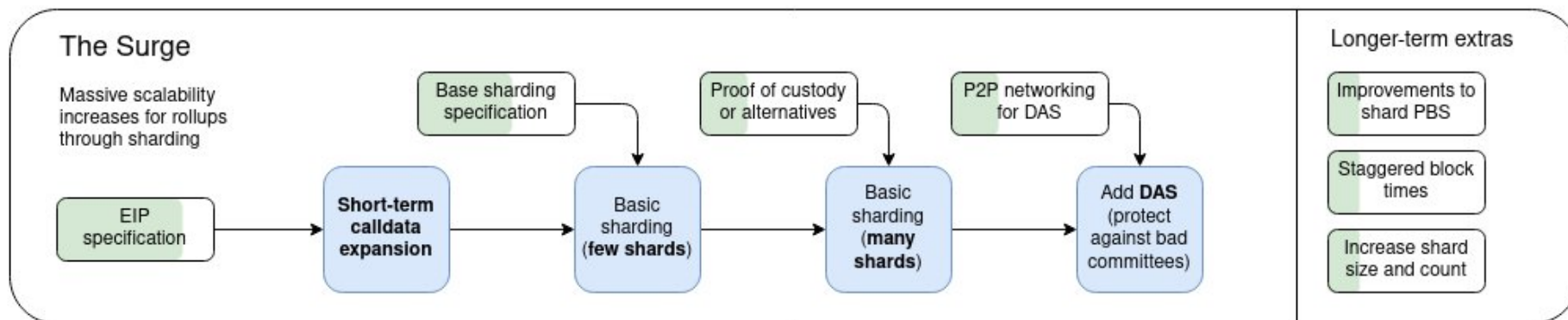
# ■ 直近予定されているアップデート

2022年～2024年の直近1～2年においてはThe MergeとThe Surgeという2つの大型アップデートが予定されています。

Proof of Stakeへの完全な移行



シャーディングによる  
スケーラビリティの向上





## ■ イーサの概要

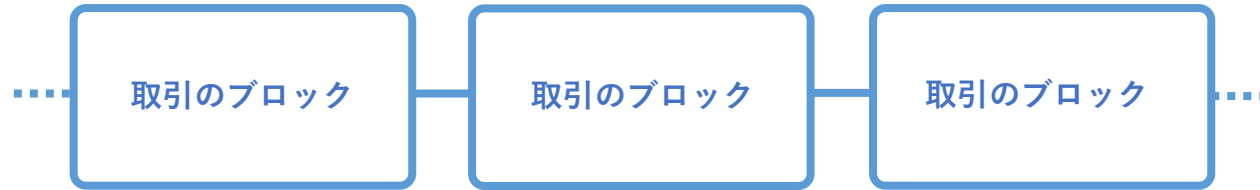
ティッカー	ETH
発行開始年月	2015年7月30日
コンセンサス アルゴリズム	PoW(Proof of Work)
上限発行量	なし
ノード数	約5663(2022年5月時点)
送金時間	約15秒~5分

2022年半ばにPoWからPoS(Proof of Stake)に移行予定。

2022年5月現在約1億2000万枚が流通している。

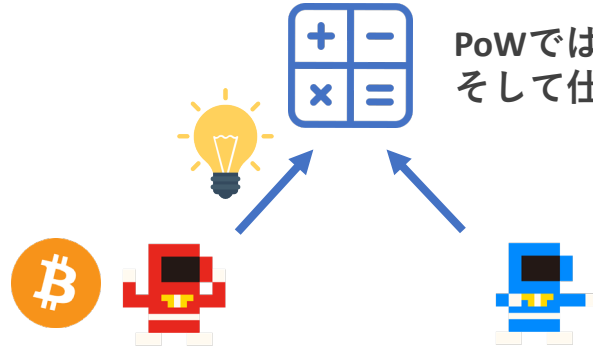
# ■ PoWの復習

## ビットコインの特徴



立会い、記録、証明の仕事を行うルールのことを  
コンセンサスアルゴリズムという。

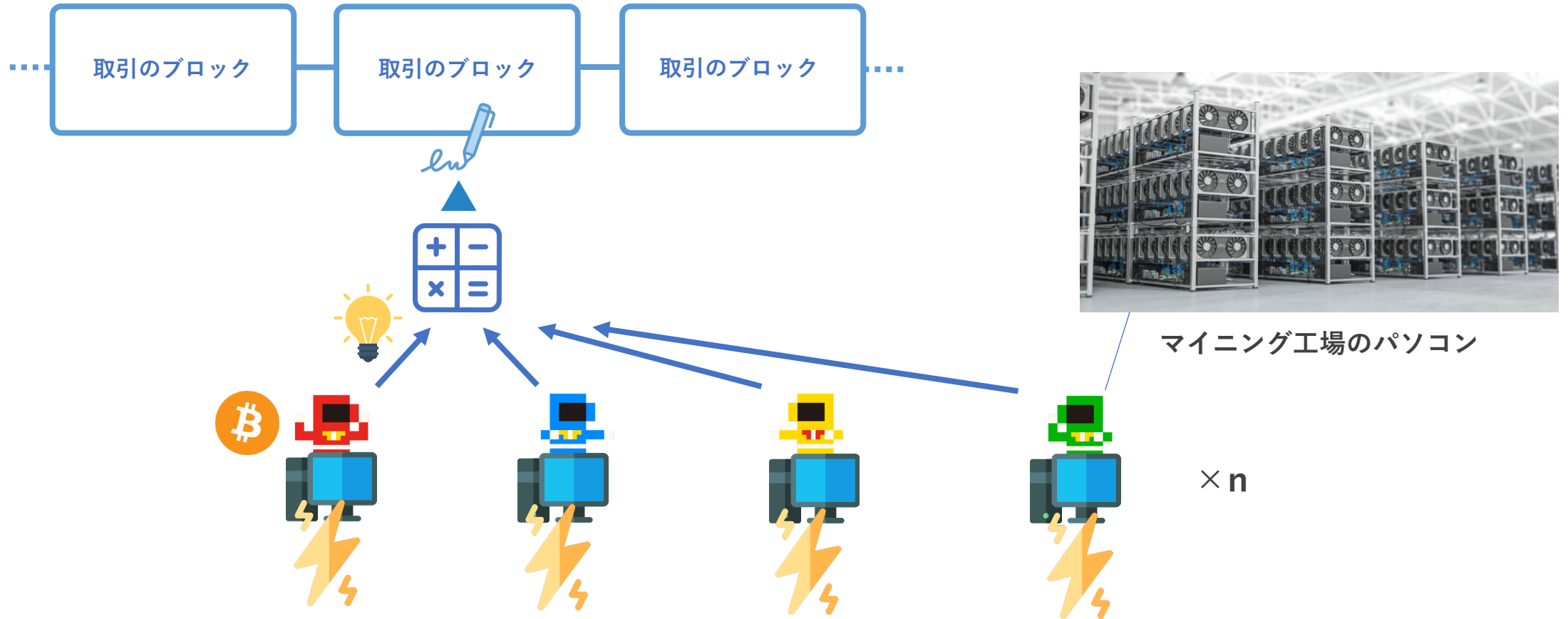
ビットコインのコンセンサスアルゴリズムは  
プルーフオブワーク(PoW)が使われている。



PoWでは、ある計算問題が出題され、一番早く解いた人が一連の仕事ができる。  
そして仕事の対価として新しく発行されたビットコインがもらえる。

この工程をマイニングという。  
マイニングする人をマイナーという。

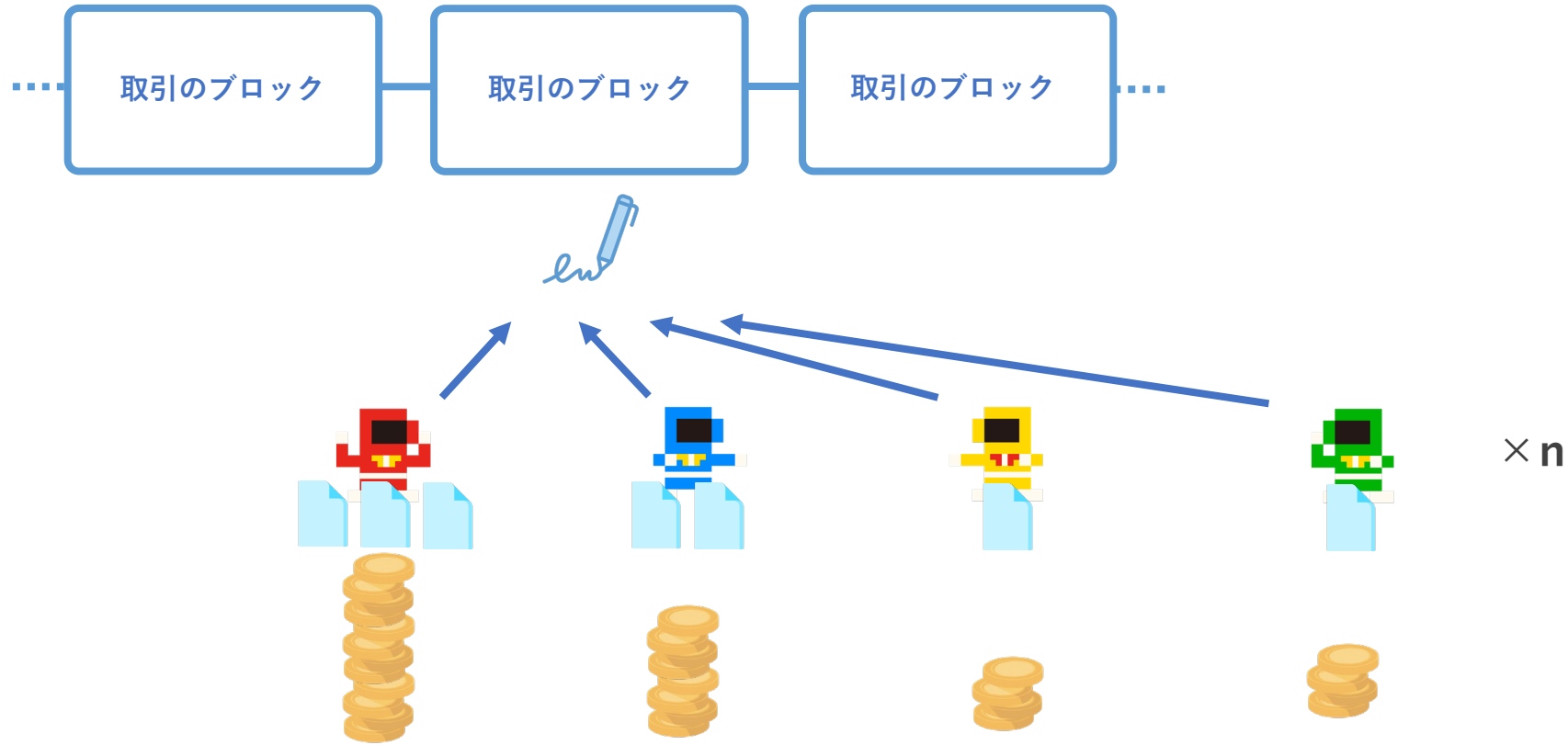
# PoWの問題点



計算問題を解くためにたくさんのコンピュータを稼働するためには電気代がかなりかかる。  
ケンブリッジ大学の試算によるとビットコインのマイニングにより消費する電力はオランダ一国の消費電力とほぼ同じとされている。

このような膨大なエネルギー消費の観点から、PoWに代わるコンセンサスアルゴリズムが研究され始めた。

# ■ PoS(Proof of Stake)①



Proof of Stakeとは一言で「資産の証明」のことです。これは自分の持っている仮想通貨(イーサ)の量によって多数決の票が変わる仕組みです。イーサを持っていれば持っているほど多数決の票を多く獲得できます。

PoWはお金で電力を買って、電力を消費(計算を解く)することで、多数決の票を獲得する仕組みでした。PoSはお金から直接、票を獲得する仕組みであるから、エネルギーを消費を抑えられるわけです(PoWの約0.05%)。



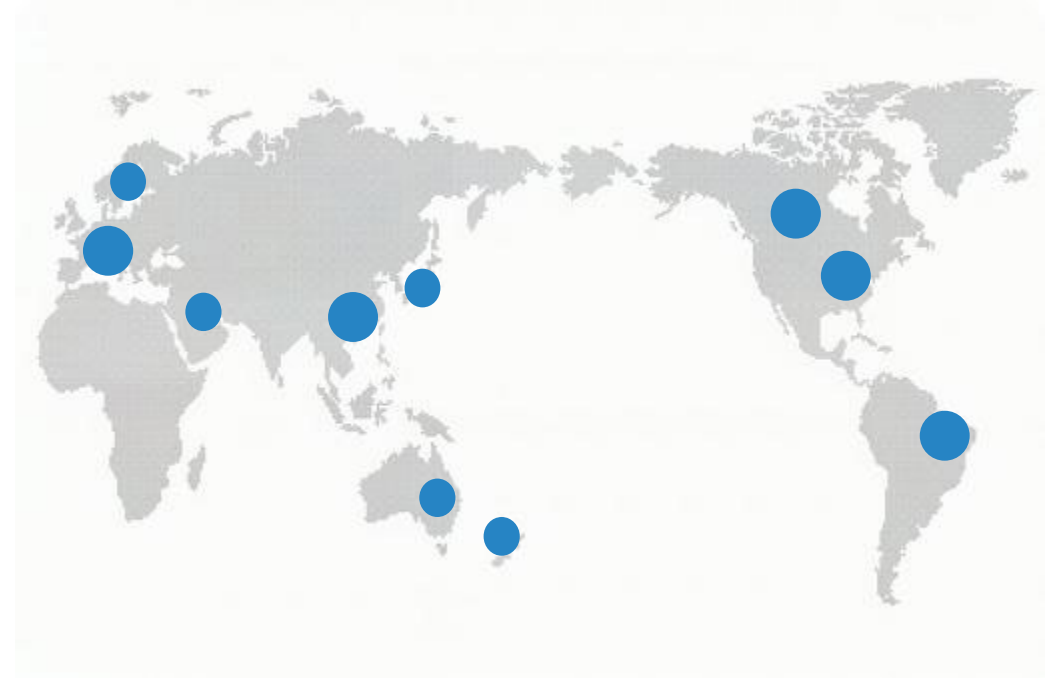
## ■ PoS(Proof of Stake)②

PoSは地理的な分散性の点でもPoWよりも優れています。



PoWの地理的な分散性

報酬を得るために電力を消費するから、  
電力の安い地域に集中しやすい。  
ネットワークセキュリティを弱める方向に作用する。

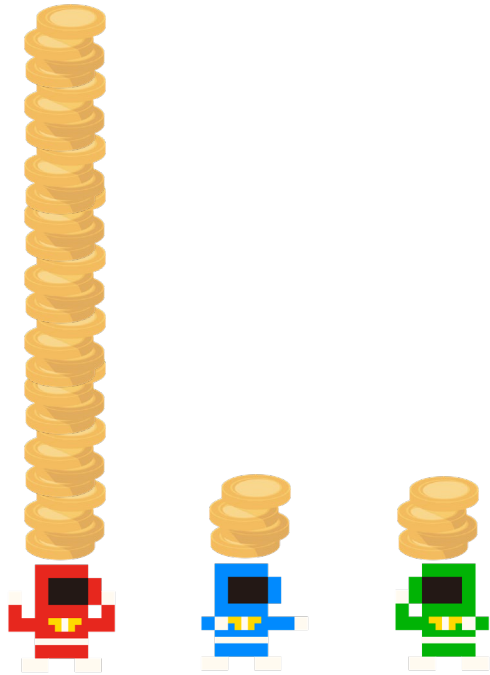


PoSの地理的な分散性

報酬を得るために資産をもっておけばよいので  
世界中のどこでもいい。  
ネットワークセキュリティを高める方向に作用する。

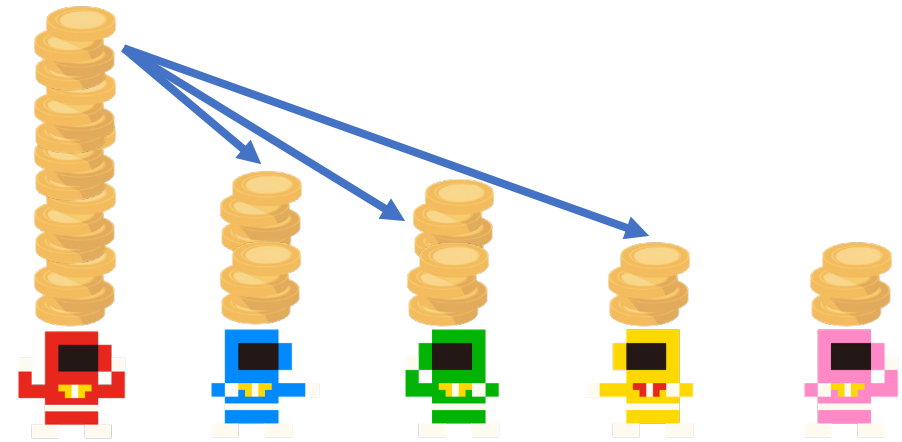
## ■ なぜ最初からPoSにしなかったのか①

イーサリアムのコンセンサスアルゴリズムがなぜ最初からPoSではなくPoWだったのか。それは資産の分散性という観点と深く関わっています。



PoSの資産の分散性

PoSでは資産を多く持つ人ほど報酬(ETH)が得られる仕組みのため、大口保有者は報酬を売らず保有し続けるメリットが大きいです。なので、大口保有者が発行通貨の多くを保有という結果になりやすいです。



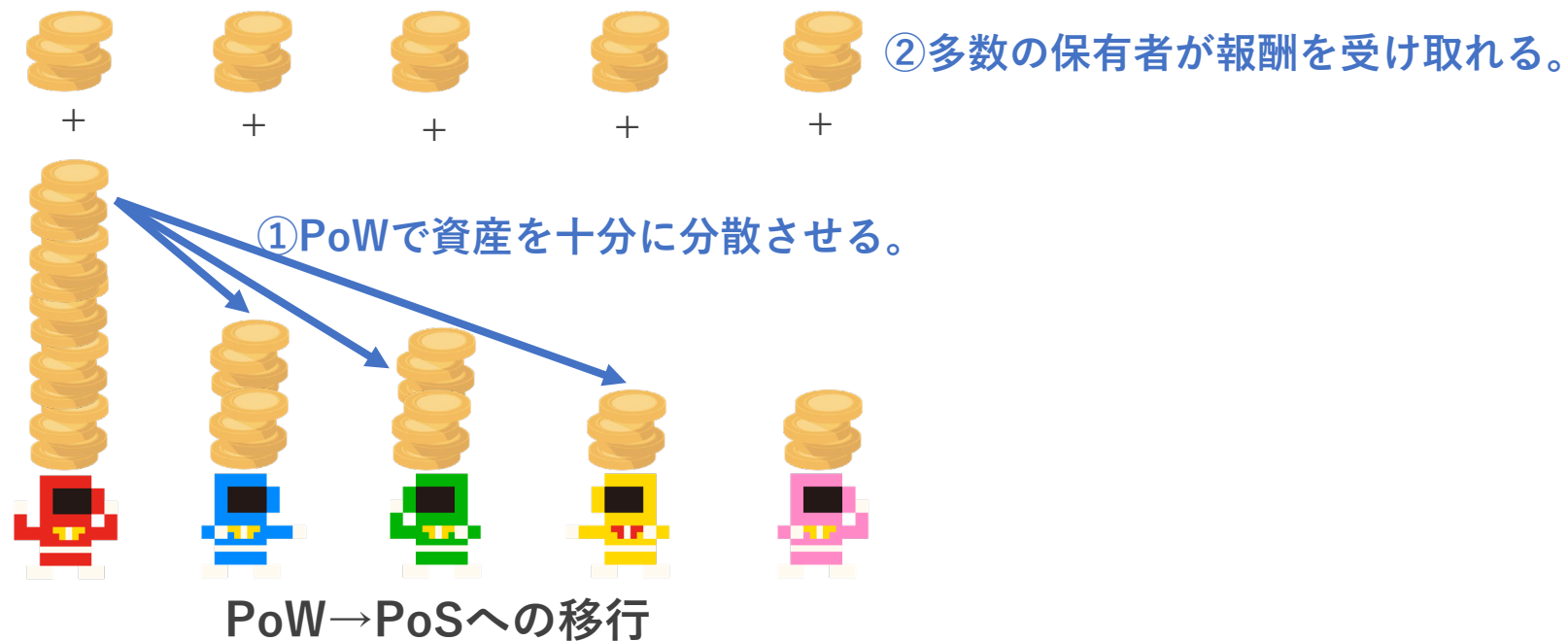
PoWの資産の分散性

PoWではマイナーは電気代をペイするために新規発行された仮想通貨をすぐ売ります。売った仮想通貨は誰かの仮想通貨になります。

資産の分散性という点ではPoWの方がPoSより優れているといえます。

## ■ なぜ最初からPoSにしなかったのか②

イーサリアムはPoWで資産を十分に分散させた後にPoSに移行し、エネルギーの効率性と高いネットワークセキュリティを享受するといういい所どりを旨とした。



イーサを保有して報酬を受け取ることをステーキングという。  
ステーキングするには32ETHを保有する必要がある。  
(小口でもステーキングができるサービスはたくさんある。)



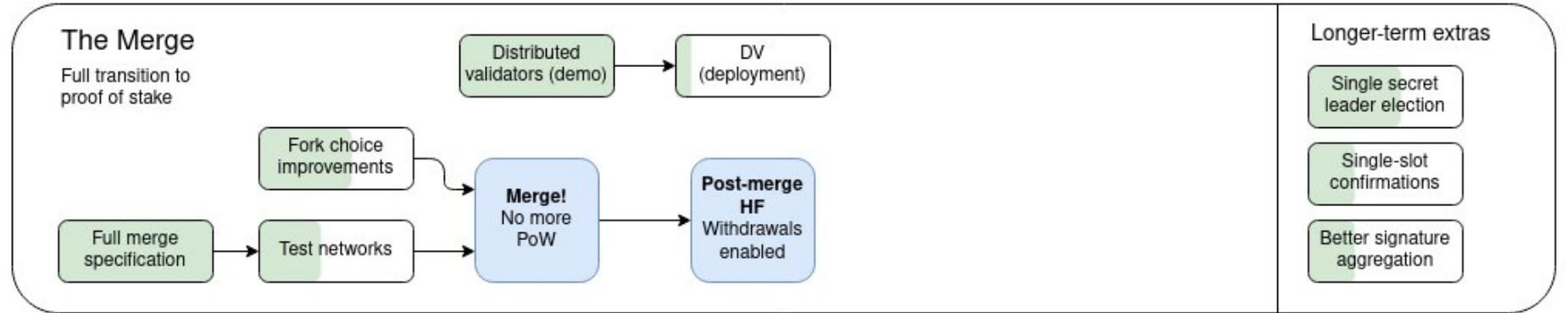
An aerial photograph of a city skyline, likely New York City, with a strong blue color cast. The image is hazy, with fog or low clouds partially obscuring the buildings. The skyscrapers are densely packed, and the overall atmosphere is misty and ethereal. In the center, the Japanese text 'シャードディングの実装' is overlaid in white.

# シャードディングの実装

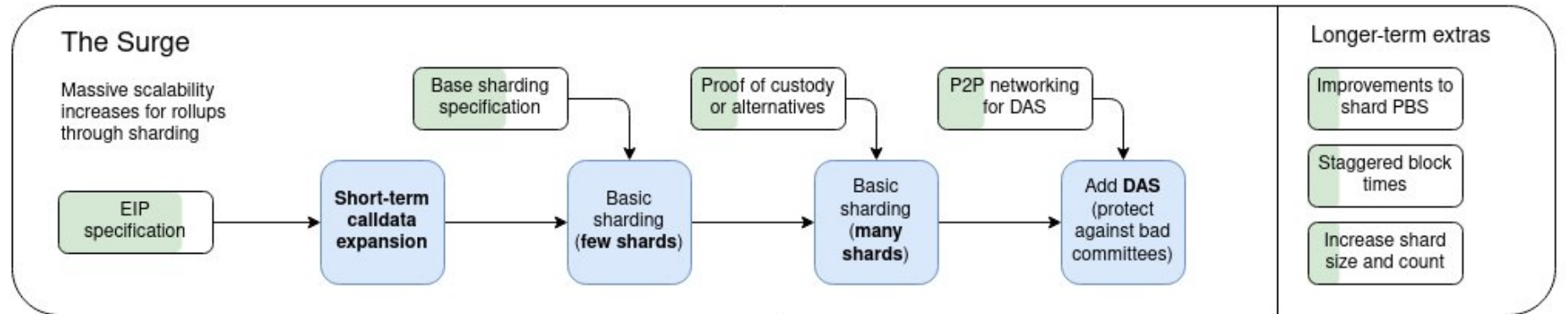
# ■ 直近予定されているアップデート

2022年～2024年の直近1～2年においてはThe MergeとThe Surgeという2つの大型アップデートが予定されています。

Proof of Stakeへの完全な移行



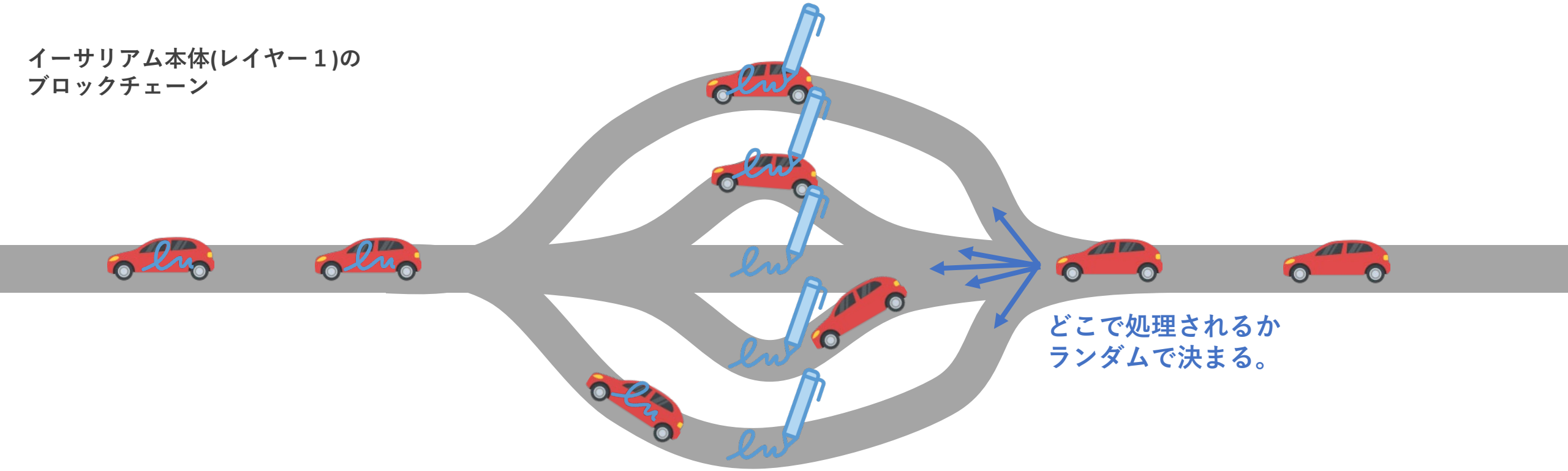
シャーディングによる  
スケーラビリティの向上



## ■ シャーディングとは

シャーディングとはブロックチェーンを複数の並列のチェーンにランダムに分けて処理することで処理速度を大幅に上昇させる技術です。

イーサリアム本体(レイヤー1)の  
ブロックチェーン



シャーディングの実装により取引処理速度と取引手数料の大幅な減少が実現すると考えられています。