

# 自律分散型組織(DAO) としての *Dash*

—ビットコインをベースとしながら独自の進化を遂げる暗号  
通貨Dashの現状

2020年7月30日

ハンドルネーム:とみ三 ([Twitter: @samurai3311](https://twitter.com/samurai3311))

- 2017年3月からDashに関わり始める
- 2017年10月にDashの日本語情報サイト[DashJapan.com](https://dashjapan.com)を開設
- 2018年3月に[Dashフォーラム](#)に[The situation in Japan](#)というスレッドを立て、日本の規制状況等を英語で発信
- 2020年3月に日本から初の予算提案をDashネットワークに提出し、現在資金提供を受けて活動中

【リリース】 2014年1月18日

【創始者】 エヴァン・ダフィールド(2011年からビットコインの開発に携わっていた)

【時価総額】 約790億円(2020年7月28日午前6時現在。[CoinMarketCap](#)のランキングで23位。)

【コードベースと名称の変遷】 リリース時はXCoinという名称でLitecoinのコードをベースにしてスタート。リリース翌月にDarkcoinに改称。リリース翌年3月にBitcoinのコードをベースとし、Dashに改称。



- 目的... すべての人々に経済的自由をもたらす
- 使命... できる限り迅速で簡単、安全で廉価な支払い手段の実現

---

プライバシーに主眼を置いた暗号通貨



ペイメント(支払い)に主眼を置いた暗号通貨

ホワイトペーパーの副題をこちらに更新

## ビットコインとDashの比較(1)

	ビットコイン	Dash
リリース日	2009年1月3日	2014年1月18日
創始者	サトシ・ナカモト	エヴァン・ダフィールド
ハッシュアルゴリズム	SHA-256	X11
ブロック生成間隔	10分	2.6分
採掘難易度調整	2週間ごと	1ブロックごと
ティッカーシンボル	BTC / XBT	DASH
総供給量	2100万BTC	<a href="#">1774万~1892万DASH</a>
ブロック報酬の削減	4年ごとに半減	約383日ごとに7.14%削減
取引の認証方式	Proof of Work (PoW)	Proof of Work + Proof of Service (PoW / PoSe)

## ビットコインとDashの比較(2)

	ビットコイン	Dash
公式クライアント	Bitcoin Core	Dash Core (Bitcoin Coreがベース)
ネットワーク構造	1層	2層(第2層はマスターノードネットワーク)
自己資金調達	なし	あり(ブロック報酬の10%)
ブロック報酬の内訳	マイナーに100%	マイナー45%、マスターノード45%、自己資金10%
意思決定方法	ハッシュパワー	マスターノードによる投票
分散型のプライバシー向上機能	なし	あり
送金の即時承認機能	なし	あり(2秒以内)
スケーリング手法	スモールブロック・オフチェーン	ウルトララージブロック・オンチェーン

## Decentralized Autonomous Organizationの略

分権型で自主的な組織

Vitalik Buterin氏の  
記事を基に作図。  
2014年5月のこの  
記事の中で、彼は  
ビットコインをDAO  
としている。

中枢が自動化

中枢が人間

末端が自動化

末端が人間

AI	DAO
ロボット	旧来型組織

## ビットコインDAO

代表者・中央管理者



存在しない

ネットワークから報酬を受ける「従業員」

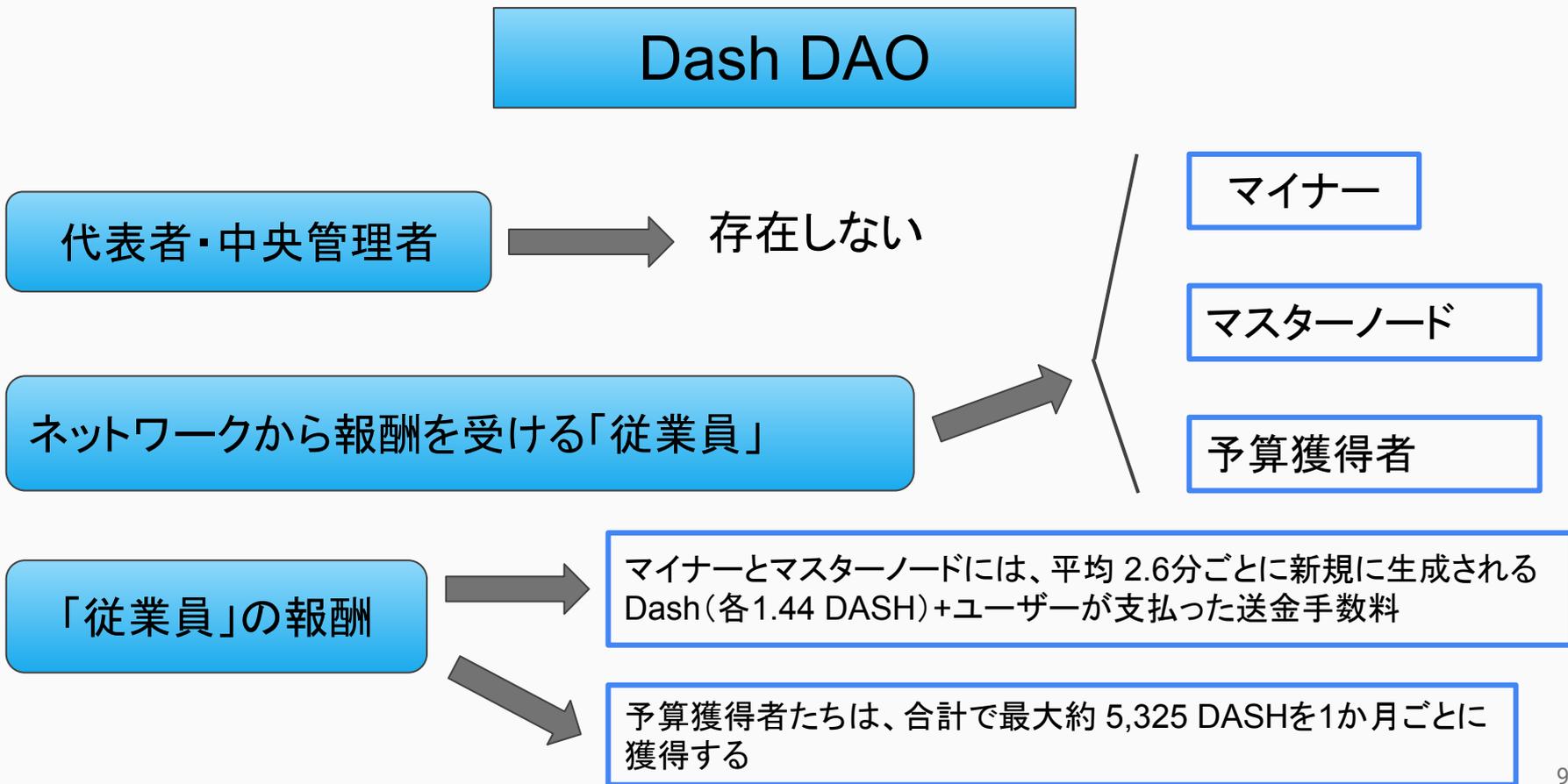


マイナー(採掘者)

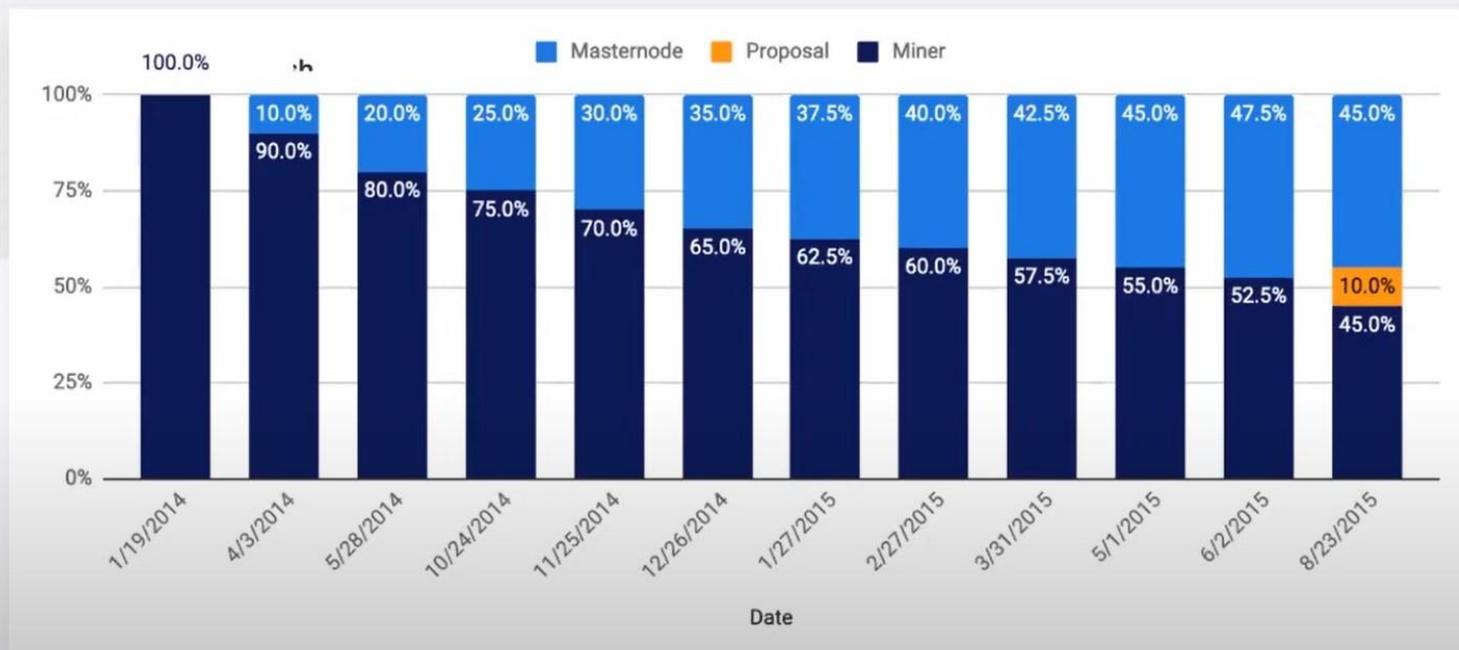
「従業員」の報酬



平均10分ごとに新規に生成されるビットコイン  
(6.25 BTC)+ユーザーが支払った送金手数料

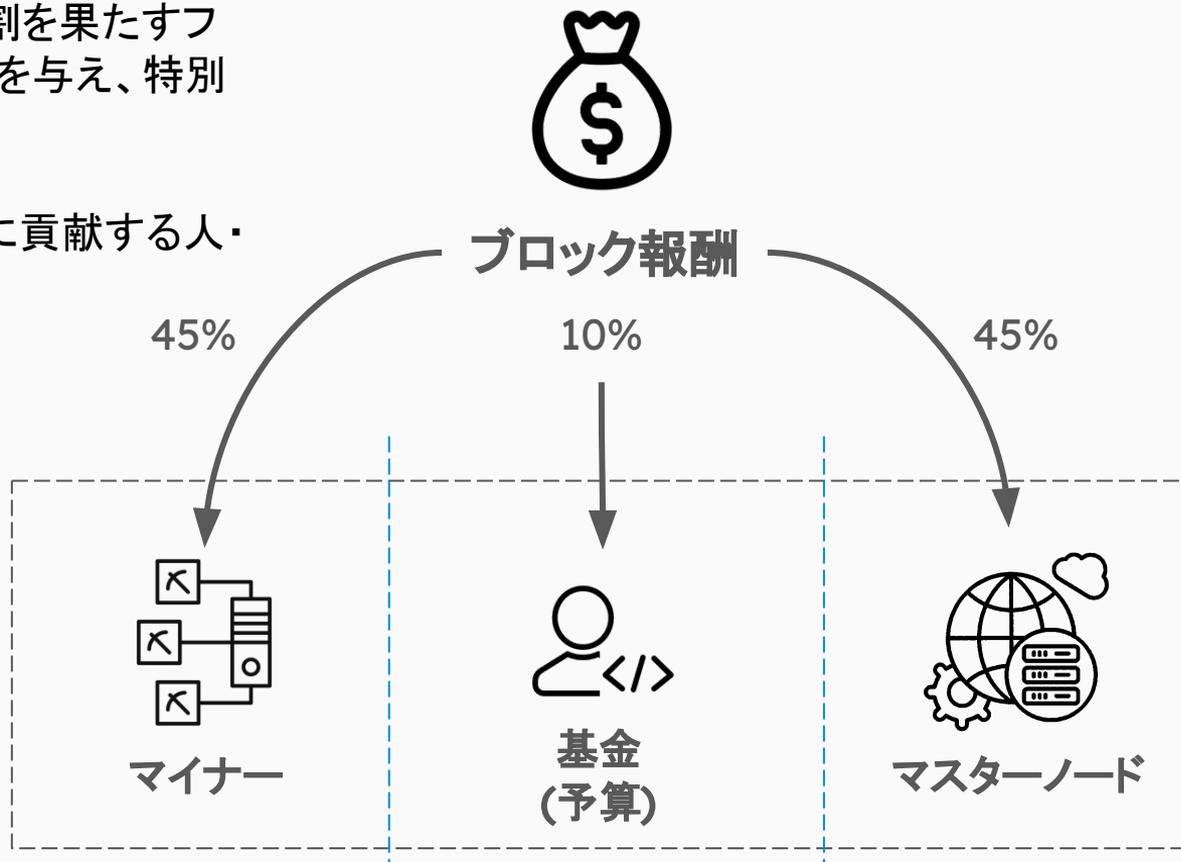


## Reward Allocation History



# 現在のDashのブロック報酬の配分

1. ネットワークで重要な役割を果たすフルノードにインセンティブを与え、特別な役割も持たせる
2. 開発者などネットワークに貢献する人・組織に資金を提供する



※今秋から4年半かけてマイナー36%・マスターノード54% (比率は4対6) にブロック報酬を徐々に再配分する意思決定提案が今月27日に可決された。

DGBB(Decentralized Governance by Blockchain)とも呼ばれる

予算提案(Budget Proposal)への投票

意思決定提案(Decision Proposal)への投票

- 提案の提出にはネットワークに 5 DASHを支払う必要
- 誰でも提出可能

投票権者



マスターノード

1マスターノードが1票を持つ

現在の総数: 4922

16616ブロック(約30.29日)ごとに生成されるスーパーブロックに合わせて投票が行われる  
賛成票から反対票を除いた数がマスターノードの総数の 10%以上に達することで予算提案は可決される

## 現在のマスターノード情報

マスターノード数	4923
マスターノードへの報酬支払間隔	約8.97日ごと
マスターノードへのブロック報酬	1.44 DASH(約12,518円)
1 DASHの価格	8,693円
1,000 DASHの価格	8,693,000円
1年間の価格平均が8,693円だった場合の1年あたりの報酬	約509,372円
1年間の価格平均が21,265円だった場合の投資利益率(ROI)	約5.86%

[Dash Masternode Information](#) をもとに作成(2020年7月29日23時20分現在)

Dashネットワークの価値を向上させるものであることが求められる

提出・議論・投票用プラットフォーム

[Dash Central](#)

[Dash Nexus](#)

2015年8月からこれまでに提出された予算提案と意思決定提案は計 960件

2015年8月から2018年7月までに提出された提案の一覧

<https://dashvotetracker.com/past/>

2017年2月から現在までに提出された提案の一覧

<https://www.dashninja.pl/governance.html#proposalsdetail>

2MBブロックへの移行

2016年1月

新ロゴの決定

2018年3月

ブロック報酬の再配分

2020年7月

2020年7月30日に生成されたスーパーブロックのコインベーストランザクション

票決で予算を獲得した各エンティティは、月に一度生成されるスーパーブロックから新規生成コインを直接受け取る

## Details for Block #1312664

Hash	< 00000000000004a61670e79e305b66ff8e2bba9d792c11c3a0f2618ff0a4926 >
Date/Time	2020-07-30 02:52:05 extracted by Luxor Mining Pool
Transactions	15 <span>15.9 kB</span>
Value Out	4,459.45449477 DASH
Difficulty	182305568.019275
Outstanding	9,628,132.33155775 DASH
Created	4,422.57714099 DASH

Hash	Value Out	From (amount)	To (amount)
322a1dbe...	4,422.57729509 DASH	Generation + Fees	
			XoSxpd5VYNQvKbXbEaDKt6P1aZANzAkXrJ 1.44243961 DASH
			XiioyXCLvK4jPEYTPzUxocAf9jExAzYPhd 1.44243949 DASH
			XvriNAE+rPGGCngw2jjKofVf0NKGbe7zK2mt 264.40939775 DASH
			XuLHt4TN6CinfMM2zHfy7Rsb4terC1MRX5 2,663.0 DASH
			XrUCrVmAwSwwktEMzaJ9OoDY25VeX8umdL 65.28792526 DASH
			Xia9UMRgDMCtXv1vZX76WmDfWTRjhvrQCK 60.0 DASH
			Xt4p2sjNKgPPxYLSdg2xTPFDGGYe9FHDSd 189.0 DASH
			Xvhh4TMs0M6aBmaz87aJX4RZ7MM3dX82h4 60.0 DASH
			XuLHt4TN6CinfMM2zHfy7Rsb4terC1MRX5 400.0 DASH
			XhZNCarmtR64USTpRnUBGUGrs1HFj3mu3q 39.0 DASH
			XpmXvyY3EgfJw5TuFdrCRYcOv2GJK&YhQz 90.0 DASH
			XbFb9b1qa0LyknagDbUwBVBFwSHuWQRhSoc 155.0 DASH
			XsHCKhTW2xAFYCdG1zjKdjuPhxWAHksdRC 62.0 DASH
			XfsuZgsXm45Xhpaas5iavbJACvpeKokW3S1T 118.0 DASH
			XjA2Z53RjSz2xHSSk2fXoP1GN8ZZkvZoy8 116.99509298 DASH
			XnNdk5s2JNPEVYB4brKmfFNuotoujWEuQdd 132.0 DASH
			XnNdk5s2JNPEVYB4brKmfFNuotoujWEuQdd 5.0 DASH

## Dash Core Group, Inc. (DCG)

Dashの開発・マーケティング等をリードする開発チーム

現在、予算の約60%を獲得している

純粋にDashネットワークを成長させることを目的とする企業

2017年7月に米国デラウェア州で設立された株式会社

本拠はアリゾナ州スコッツデール

CEOはライアン・テイラー

2020年7月時点で31名の有給スタッフと7名のボランティアが働く



[チーム詳細](#)

# Dashのメジャーアップデートの流れ (Spork)

新バージョンのクライアントソフトウェアのリリース後、マイナー・マスターノードが更新作業をする

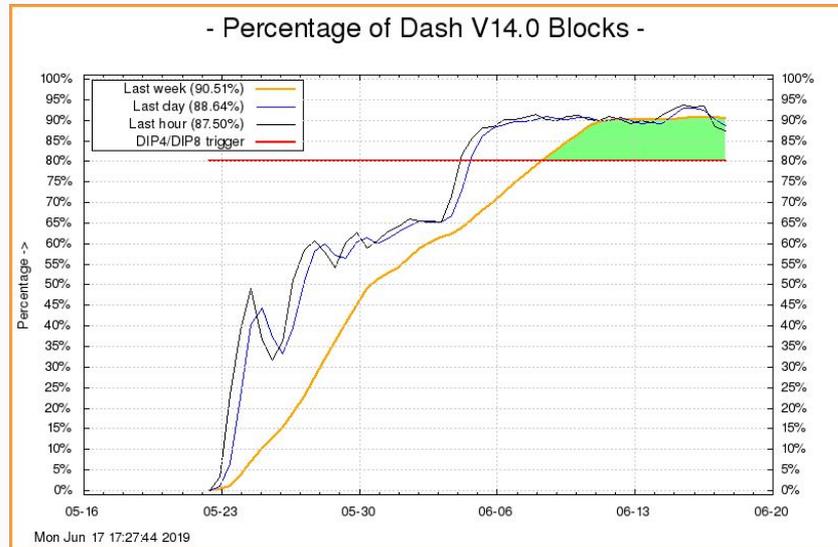


新バージョンのブロックが80%に到達し1週間経過



DCGの複数メンバーがそれぞれの秘密鍵でネットワークメッセージに署名して新バージョンをアクティブ化

脆弱性が見つかった場合は非アクティブ化もできる



古いバージョンのマスターノードは、ブロック報酬を得られなくなるためマスターノードは更新するインセンティブがある

正式名称: The Dash DAO Irrevocable Trust  
ニュージーランドで2017年7月に設立された  
撤回不能信託

委託者  
DCG

受託者  
Dashトラスト

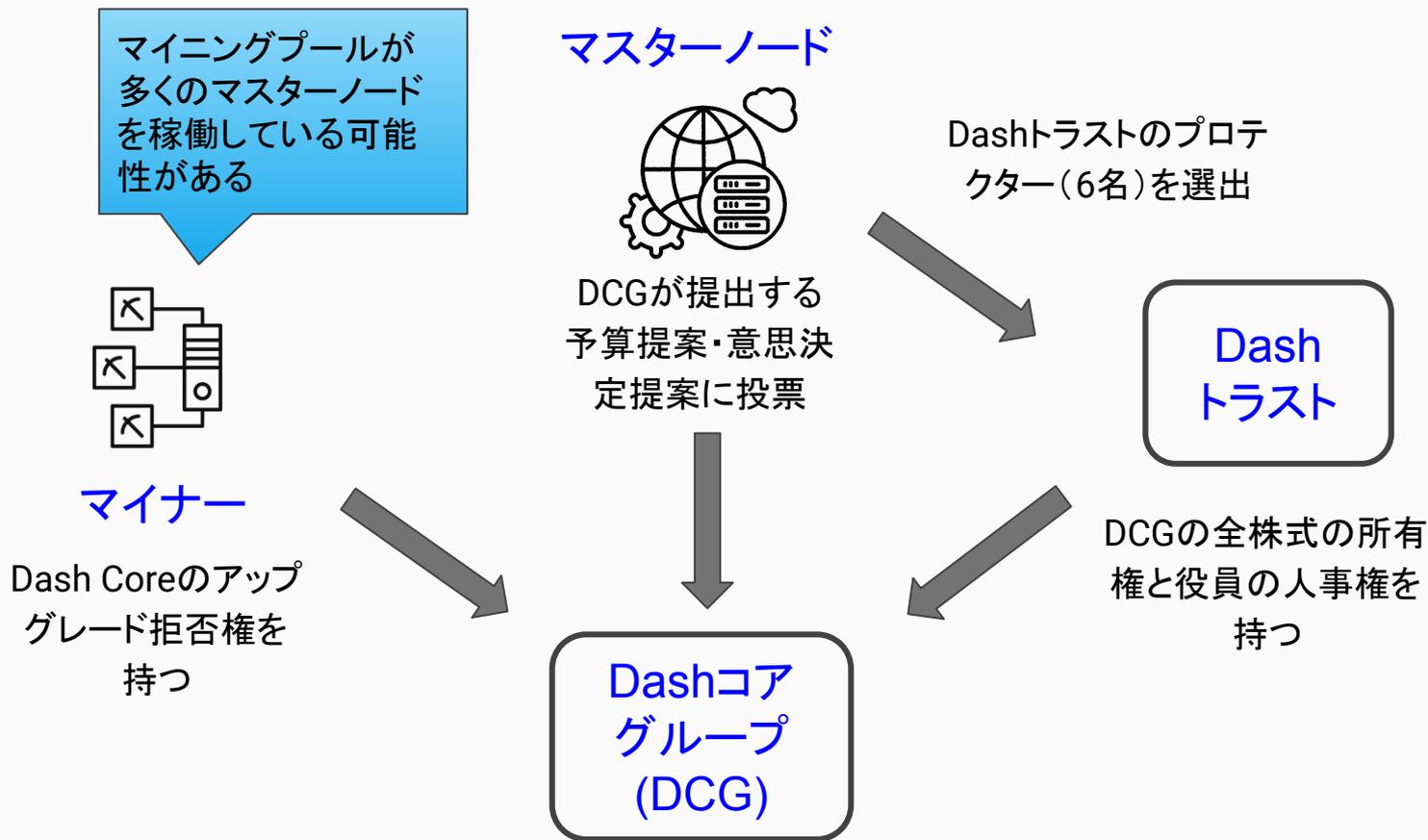
役員にあたるトラストプロテクター6名を毎年選出する

受益者  
マスターノード

## 役割

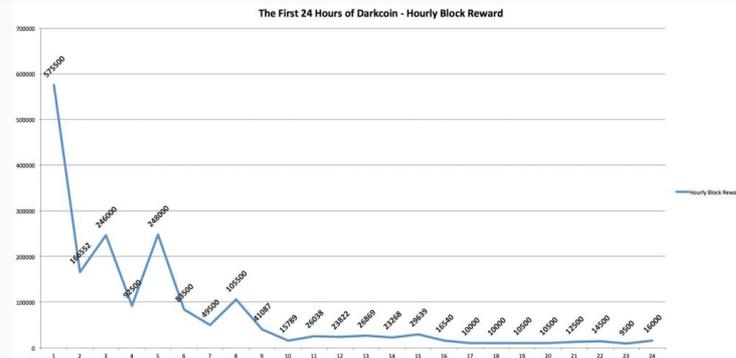
1. DCGの全株式の保有
2. マスターノードの意思決定に基づいてDCG役員の変更人事を行う
3. Dashネットワークに関連する特許権・商標権などを保有する

# Dashのガバナンスシステムを図にすると



リリース後、最初の34時間で約199万DASHが採掘されたという事象

これは、現在までに供給されたDashの約20.8%にあたる



1. リリース時の Dash (当時 XCoin) は Litecoin のコードをベースにしていた。Litecoin はリリース時の難易度が意図的に下げられていて、Litecoin でも最初の 24 時間で約 50 万 LTC が採掘されている。
2. XCoin のリリースは Bitcointalk 上で事前に発表されていた。Litecoin と比べ比較的多数の CPU 採掘者が初めからいたため、採掘の速度が早まった。
3. XCoin の採掘報酬アルゴリズムにエラーがあり、約 21 万 DASH が余分に供給された。
4. 当時の開発チームのメンバーは、エヴァン・ダフィールドとカイル・ヘイガンの 2 人のみだった。カイルは、リリース後数ヶ月以内にすべてのコインを売って以来プロジェクトには関与していない。現在の開発チームのすべてのメンバーはインスタマインよりも後からプロジェクトに参加している。

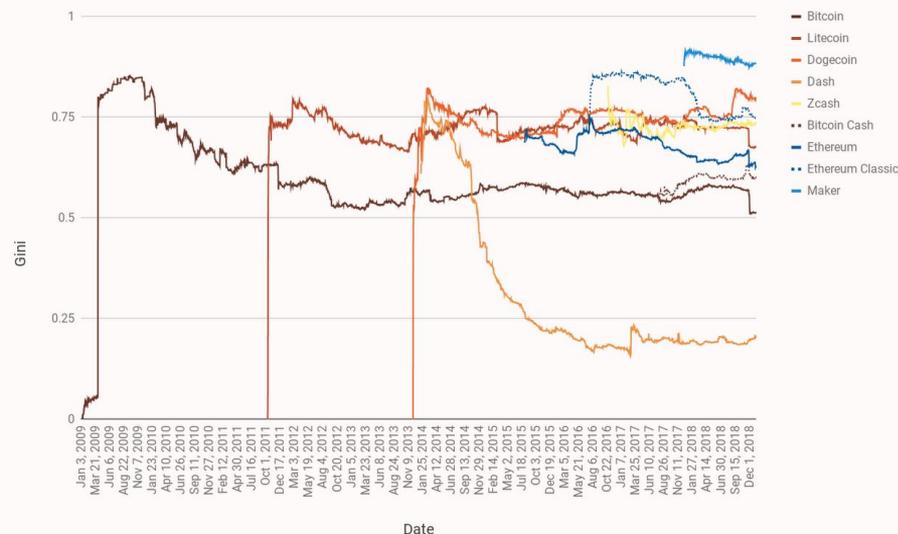
参照元: [Dash Instamine Issue Clarification](#)

# Dashの上位1万アドレスのジニ係数

[Google Cloudのブログ](#)に掲載された[BigQuery](#)を使った暗号通貨のビッグデータ解析事例として上位1万アドレスのジニ係数が調査された

Dashはマスターノードの稼働のために大口所有者のアドレスが複数の1,000DASHのアドレスに分散されるが、それを考慮しても非常によく分散されていると書かれている

Gini coefficient, top 10K balances



[引用元](#)

インスタミンに参加したマイナーが取引所等でコインを大量に売ったことで流動性が高まった可能性と、マイニング参加していない多くの人がコインを買ったことでコインの分配が進んだ可能性がある

 **CrowdNode**  
Login or signup

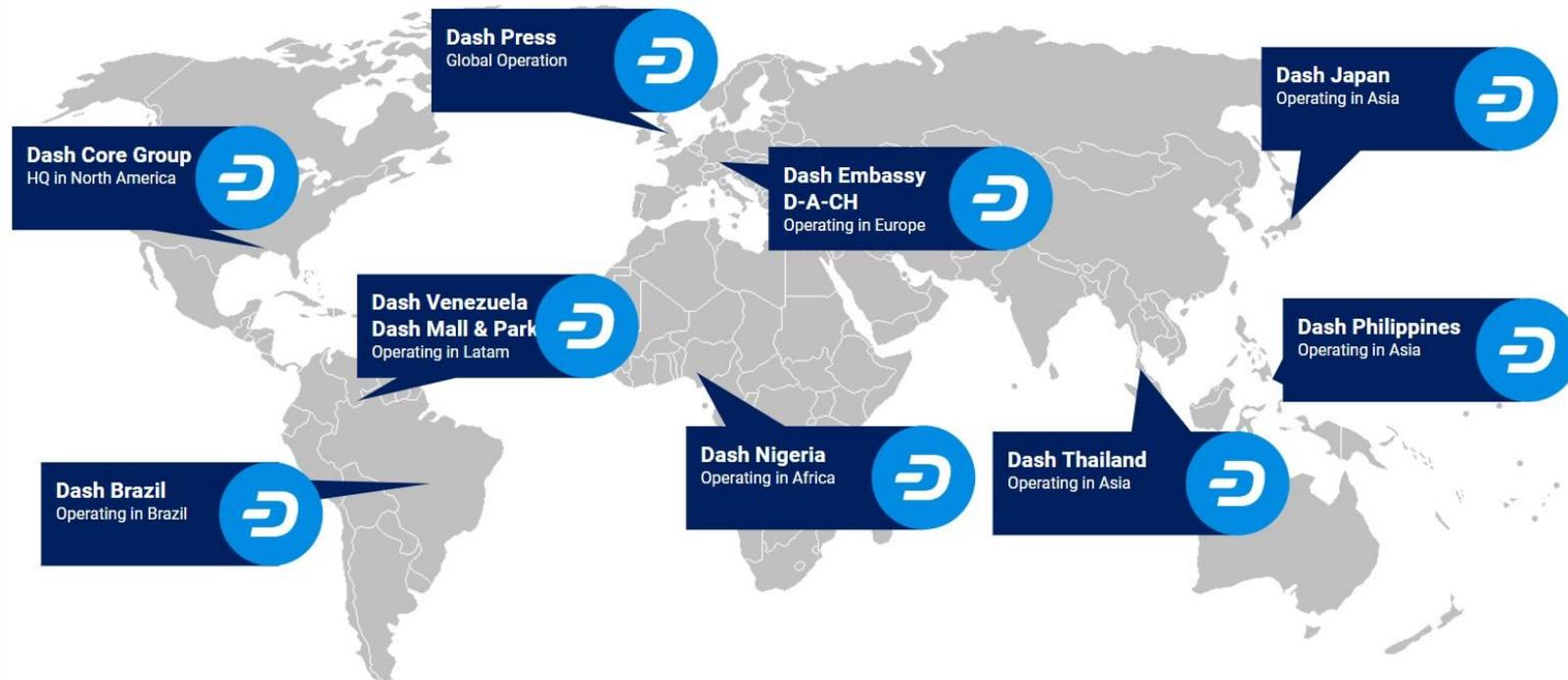
[Transparency Reports](#) [Masternode hosting](#) [Security](#)

## Become part of a Dash Masternode

CrowdNode unites smaller investors to achieve rewards from Masternodes.

[LEARN MORE](#)

# 世界中で予算を獲得したエンティティが活動中



Dash Embassy D-A-CHから資料提供

# 予算提案の種類

開発

パートナーシップ

ビジネス開発

教育・普及

広報

広告・宣伝

## Listing Dash in Japan

提案者: Samurai33

日本の暗号資産交換業者でDashを取り扱ってもらうために、Dashに対する誤解を解くためのメモランダム(≒覚書)を作成するという提案

弁護士と公認会計士が作成した客観的な事実に基づくメモランダムを登録されているすべての交換業者と共有し、JVCEA、財務局・金融庁に提出するというもの

Dashのプライバシーや匿名性については、Dashコアグループが[声明](#)を出しているが、より客観的な資料を提供することが目的

合計約315万円相当の予算  
を2020年3月・4月の2か月に  
分けて要求



賛成票896票、反対票45票で可決

# Dashに対する誤解

ブロックチェーンが  
非公開



ブロックチェーンエクスプローラー等で、ビットコインと同じレベルで取引記録が公開されていることを確認できる

追跡ができない



ビットコインでもDashのPrivateSendと同様のトランザクションを作成することは可能。送信元・送信先・送金額はすべて公開されており、Chainalysis等でBTCと同様にブロックチェーン解析が可能。

監査が不可能



ホット&コールドウォレットのすべてのアドレスを公開しているカストディアン業者が存在。アドレス残高はBTCと同様に公開。例えば、その業者がそれらのアドレスに会計監査人が指定するメッセージを入れて秘密鍵で署名をすればBTCと同様に残高証明が可能。

ダークネットで悪用



ランド研究所の調査等でダークネット市場の主流通貨がビットコインであることが報告されている。ビットコインにも匿名性があり、本人確認が不要な市場での流動性の高さから最も使用されていることが考えられる。

LLMQの6割が最初に発見・署名したチェーンを正とする「第一発見(first-seen)ルール」を導入し、極めて高い51%攻撃耐性を獲得

攻撃者が制御しているマスターノードを全体の30%未満と想定する場合、今後1澗(かん)(=1兆×1兆×1兆)年の間に、攻撃者が悪意のあるChainLocksを生成する確率は100兆分の1未満

LLMQ\_400\_60

ランダムに選抜された400のマスターノード



12時間毎に再構成

## 最近実装された機能 2 LLMQ-Based InstantSend

LLMQのうち60%がメモリプール内に追加されたトランザクションを適格であると判断

トランザクションがロック

マイナーによる承認の制約を受けずにメモリプール内にあるDashを不可逆的かつ連鎖的に送信することが可能に



イメージ動画

LLMQ\_50\_60

ランダムに選抜された50のマスターノード



約1時間毎に再構成

ブロックのダウンロード・  
検証・伝達

PrivateSendミキシング  
の参加者間の調整

予算提案・意思決定提  
案への投票

LLMQを形成し、全ての  
適格なトランザクション  
を即時にロック  
(InstantSend)

LLMQを形成し、ブロッ  
クを確定(ChainLocks)

Dashプラットフォームを  
構築・稼働【予定】

仮に、ビットコインがCPUでマイニングできた時代に、サトシ・ナカモトがマスターノード制の導入を提案し、コミュニティの賛同を得て、それが実現していたら、あなたはそのビットコインを支持しますか？

[10年前のサトシ・ナカモトの投稿](#)

- 傍観者から「従業員」に
- 活躍の場はいくらでもある
- Dashの予算は誰でも利用できるもので、インターネット上にある公共の財産だと考えることもできる

- Dash Core Group, Inc. (2020年)「Dash Documentation」,  
<<https://docs.dash.org/en/stable/index.html>>2020年7月29日アクセス.
- ビットバンク株式会社ほか著(2016年)『ブロックチェーンの衝撃』日経BP社.

ありがとうございました

とみ三

[www.DashJapan.com](http://www.DashJapan.com)

Twitter: [@samurai3311](https://twitter.com/samurai3311)

ご意見、ご質問などがありましたら  
お気軽にどうぞ

Dashプロジェクトに関心のある方は、  
ぜひDashJapan.comのDiscordサーバーに  
お越しください！

質問などにも対応していて、翻訳チームも活動  
中です。



<https://www.dashjapan.com/discord/>

**Dash**  
Japan.com