

# Dashとは何か？

PoWとPoSeのハイブリッドを採用し、予算編成システムを持つ  
暗号通貨の全体像

ハンドルネーム:とみ三

Dashの日本語情報サイト[DashJapan.com](https://dashjapan.com)を運営。

[Twitter](#)での情報発信

本業があり、フルタイムでの活動はしていません。

Dashのホワイトペーパーの一部を翻訳したりしていますが、英語力は低いです。

エンジニアではありません。

【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1800億円(2018年9月27日現在。[CoinMarketCap](#)のランキングで11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のコードベースフォークとしてスタート。リリース翌月にDarkcoinに改称(Lite=Light⇔Dark?)。リリース翌年3月にBitcoinのコードベースフォークとなり、Dashに改称。

【受け入れ事業者数】 [DiscoverDash](#)によると全世界で3,100以上(うち1,590がベネズエラ。日本は1。)



## 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	2.5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	1年ごとに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
プライバシー(送金履歴難読化)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
開発中のソリューション	Lightning Network	Evolution

「匿名通貨」、「匿名性仮想通貨」？

悪いことをするための暗号通貨？

ビットコインコピー？

## 決済目的特化型暗号資産

※ブロックチェーンに所有者情報は記録されないので全て匿名通貨と考えるべき

### ブロックチェーン公開型コイン

任意で中央集権型のトランザクション難読化ができるコイン  
(BTC・BCH・LTC・MONAなど)  
※秘匿トランザクションなどのプライバシー向上技術の導入を検討しているコインもある。

任意で分散型のトランザクション難読化ができるコイン(DASHなど)  
※ユーザーにとって比較的安全な難読化技術

### ブロックチェーン一部非公開型コイン

任意でトランザクション秘匿化ができるコイン(ZECなど)  
※ZECはデフォルトでの秘匿化に移行予定?

デフォルトでトランザクションが秘匿化されるコイン(XMRなど)

## ビットコインのプライバシーとファンジビリティは低い

アドレスの所有者は基本的にわからない

しかし、取引の当事者は取引相手のアドレスがわかるので、そこから取引相手の保有量、使用状況などが推測できる

ネット上に晒されるリスクもある

**ファンジビリティ(代替性、等価性)**

通貨に必要不可欠な特性

犯罪に使われたコインは価値が低い

マイニングされたばかりのコインは価値が高い



- 買い物用ウォレットを貯蓄用ウォレットと完全に分離する
- 取引所への入出金 (取引所のホットウォレットで他のユーザーのコインとごちゃ混ぜになる)
- ミキシングサービス

**現状では取引所の果たしている役割が大きい。しかし中央集権型で信用が必要になる(ビットコインを預ける必要がある)**

Dashはマスターノードがミキシングの場となる  
(ミキサーとなること)で信用不要(トラストレス)  
で分散型のミキシングを提供している

Dashのマスターノードはビットコインのフルノードにあたる

フルノードの役割—**ダウンロード、検証、伝播**

マスターノードはその役割に加えて、

**守秘送金(プライベートSEND)のミキサー**

**即時送金(インスタントSEND)の承認**

の役割を担う

## マスターノード稼働に必要な要件と権利

- 1つのマスターノードを稼働するには、1,000DASHの所有を証明する必要がある。
- マスターノード所有者は1,000DASHをいつでも動かすことができる(マスターノードを解消することができる)。
- 1,000DASHをどこかに預ける必要はなく、没収されることもない。また、オンラインウォレットに保管しておく必要はなく、ハードウェアウォレットでの保管が推奨されている。
- マスターノードには予算提案(バジェットプロポーザル)と重要事項の決定への議決権が与えられる。1マスターノードにつき1票。
- マスターノードにはブロック報酬の一部が与えられる。

## 現在のマスターノード情報

マスターノード数	4861
マスターノードへの報酬支払間隔	平均8.86日ごと
マスターノードへのブロック報酬	1.67DASH(約35,513円)
1 DASHの価格	21,265円
1,000 DASHの価格	21,265,000円
1日あたりの報酬	約4,008円
1年間の価格平均が21,265円だった場合の1年あたりの報酬	約1,462,920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6.87%

[Dash Masternode Information](#) をもとに作成(2018年9月26日15時現在)

## プライベートSEND(守秘送金)の仕組み

ビットコインの取引履歴難読化技術としてG・マクスウェルによって開発されたCoinJoinを発展させたもの

Dash Core ウォレットに入っているDashを4つの金種(10・1・0.1・0.01 DASH)に分割する(ミキシングは金種ごとに行われる)



マスターノードにミキシングを要求。他に2人のユーザーが集まるとミキシング開始。ミックスされたDashがウォレットの新しいアドレスに返ってくる【1ラウンド】(4ラウンド以上が推奨。ラウンドを重ねるごとに指数関数的に追跡が難しくなる)※ミキシングはバックグラウンドで実行される



プライベートSENDを選択して取引相手のアドレスに送信をする

# Dash Core ウォレットでのプライベートセンドの操作(1)

The screenshot shows the Dash Core wallet interface. At the top, there is a menu bar with options: ファイル(F) 設定(S) Tools ヘルプ(H). Below the menu bar, there are navigation buttons: 概要(O), 送る(S), 受信(R), 取引(T), and Mastermodes. The main content area displays the Dash logo and a summary of balances:

- 利用可能: 0.00000000 DASH
- 検証待ち: 0.00000000 DASH
- 合計: 0.00000000 DASH

Below the balances, there is a section for PrivateSend:

- PrivateSend
- 状態: Disabled, keys left: 999
- Completion: 0%
- PrivateSend Balance: 0.00000000 DASH
- Amount and Rounds: 1 000 DASH / 4 Rounds
- Submitted Denom: n/a

At the bottom, there is a large blue button labeled "Start Mixing" which is circled in red. Below it are three smaller buttons: "Try Mix", "Reset", and "Info". On the right side of the interface, there is a vertical column of seven blue arrows pointing downwards, with the text "最近のトランザクション" (Recent Transactions) above them.

# Dash Core ウォレットでのプライベートセンドの操作(2)

The screenshot shows the Dash Core wallet interface for creating a transaction. The window title is "Dash Core - ウォレット". The menu bar includes "ファイル(F)", "設定(S)", "Tools", and "ヘルプ(H)". The main navigation bar has "概要(O)", "送る(S)", "受信(R)", "取引(T)", and "Masternodes".

The "コインコントロール機能" section includes an "入力..." button and an "自動選択" option. Below this is a "カスタムおつりアドレス" field with a placeholder "Enter a Dash address (e.g. Xx7qvyEa7SXGcDobMR49BivaQEYjt6YYBY)".

The "送る" section includes:

- "送り先 (T):" field with the same placeholder as above.
- "ラベル (L):" field with the text "アドレス帳に追加するには、このアドレスのラベルを入力します".
- "金額 (A):" field with a "DASH" dropdown menu and a "Subtract fee from amount" checkbox.

The "トランザクション手数料:" section includes a "Hide" button and a "推奨:" radio button selected. The recommended fee is "0.00001000 DASH/kB" with a note "6 ブロック以内に検証が開始されると予想されます." Below this is a "Confirmation time target:" slider ranging from "普通" to "高速", currently set at "15 m / 6 block(s)".


The "カスタム:" radio button is unselected. It includes:

- "1キロバイトあたり手数料" selected, with a value of "0.00000000" and a "DASH" dropdown.
- "最小手数料" unselected.
- A checkbox "Pay only the required fee of 0.00001000 DASH/kB (ツールチップをお読みください)".

At the bottom, there are buttons for "送る (e)", "すべてクリア (A)", and "受取人を追加 (R)". The "PrivateSend" checkbox is checked and circled in red. The "InstantSend" checkbox is unselected. The balance is shown as "残高: 0.00000000 DASH".



# プライベートセンドのトランザクションの一例

4738a1887f7dab6b3d8e7181a4b5c2b05d13d306f021af1dff6893d76682e56b  mined Aug 4, 2018 5:07:06 PM

Xh9hi2JMzng6eNoeFN3TsH5Wu2fCfEvUr	0.0100001 DASH	>	Xkga7uNTp2SVhvnHpkFtuIaeWvudCc24	0.05999 DASH (S)
XkeopFZxHikM1Fhfacn1gs3xrQxXC3xZV4	0.0100001 DASH			
XpQooovjhGs7AScKrEAib4rTNSYLTDniqi	0.0100001 DASH			
XsCXNXmYLxP6yZzErhGANW32xkbjoF8rwJ	0.0100001 DASH			
XyhuypaWfHiEkCfnHZomhWazpstVKfCtIm	0.0100001 DASH			
XvRmtibrTbQD6ZuMUAeSWmvNi8BN1B14Go	0.0100001 DASH			

[^ Show less](#)

FEE: 0.0000106 DASH

29520 CONFIRMATIONS

0.05999 DASH

## インスタントSEND(即時送金)の仕組み

ビットコインは承認に時間がかかるという問題がある。ゼロ承認で即時に決済完了とするのはリスクがある。

Dashはマイナー(採掘者)の承認ではなく、マスターノードにインスタントSENDの承認を任せている。

---

インスタントSENDを選択して取引相手にDashを送信



ランダムに選抜された10のマスターノードのうち6つが承認して決済完了



マスターノードがトランザクションをロックし、ブロードキャスト



該当トランザクションは必ずブロックに取り込まれ、競合するトランザクションは拒否される

マスターノードがプライベートセンドのミキサーとなり、インスタントセンドの承認をすることでブロック報酬を得る仕組みを**Proof of Service (PoSe)**という。決済に使われる際の問題をマスターノードを使って解決したと言える。

その他にも**ガバナンス・意思決定機能**。

大口所有者が売買を繰り返さなくても利益を得ることができるので、**価格変動性を低くする効果**も期待されている。

Dashは現在2MBのブロックサイズを拡張していく予定。**分散型の状態でビッグブロックに対応できる仕組み**でもある。

現在マスターノードのランニングコストはそれほどかからないが、将来ブロックサイズが拡張すると専用のハードウェアを購入する必要がある。

ブロック報酬の10%はコミュニティ内で自由に使える自己資金となる

使い途はマスターノードによる投票で決める。予算提案は5DASHを支払うことで誰でもできる。

財団のようなものがある蓄えるのではない(内部留保やキャリーオーバーはない。)

予算は毎月1回生成されるスーパーブロックから予算獲得者のアドレスに直接支払われる

2018年10月2日のスーパーブロック...使用可能な予算は最大6,177 DASH  
(日本円で約1億2763万円)

### 現在の投票状況

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(現在486票)に達することで提案は可決される

- ・Dashコアグループ(開発請負業者。スタッフ数39名。米国アリゾナ州に[オフィス](#))  
の[報酬](#)
- ・[アリゾナ州立大学との提携](#)
- ・ベネズエラのコミュニティ(Dashカンファレンス、[Dash Help](#)、[Dash Text](#)など)
- ・[Alt36社](#)
- ・[Dash大使館](#)
- ・Dash Force [独自メディア](#)

等々、多岐にわたる

一例...[2MBブロックへの拡張](#)

24時間以内に可決された

ユーザーネームを登録、ログインして利用

「あなたのおばあちゃんでも理解できる」を合言葉に開発されているUI、UXを重視した公式ウォレット

開発はクローズドソース。リリース時にオープンソースになる予定。  
特許取得予定

世界初の分散型API(DAPI)によりサードパーティのDash統合が容易になる

自動引き落とし機能、トラストレスマスターノードシェアの構想も

ネットバンキング、メッセージングアプリ、マーケットプレイスを融合したようなものになるのか？年内にリリース予定

1. Dashはビットコインのプライバシーを向上させることを目指して始まった
2. Dashはマスターノードの仕組みを導入したことで、Proof of WorkとProof of Serviceのハイブリッドを採用する暗号通貨となり、高機能となった
3. Dashは、ブロック報酬の10%を自己資金とし、マスターノードの投票による予算編成システムを持ったことで世界最大のDAO(自律分散型組織)となった



日本語翻訳チームが活動中

Dash Forum

Discord Dash Nation

- アンドレアス・M・アントノプロス著(2016年)『[ビットコインとブロックチェーン](#)』NTT出版.
- A・ナラヤナンほか著(2016年)『[仮想通貨の教科書](#)』日経BP社.
- Dash Core Group, Inc. (2018年)「Dash Documentation」,  
<<https://docs.dash.org/en/latest/index.html>>2018年9月25日アクセス.

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

## 著作権について



<https://creativecommons.org/licenses/by/4.0/>

この資料は、クレジットを表示したうえで、ご自由に複製・再配布していただいて結構です。商用利用も可能です。資料を改変した場合はその旨を明記して下さい。

ご利用にあたっては、下記のクレジットを必ず表示してください。

© 2018 DashJapan.com クリエイティブ・コモンズ・ライセンス ([表示4.0 国際](https://creativecommons.org/licenses/by/4.0/))

**Dash**  
Japan.com