



BitZeny-Project

2018 年 月 日

著 : All BitZeny developers

このプロジェクトを
すべての作り手たちに捧げる

[概要](#)

[目的](#)

[発行仕様](#)

[開発母体とその構造](#)

[開かれた開発環境](#)

[現在の開発者](#)

[CPUへの最適化](#)

[学術的資料として](#)

[555](#)

[BitZeny Core Program](#)

[開発ベース](#)

[yescrypt](#)

[DarkGravityWave3](#)

[ブロック報酬と半減期](#)

[segwit](#)

[開発ロードマップ](#)

[道程](#)

[予定](#)

概要

BitZenyという暗号通貨がどのような目的で開発され、既存社会に対してどのような方向を目指しているのかについて述べる。

目的

BitZenyが目指すべき、担っていくべき社会的な立場について。

1. すべてにおいて民主的であること
2. 互助社会の醸成
3. あらゆる創造的活動への正当な評価体制の構築
4. より公平でより民主的な社会規範の創造
5. 後進の効果的な育成

以上を目指すものとします。

発行仕様

稼働開始日	2014/11/8
シンボル	ZNY
アルゴリズム	Yescrypt-r8
最大発行枚数	250,000,000
プレメイン	なし
ブロック生成時間	90秒
難易度調整	DarkGravityWave3
ブロック発見報酬	250枚
半減期	500,000ブロックごと
ポート	9253

RPCポート	9252
--------	------

開発母体とその構造

I. 開かれた開発環境

BitZenyの開発に参加する為の特別な条件はありません。

githubのアカウントがあれば、今後の開発方針を含めたすべての開発にかかわることができます。それはつまり、発行主体のアルゴリズムにかかわる論議を含めたすべての開発をさします。

私たち一人ひとりの小さな意見も、丁寧に議論され解決のための方向性を模索できます。

そのための管理手段もまた、共有されます。

しかし、圧倒的な権限を有したユーザーは限られており、与えられるには条件が設けられます。私たちは常にそうした新しい開発者の誕生を願っています。

II. 現在の開発者

私たちは特に決まった開発主体というものをもたないことを主体とします。

だれもが開発者として参加できるので、BitZenyをよりよくしたいと考える人も、害をなそうと考えている人も参加できます。しかし、そうした悪意あるプログラムをプルリクしたとしても、他の開発参加ユーザーと精査し合うことでこれを排除することもまた、容易です。

その時には最善であったとしても、状況によって不適切な開発に結果として至った場合、これを改善するための協議は極めて迅速に行われ、最適化のプロセスを得られます。

III. CPUへの最適化

採掘の公平性はPoWアルゴリズムの根幹です。

これはASICやGPUなどの専用機の影響を可能な限り低くすることと直接的な因果関係にあるからです。

機材を用意することが難しいASICや入手金額がそもそも高価なGPUに比べて、CPUであれば媒体を問わずに用意することが容易です。そのため承認作業に参加することも簡単にできるようになるため、承認における不正を防ぐためのインフラが整いやすいと言えます。

しかしながら問題もあります。

BotNETと呼ばれるウイルスを用いた方法や、資本に物を言わせてマイニングに参加し大きなシェアを得る方法です。また、採掘プールの一極化についても問題視されていますが、CPUとの効率がよほど剥離しない限りは大きな問題にはつながらないと考えています。

IV. 学術的資料として

BitZenyが開かれた開発環境をもつ最大の理由として、ブロックチェーンを使った様々な実地動作研究対象としての側面があります。

これは先々において国内(もしくは国外)の技術者の醸成を育み、暗号化技術やブロックチェーン技術者の育成をより効果的なものにしていくためです。

私たちは新しい開発者の参加とその研究結果を常に公開し、多くの技術者と共有します。

V. 555

テスト

BitZeny Core Program

I. 開発ベース

BitZenyの開発は、Bitcoinの0.9.3をベースにorphanate氏の手により開始されました。

しかし、あまりにも古いバージョンのためソースからのビルドが簡単とはいいがたく、有志による開発が行われました。

2017年11月から最新版のBitcoinCoreをベースとしたものにアップデートする計画を進め、翌2018年2月にリリースしました。

真新しい特別な機能を備えているわけではありませんが、開かれた開発母体を持った特異な開発環境にあるコインとして、あらたな産声を上げた瞬間と言えます。

以降も真新しい機能を与えられるかどうかの方向性も、開発陣という名のユーザー自身に委ねられています。

II. yescrypt

PHDで公開された仕様書

<http://www.openwall.com/presentations/PHDays2014-Yescrypt/>

III. DarkGravityWave3

ソース

<https://gist.github.com/Geertlohan/b28da8105babf0553f21>

DarkGravityWave3は、X11 / Darkcoin / Dashの開発者であるEvan Duffieldによって作成された難易度調整アルゴリズムです。

1ブロックごとに前ブロックの承認速度に応じた難易度を設定し直す機能をもっています。難易度調整が頻繁に行われるため、ブロック承認時間にずれが発生しにくく、ブロック生成時間の大幅な遅延が起き難くなっています。

BitZenyの開発当初はKimoto Gravity Wellも候補にあがっていましたが、問題なく現在まで稼働しているため現在は変更される予定はありません。

IV. ブロック報酬と半減期

250zny/blockが最初の50万ブロックに適用され、半減期を迎えます。その後の採掘は以下のように変化します。

Blocks	Reward
500,001~	125
1,000,001~	62.5
1,500,001~	31.25
2,000,001~	15.625
2,500,001~	7.8125
3,000,001~	3.90625
3,500,001~	1.953125
4,000,001~	0.9765625
4,500,001~	0.48828125
5,000,001~	0.244140625

V. segwit

BitcoinやMonacoin、Litecoinで採用されたトランザクション処理技術の一つです。

具体的にはトランザクションデータを圧縮し、署名データを別管理させるためのプログラムです。BitZenyでは1237015ブロックで有効化されました。

開発ロードマップ

道程

2014.11.8	orphanate氏によりz1.1.xが始動
2017.11	z1.2.x公開(新チーム) z1.3.test 公開(Dev版)
2018.1.28	z2.0.0公開 シンボル及びロゴマークの公募を開始
2018.2.22	z2.0.1公開
2018.3.17	ロゴマーク策定
2018.9.26	z2.0.2公開

予定

未定

BitZenyPlus(z3.0.x)
