



ホワイトペーパー(白書)
ver. 1.41 日本語版

目次

序説	3
XDNA 機能及び技術仕様	4
仮想通貨における問題点の私達の解決方法	5
BitGun(ビットガン).....	10
T.N.T(ティーネヌティー).....	14
XDNA 基金.....	17
タイムラインとブロックの報酬分布	19
文献リスト	22
クレジット	23

近日、仮想空間での仮想通貨は何百万人もの人々の心をつかまえ、大旋風を巻き起こしています。ビットコインの栄光と成功は多くのファンを魅了し、その結果、毎日多くのデジタルコインとトークンが作られるようになりました。

幾らかは驚異的なものがある一方、残念ながら、仮想通貨の約 90%の品質は不十分なものです。他人を犠牲にして利益を求める人たちは、有名な仮想通貨のクローンを作成し、ソースコードやバイナリに隠されたウイルスを注入するなどの詐欺の手口で利益を上げたりしています。仮想通貨の空間は今までこのような危険な場所ではありませんでした。

やまを狙う理由目的でのアルトコインのお祭り騒ぎが横行するなかで、仮想通貨のエキスパート達はプロフェッショナルな目線でハイクオリティな仮想通貨のアイデアを考え出しました。

新しいデジタル経済の情報化社会に存在する人々が今までに見た事のない、そんなプロジェクトを創造するアイデアです。

成功したデジタル通貨の全ての良い面を組み合わせると同時に、その欠陥と欠点の全てを考慮に入れたプロジェクトです。

このプロジェクトは、マイナー、投資家、そして日常のデジタル空間を知らない一般の人々さえ満足させるものです。

このプロジェクトはデジタル世界のみならず、現実社会にも明らかなメリットをもたらします。

このプロジェクトは Ethereum, Dash, Neo, Zcash, Monero,その他全てのユーザーの心をつかめます。

その過程で私たちはいくつかの原則に従いました：

- 私たちのプロジェクトは、現代の仮想通貨(暗号化通信)に関連するいくつかの特定の問題を解決しなければなりません。
 - 私達のプロジェクトは、マイナーと投資家の両者を満足させなくてはなりません。
 - 私達のプロジェクトは、現実的な利益を人類にもたらす必要がある。
- これらの原則を守る事で、単なるデジタル通貨以上の物を想像し、仮想世界と現実世界の間に持続可能なチェーンを構築することを可能にしました。

イベント、交友関係、家族関係のチェーンと最もハイテクなブロックチェーンが客観的な現実としっかり絡み合うでしょう。

そのような絆なしでの人生は考えられません。そこで、私たちは自信を持って、新しく、革新的なデジタル通貨をあなたに提供いたします。 - XDNA.

XDNA 機能

BitGun(ビットガン)

ブロック報酬が流動的に変化する革新的な機能

T.N.T.(ティエヌティ)

高度なマルチレベル マスターノード コンセプト -
トリプル ノード テクノロジー

XDNA 基金

非営利慈善仮想通貨ファンド

技術仕様

- 名称とティッカーシンボル: XDNA
- コンセンサス アルゴリズム: PoW/POS
- POW フェーズ期間: 1440000 blocks
- PoW ブロック報酬: 可変, 4-511 XDNA
- インスタマイン プロテクション: First 720 blocks
- ハッシュ アルゴリズム: Keccak
- XDNA 推定供給期間 POW: 138,000,000
- POS スタートブロック: 1440001
- POS フェーズ期間: 無制限
- POS ブロック報酬: 57 XDNA より 525600 ブロック毎に 1 XDA に到達するまで 4 コインずつ低下
- POS ブロック報酬分配: SeeSaw
- POS による 15 年間 XDNA 供給量推定: 228,000,000
- 事前採掘量: 971,712 XDNA (POW 総供給量の 0.7%)
- ブロックサイズ: 1 MB
- ブロックタイム 平均: 1 min (DGW/3)
- トランザクション承認数: 6
- 満期: 60 confirmations(コンファーム)

仮想通貨における問題点の私たちの解決方法

20 世紀と 21 世紀の境目、ビットコインは私達の生活に登場しました。この出来事は地球上の進歩的なありとあらゆる人を感動させ、それを見た殆どの人はビットコインを探求し、新しいタイプのデジタル通貨を開発、実装しようとしてきました。

しかしながら、(他のハイテク分野と同様に)仮想通貨の分野ではスケーラビリティ、セキュリティ、少額取引によるネットワークの混雑、他にもいくつかの問題があります。これらの問題は、本来、本質的な性質であり、既知の方法により効率良く解決できることではありません。

いくつかのマイナーな問題は、いくつかのプロジェクトにより既に解決されているものの、仮想通貨に関する根本的な問題に加えて、その他の重大な問題は不当にも過小評価されたままになっています。

以下の様な欠陥は仮想通貨をざっと調査しただけで思い当たる事です。

1. トランザクション確認の長期化。

私達の世界がダイナミックに発展していく事を考えると、待ち時間 30 分、もしくは 60 分というのは時間の無駄遣いとなってしまいます。

2. POW アルゴリズムをサポートする ASIC の登場。

機器のコストを考慮すると人口の殆どが Script, X11, Sha256 とその他の仮想通貨を利用することができない結果となってしまいます。更に ASIC の出現は、サトシナカモトが策定した一般的な原則に反して、システムの分散化に大きなダメージを与えてしまう結果となります。

3. “インスタマイン問題”。

正式なりソースのアナウンスを遅らせて、コイン開発者自身がネットワーク起動の初期に大量の仮想通貨コインを提供してしまう。

4. “事前採掘”。

開発者は最初のブロックでかなりの量の仮想通貨トークンを獲得してしまいます。残念な事に、仮想通貨の開発者は高確率で事前採掘を行い、個人の利益の為に、コイン取引開始の初日に沢山のトークンを売却する傾向にあります。これは以下の問題と密接に関係しています。

5. 新規の仮想通貨開発者は多くの場合、財源が不足しており、自らの創造物を慈善目的に適用する意欲を持たず、単に自分が豊かになる為の手段としか考えていません。

実際に、時価総額が最も成功したプロジェクトを考慮すると、事前採掘したコインをチャリティーに利用しようと思う人はごく僅かです。それと同時に、食料、清潔な水、医薬品及びその他の必需品を必要とする人々は世界中に沢山存在します。

6. 各ブロック報酬のかなりの部分が開発者に対して支払われます。

仮想通貨の開発者の一部は報酬の一部をトラブル解決の為に利用しますが、一部のプロジェクトではこの料金の額が大き過ぎたりしています。

7. マイナー報酬の大幅な減少。

トータルのネットハッシュに従い、採掘難易度も上昇し、ブロックチェーン機能をサポートするマイナーの"賃金"が低下します。 後者の問題はかなり明白な理由があります。 マイナーの収入は通貨価格に比例し、トータルネットハッシュに反比例します。

8. マスターノードコスト

あまりにも高いマスターノードコストは"一般マイナー"による実行ができなくなります。コストが低すぎる場合、投資家は買収に関心を示さなくなるでしょう。

XDNA 作成の為に:

- 上記の問題を部分的に解決し、既存の仮想通貨の問題を打ち消す。
- マイナーと投資家の調和を図る。
- 現実世界に利益をもたらす。
- ネットワーク容量の増加に伴い、マイナーの収入を削減するという確立されたパラダイムを変える。

問題の解決策 1

遅いトランザクションのスピードを克服する為に、60 秒のブロックタイムを XDNA のコードに設定します。DarkGravityWave3 アルゴリズムを利用して、各ブロックでの難易度を設定します。

取引の検証には 6 件のみの検証で済む為、XDNA の世界各地への取引は 6 分以上かかる事はありません。

XDNA はインスタントトランザクションメカニズムである InstantSend [1]を利用して、マスターノードを介して所定のトランザクションをインスタントブロードキャストし、受信者のウォレットバランスに直ぐに着金表示をさせる事を実現します。

問題の解決策 2

Proof-of-work の実証済アルゴリズム Keccak がネットワーク機能の PoW フェーズ中にネットワークでコンセンサスを達成する為に利用されます。このアルゴリズムは様々なメーカーの GPU で快適に利用できる程、十分に優れている事が証明されています。更にこのアルゴリズムは ASIC で対応できない為、世界中のマイナーが GPU を利用して、XDNA のネットワークを安定して維持することができ、巨大な産業用採掘施設の氾濫のリスクがありません。

でもどうして Keccak?

まずこのアルゴリズムは ASIC で対応する事ができません。

第二に、マイニングプロセスに"赤"と"緑"のカードを効果的に使用できます。

第三に、Keccak はデュアルマイニング先として利用する事ができます。これにより、マイナー設備の多様化を図る事ができます。

そして最後に、2012 年にハッシュアルゴリズム Keccak は米国国立標準技術研究所(NIST)によって推進された暗号ハッシュリズムコンペの賞を獲得しました。

私たちはいくつかのよく知られた基本シーケンスでの流行りのハッシュアルゴリズムは利用しません。Keccak を選び、このアルゴリズムを作成した暗号分野の科学者に敬意を表します。科学者や研究の結果が無ければ暗号や電子通貨は存在せず、XDNA も存在し得なかったでしょう。

私達は Keccak の著作者に深く感謝の意を表します: *Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche.*

問題の解決策 3

instamine を防止する為に最初の 720 ブロックに 1XDNA の報酬を設定する。

問題の解決策 4

一部の仮想通貨クリエイターは最初のブロックの最大コイン供給量の 50%まで事前採掘をします。

XDNA チームは良識的な考えを持っています。私達の事前採掘は、POW、又は総推定供給量 971,712 XDNA のうちの僅か 0.7%のみです。

他の章で XDNA 事前採掘の配布についてもっと知る事ができるでしょう。

問題の解決策 5

XDNA チームは世界中の膨大な数の人々から必要とされていると心から信じています。事前採掘された殆どの部分、すなわち 350.000XDNA は XDNA 財団の慈善基金を創設する為に使用されます。これにより、世界中の困っている様々な組織や人々を助ける資金を調達し、配布する事ができます。

国際社会と共に、私達は単なる仮想通貨以上のものを作り上げる事ができます。

問題の解決策 6

XDNS 開発チームへの報酬として、各ブロック報酬うちの 1%が報酬として使用されます。これはプールで利用されているコミッションの手数料に匹敵します。

私達は酷い事前採掘は行いません。私達は ICO をしません。私達に隠す事は何もありません。

1%.

それで全てです。

問題の解決策 7

最後に、XDNA 創立の初期の理由について。マイナーの報酬の削減の問題を解決する為に、トータルネットハッシュにより報酬量に変化するユニークな機能を開発しました。"BitGun" XDNA の開発者の一人がそう名付けました。

BitGun の原則は、マイナーへの従来の報酬分配方法とは異なり、XDNA ネットワーク機能を維持し、(一定の限度内で)比較的安定した報酬を受け取る事を可

能にする為に段階的にブロック報酬を増加させる機能です。詳細については、BitGun の章を参照してください。

問題の解決策 8

マイナーと投資家の両方が XDN マスターノードに魅力を感じてもらうように、私達は3タイプのマスターノードが相互に同時に機能する事を可能にするシステムを開発しました。各タイプを担保する為のコインの量はそれぞれ異なり、それぞれ異なる量の報酬を得ることになります。私達はこのシステムを T.N.T.(TripleNodeTechnology)と名付けました。

詳細については T.N.T.の章を参照してください。

BitGun

ネットワークのハッシュレートがマイナー報酬に反比例してしまう、長年に渡るパラダイムを変える為に私達は高度な BitGun 機能を開発しました。

通常、マイナーの報酬はネットワークハッシュレートに依存しますが、これはネットハッシュが大きいほど、マイナーへの報酬が少なくなる事を意味します。言い換えれば、ネットワーク内の GPU の数が 1000 倍に増えれば、与えられた時間枠内のマイナーの報酬は 1000 分の 1 になるということです。いくつかの仮想通貨は非線形依存を利用しますが、その原則は同じで、ネットワークハッシュレートが上がると各マイナーへの報酬が少なくなります。BitGun は別のアプローチを採用 - ネットワークハッシュレートが上がるとブロック報酬は徐々に増加し、平均的なマイナーへの報酬を比較的に安定させる事ができます。

仕組みをご説明しましょう。

各ブロックの報酬量は、以前の 24 ブロックで記録されたネットハッシュの総平均値に応じて、ブロック生成の瞬間に変化します。

各ブロックの報酬量は、フィボナッチ数列を反映した"level"に従って変化します。全部で 15 レベルまであります。

表 1 は合計ネットハッシュとブロック報酬の量により定義されているレベルを表しています。

ブロック報酬の量が自動的に変更されるには、XDNA ネットハッシュの合計が表内に示される しきい値を超える必要があります。

このアプローチを利用する理由は何でしょう？

BitGun では、従来のブロック報酬の計算方法と比較して、一定期間内にマイナーが受け取る報酬額を安定させる事ができます。ネットワークハッシュレートが十分に成長すると、僅かに平均報酬は減少しますが、従来の分配システムより遥かに大きな報酬を受け取る事ができるでしょう。

表 1

Level(レベル)	Network hashrate (Th/s)	ブロック 報酬
1	1	4
2	2	5
3	3	7
4	5	9
5	8	11
6	13	15
7	21	20
8	34	27
9	55	39
10	89	57
11	144	85
12	233	131
13	377	204
14	610	321
15	987	511

表 2 は 1 枚の Nvidia GTX 1080Ti GPU を使って、古典的な計算方法と BitGun を 24 時間利用した場合の平均報酬を比較したものです。

表 2

	概算総額/1080ti	XDNA/1080ti/日	XDNA/1080ti/日 BitGun 利用
Levels 1-5	1,000	4.032	4.032
	3,000	1.344	2.352
	5,000	0.8064	1.8144
Levels 6-10	10,000	0.4032	1.512
	30,000	0.1344	0.9072
	50,000	0.08064	0.78624
Levels 11-15	150,000	0.02688	0.5712
	300,000	0.01344	0.68544
	450,000	0.000896	0.45696

上記の表に示されるように、ネットワークハッシュ値が低い場合、報酬はほぼ同じですが、ネットワークが増大するに連れて、BitGun の利点が明らかになります。

図 1 は 1 枚の Nvidia GeForce GTX 1080ti GPU による 1 日の報酬をネットワークのハッシュレート（GPU の数として記載）に応じて比較したものです。

レベル 1 から 8 までを数学的にモデリング化しました。このシミュレーションでは、以下の条件を使用しました。：マイナーが各ブロックから受け取る報酬量; Keccak アルゴリズムのハッシュレートは 1 枚の GPU あたり 1.35gh/s。

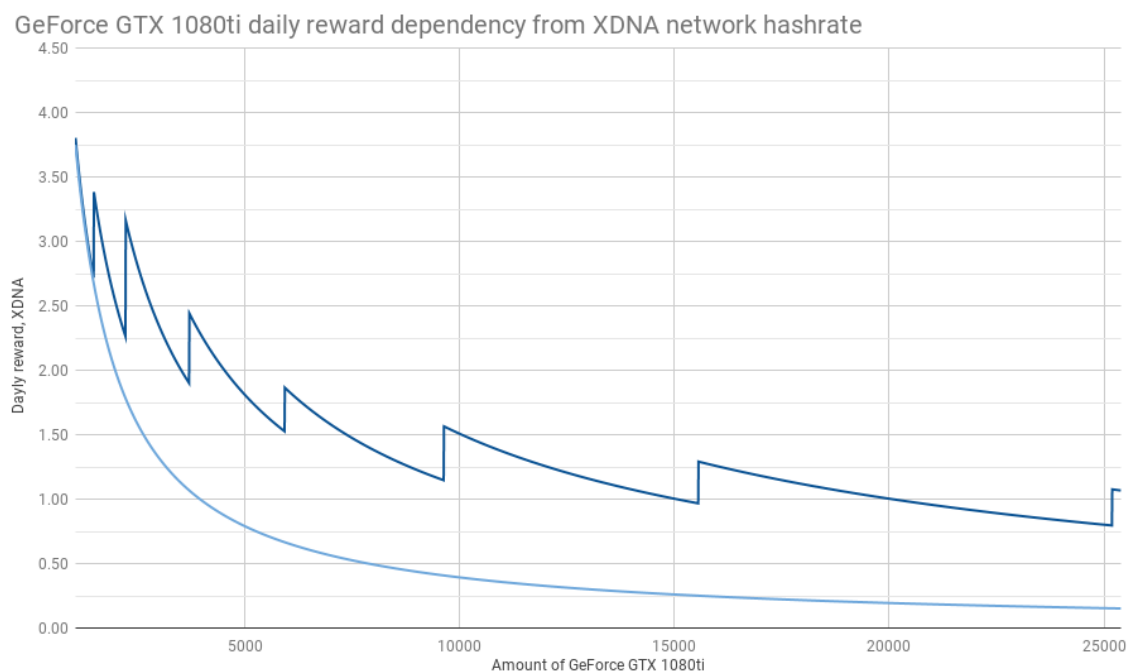


図 1

ネットワークハッシュレートが大幅に増大しても各 GPU は 1 BitGun レベル内で比較的安定した報酬を受け取り続けています。この報酬額は古典的な計算方法と比べて遥かに大きくなります。

これらのシミュレーション結果はレベル 2~14 のものですが、任意の時間間隔で正常に調整する事ができます。

このアプローチの新しさは、ネットハッシュとマイナーの収入の擬似的な関係のパラダイムを変えてしまう事です。

BitGun にはもう一つの利点があります。もし Keccak の ASIC が開発されたとしても、XDNA は GPU マイナーを保護する為にコンセンサスやアルゴリズムを

変更する必要がなく、ハードフォークを行ったりする必要ありません。少しの BitGun パラメータの調整で十分なはずです。

ネットワークハッシュレートが突然 1000 倍になったとしても、世界中のマイナーはまともな採掘報酬を受けられる事でしょう。

T.N.T.

仮想通貨をリードする世界で最も先進的な側面に沿って、ネットワークの安定性を確保する為にマスターノードを利用する事を提案します。

私たちは、異なるプロジェクトでマスターノードを利用した経験から、マイナーと投資家の希望と可能性を調和させる事をXDNAの当初から取り組んでいます。全ての人がマスターノードをセットアップする事ができるようになる為に、私たちは3つのタイプのマスターノードを開発しました。それぞれのタイプは異なる量のXDNAを必要とし、様々な収入をもたらします。このシステムをT.N.T. - TripleNodeTechnology と名付けました。

1. Light Node - 必要量 1,000 XDNA.
2. Medium Node - 必要量 3,000 XDNA.
3. Full Node - 必要量 5,000 XDNA.

POW マスターノード稼働中は、ネットワークの安定性を維持し、追加の機能を実行させる為の報酬として次の様な報酬(タイプにより異なる)を受け取ります。

- Light Node - 全ブロック報酬の 3%
- Medium Node - 全ブロック報酬の 9%
- Full Node - 全ブロック報酬の 15%

POS 稼働中のマスターノードの報酬割合は存続しますが、金額は SeeSaw algorithm [2]で決定されます。

(マスターノードの)主な業務はネットワークを安定させる事です、優れた投資手段とも言えます。

異なるタイプのマスターノードの収益性と報酬を決定する為に、一連の計算が行われています。

BitGun のレベルはマスターノードの収益性にも直接影響している事にも注視してください。

ネットハッシュが増加するとマスターノードの収益も増加します。

図 2 は様々な BitGun レベルでの異なるマスターノードタイプの収益の計算結果をネットワーク内のマスターノード数に応じて示しています。

Masternodes payback (any type), days

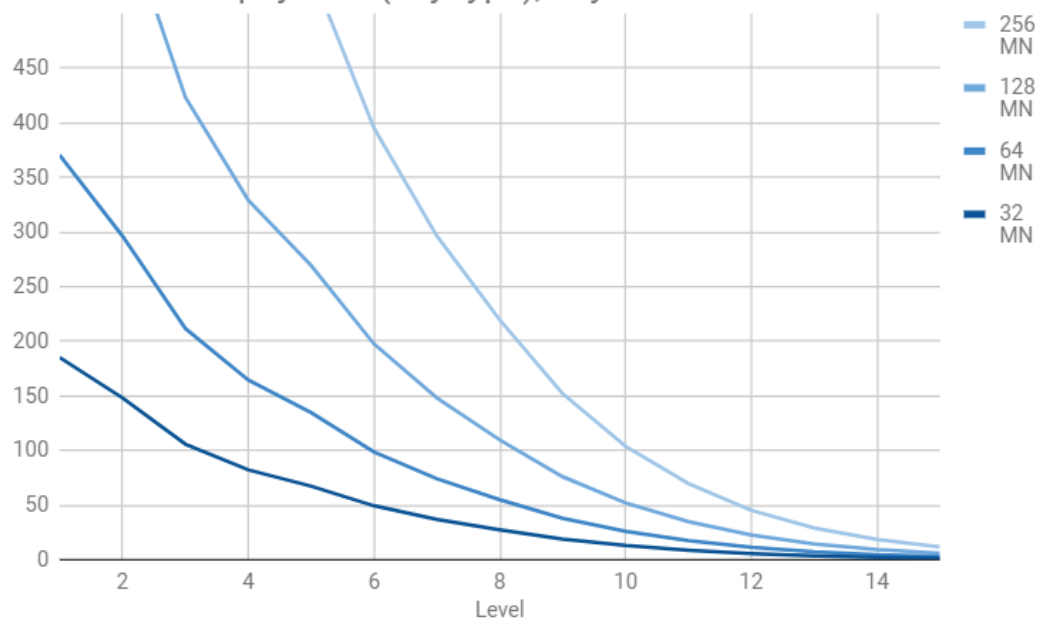


Figure 2

私たちは各々のタイプとネットワークの BitGun レベル機能に基づいて 50 のマスターノードを設定し、日ごとのマスターノードの支払いを計算しました。(図 3) また、100 のマスターノードがネットワーク上に存在するときの各々のタイプとネットワークの BitGun レベル機能について年間 ROI(図 4)の計算を行いました。

Masternodes payments per day, XDNA (for 50 MN of each type)

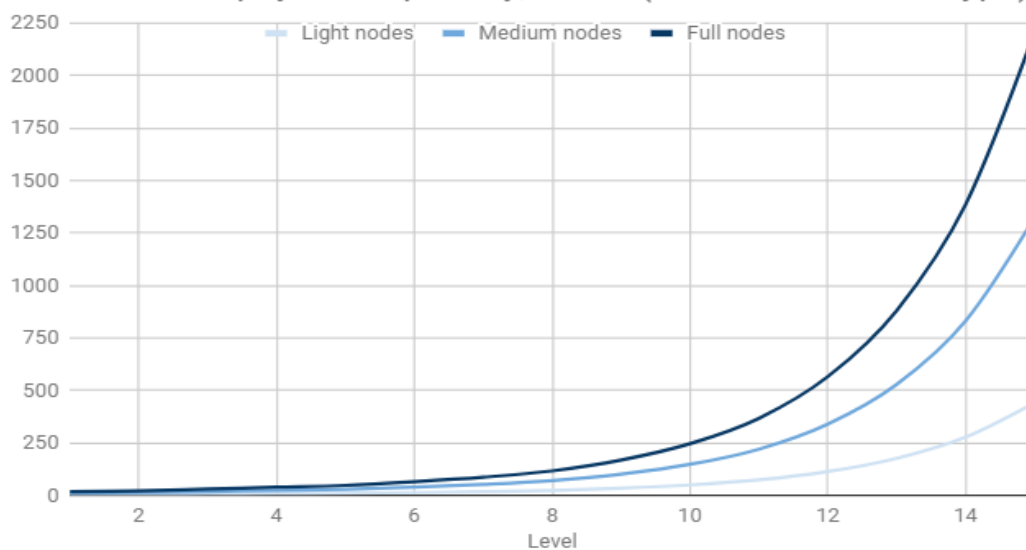


Figure 3

Masternodes ROI, % (for 100 MN of any type)

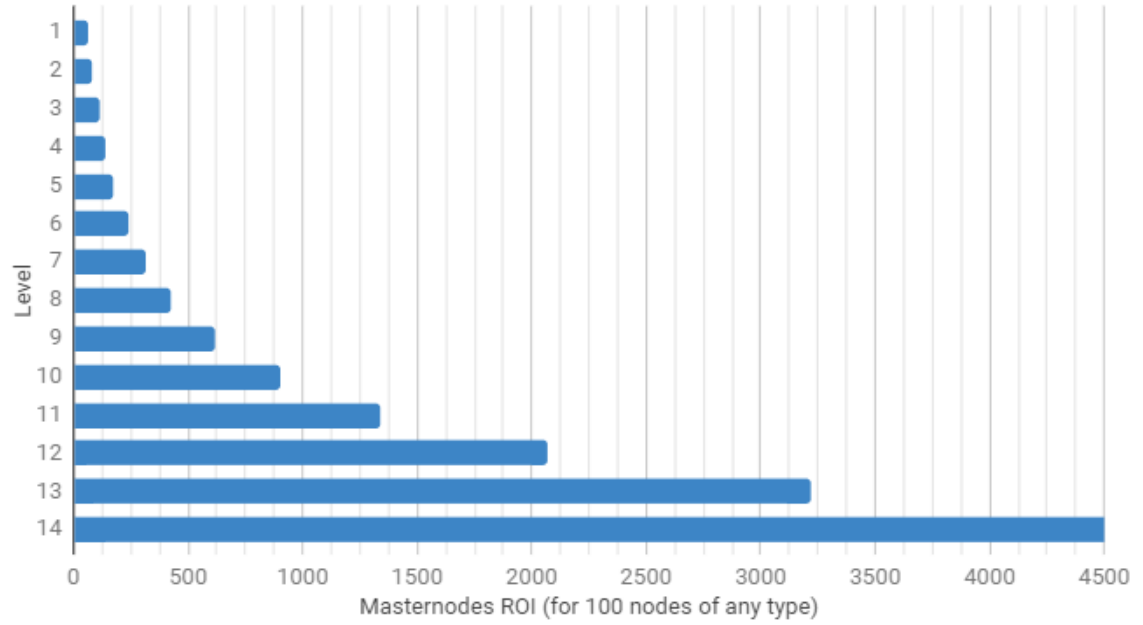


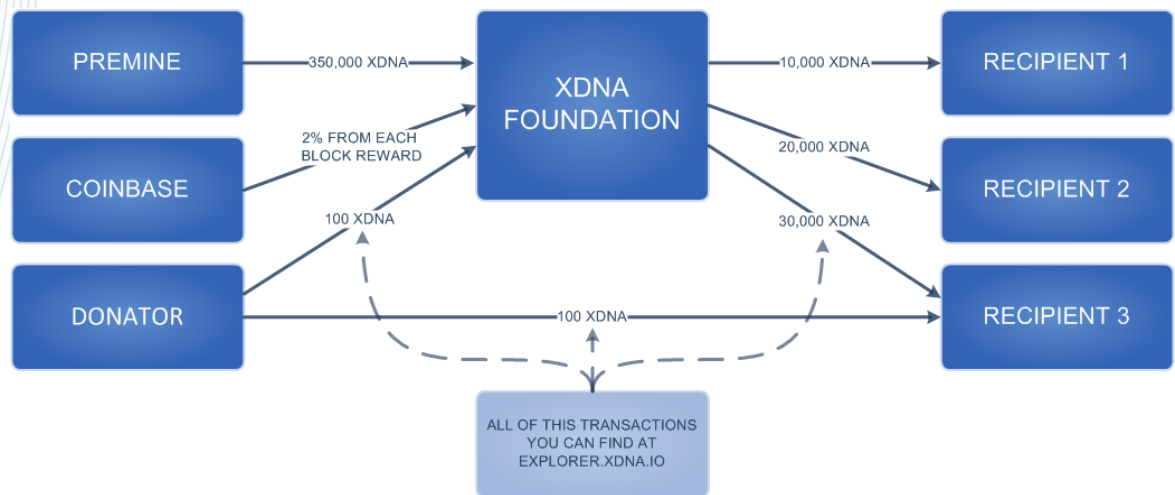
Figure 4

XDNA 基金

私達はこの世界について考えました。必要としている人々に無償で支援を行う慈善団体が世界中に多く存在すると私達は認識しています。私達も人々を助け、明るく良いものの一部になりたいと思っています。

私達は XDNA 基金を創設しました。(資金が不十分だったり資金不足に悩む団体への資金提供を主な目的とする基金。)

基金を創設する為に 350,000 XDNA が割り当てられています。このファンドの資金は基金に割り当てられた特別なアドレスに入金されます。基金のXDNAの資金の情報は一般公開されるように管理されています。: XDNA の公式サイトにあるブロックエクスプローラを参照するだけで十分わかります。



仕組みをご説明いたします。

貴方が、資金の乏しいコミュニティ、ソーシャルプロジェクトコーディネーター、ユーススポーツマネージャー、またはXDNA基金の助けを必要とする慈善団体のメンバーである場合、以下の事を行う必要があります。:

ウェブサイト内の該当するセクションのフォームに、貴方の組織とそれに関連する問題、困難の説明を簡単に記入します。

写真、書類等、一般的なものも含めて、できるだけ多くの情報を添付してください。

要請内容がが事実と判断され、私達の目的に沿っていると思われる場合は、該当するセクションに“under consideration”（検討中）と表示されます。事実である事を確認した後、XDNA 基金の管理者が最終決定を下し、もし合格であれば、予め用意されたペーパーウォレットをお送りします(または、直接お渡しし

ます)。資金を利用するには、XDNA PC WALLET をインストールし、リストアする必要があります。その後受け取った XDNA を BTC(ビットコイン)やその他、貴方の選択した方法でそれを現金化し、使用する事ができます。

もし、貴方が人々を支援したい、もしくは XDNA を利用する団体なのであれば、何もしなくて良いほど簡単です。いずれかの取引所で XDNA を購入し、基金の Wallet アドレスに送金します。本当に簡単です。別の仮想通貨で基金に送金したいですか？ 問題ありません。私達はそれを XDNA に変換して基金へ転送します。

貴方は XDNA 基金へのコインが無駄にならないと確信できます。

慈善目的で XDNA への食料、水、医療品を販売を実施したいと考えている世界中の団体へ、

我々に参加してください。共により良い世界を作りましょう。

タイムラインとブロック報酬分布

XDNA のライフスパンは2段階に分かれます。-Proof-Of-Work と Proof-Of-Stake。これらのフェーズではブロック報酬量と分布が異なります。

POW 稼働時、ブロック報酬は BitGun によって決定されます。次の様なブロック分布が適用されます。：

- マイナーへ 70%;
- Full Nodes へ 15% ;
- Medium Nodes へ 9%;
- Light Nodes へ 3% ;
- XDNA 基金へ 2% ;
- 開発チームへ 1% .

上記に基づいて、Pow 稼働中のブロック報酬分布は図5に示す様になります。

POW blockreward distribution

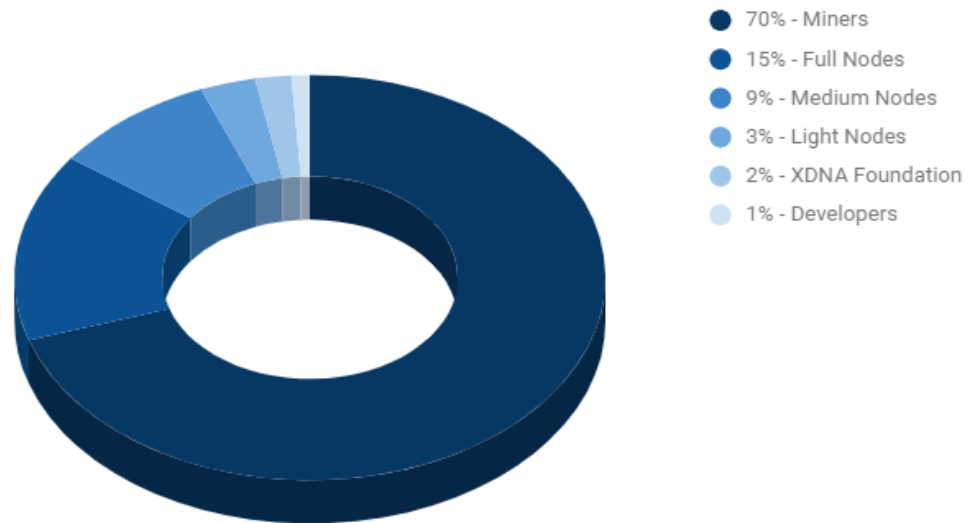


図5

1440000 ブロック到達または、1000 日後に XDNA は POS にスイッチします。

POS 開始時ブロック報酬は 57XMN になります。これは 10 番目の BitGun レベルに相当します。

この金額は 15 年後に予想される、87984401 ブロックに到達して 1XDNA になるまで、525600 ブロック(もしくは約 1 年)毎に 4 コインずつ下がります。

POS 稼働中は SeeSaw[2]アルゴリズムによって処理されます。マスターノードの報酬の割合は変わりませんが、総マスターノード報酬とステーキングウォレット報酬の割合は流動的に変化します。

それとは別に各ブロック報酬から 2%が XDNA 基金へ、1%が開発者ファンドへ行く予定です。

POW 稼働時の全体のネットワークハッシュレートを予測する事ができない為、POW フェーズの最大コイン供給量を計算することはできません。これを見積もる為にブロック報酬の平均を使用し、POW 稼働時の総供給量が約 138,000,000 XDNA である事を予想しています。

毎年ブロック報酬が減少していく POS フェーズの 15 年分の放出は約 228,000,000 XDNA。

上記の計算によると 18 年間での総コイン供給量は約 366,000,000XDNA。

この金額には 971,712XDNA の事前採掘分が含まれていません。これは 7 日間のマイニング供給と平均ブロック報酬を掛け合わせたものに相当します。

事前採掘がどの様に分配されているか以下に示します:

- 350,000 XDNA -XDNA 基金創設。
 1. XDNA 投票プロジェクト
 2. ソーシャルファンドのインフラ
 3. 慈善活動
 4. 法的支援
 5. 事務費
- 271,712 XDNA -開発チームへの支払,内訳:
 1. 開発者への初期給与
 2. seed-nodes の為の VPS レンタル料
 3. ウェブサイト作成とドメイン取得料
 4. デザイン料
 5. SSL 証明書及びプロジェクト作成のその他の経費
- 350,000 XDNA - マーケティング費用, 内訳:
 1. 特別キャンペーン
 2. ソーシャルメディアプロモーション
 3. コミュニティの選出とコンテスト

4. スポンサーシップ
5. オフラインメディアイベント
6. 上場料
7. 仮想通貨上場手数料
8. 記念品の生産
9. ブログ、ビデオブログ等の広告
10. 印刷物やその他のソースのマーケティング費用

Premine distribution (971,712 XDNA or 0.7% of POW supply)

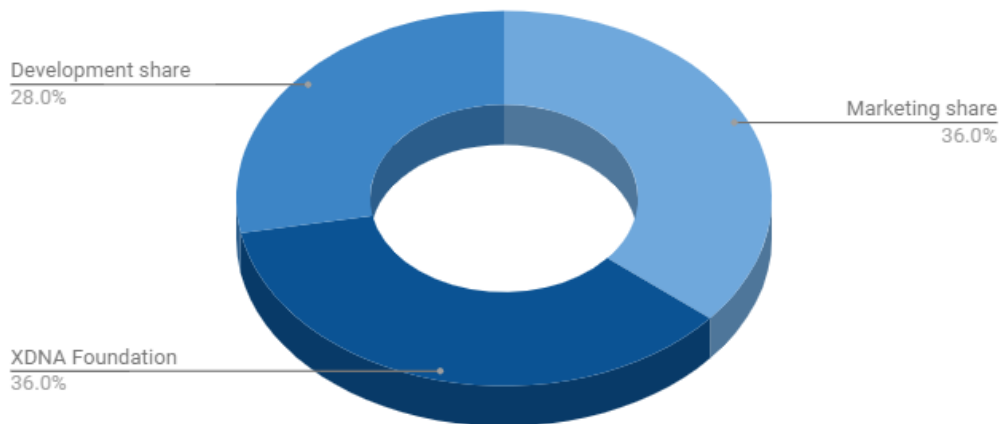


Figure 6

文献リスト

1. DASH Masternodes <https://dashpay.atlassian.net/wiki/display/DOC/Masternode>.
2. Seesaw Reward Balance System Whitepaper. Revision 0.7e, January 24, 2017 <https://pivx.org>.

クレジット

XDNA チームはプロジェクトの研究、開発、テスト、サポートにおいて、以下の人々に感謝の意を表します：

S.F.Vakano
Gunbit
Kamir
George a.k.a. Commie
nullptr
a.kapone
koksoks
SiriS
Imbalance911
msbishop
TheUnknownHero
Allison
B52
oGrInGo
Satt
Kaseman
TeMbl4
marikun