



NULS - プルーフ・オブ・クレジット (POC) プロトコール

白書 バージョン 1.1 ベータ
2017年12月5日 更新

「Null」はゼロ、
「NULS」はブロックチェーンの世界の全てを

NULSとは何か？

NULSとは、マイクロカーネルや機能本位のモジュールを搭載する、カスタマイズ性に長けたオープンソースのモジュール型グローバルブロックチェーン基盤です。NULSはスマートコントラクト、マルチチェーン構造とクロスチェーンコンセンサスを提供します。ブロックチェーンに必要な知識や技術へのハードルを下げるとともに、開発に必要なコストを抑え、ブロックチェーン技術をより広い層へ拡張します。



Mission

現在、ブロックチェーンの世界では、「簡単」「便利」「高機能」という3点を全て実現することに苦戦しています。

私達NULSは、カスタマイズ性に長けた公共のブロックチェーン基盤の提供を目標としています。

私達のプラットフォームの目的は、各企業の分散型アプリケーションの信用性の向上の実現を目指し、サポートとなる事です。



要約

NULSのブロックチェーンの基本構造においては、
スマートコントラクト、モジュールやサブチェーンの拡張が可能です。

NULSはオープンソースの事業であり、各機能を
「スマートコントラクト」「マルチチェーンシステム」「クロスチェーンコンセンサス」
など、カスタマイズ可能なモジュールに分離しています。

将来的にNULSでは、主体となるメインチェーンの機能構造から分離された複数の
サブチェーンを確立します。それらのサブチェーンは、NULSの基本プロトコルや
その基本構造を使用する事で、各企業のニーズに合わせて簡素化します。

Website: nuls.io

Mail: hi@nuls.io

Contents

1. ブロックチェーンの未来	5
2. NULSとは何か?	5
3. NULSはなぜ開発されたのか?	6
4. NULSの目的.....	6
A. 使いやすさ.....	6
B. 数々のアプリケーションに対応.....	6
C. 高性能.....	6
D. 平衡的透明性とデータの匿名性.....	7
5. NULSの実利モデル.....	7
A. NULSの4つの配給区分:	7
a. エアドロップ	7
b. 開発費	7
c. コミュニティへの基金.....	7
d. ビジネス提携.....	7
B. ネットワークメンテナンス.....	8
6. サブチェーンの運用	8
A. サブチェーンベースの通貨と高度な両替	8
7. NULS技術のデザイン	9
A. コンセンサスメカニズム - プルーフ・オブ・クレジット (POC)	9
B. イエローカード警告.....	9
C. レッドカード警告	9
8. クレジット評価.....	10
9. コンセンサスリワード.....	10
A. サブチェーン上のコンセンサスメカニズム.....	10
B. モジュールの構造.....	10
C. NULSモジュールとモジュールマネージャー.....	11
D. マルチチェーンシステム.....	11
E. クロスチェーンのコンセンサスドメイン (C3D)	11
F. クロスチェーンのコンセンサスノード (C3N)	13
G. 安全性.....	13
10. NULSスマートコントラクト.....	14
11. オープンソースコミュニティ	14
12. NULS開発ロードマップ.....	14
13. 結論.....	15

1. ブロックチェーンの未来

私達は、人類の始まりから「生存」「教育」「順応」を通して次世代へと適切に進化してきました。その絶え間ない進化により、「科学技術の時代」である21世紀に突入できました。私達の生活は、衰えること無く日々加速をしています。ブロックチェーンという技術の登場により技術革新を更に促進させ、クリエイティブな人々をも取り込んできました。活気に満ちているブロックチェーンの環境は、技術者だけでなく世界中のさまざまな個人にまで浸透し、多様な人材がこの革新的な技術の成長に徐々に関わり始めています。

一方、この技術が成熟する渦中、現実社会における課題を解決する必要性が浮き彫りになってきました。しかしながら、ブロックチェーンはまだ初期段階にある為、実社会への導入に至っていないのが現状です。その背景の一部には、技術そのものの学習曲線の高さが挙げられます。更に、既存のブロックチェーンの多くは、得意分野が限定的であるか、反対に広すぎるがゆえに個人や企業のニーズに対応できていません。そこで、いろいろな企業や個人のニーズに容易に合わせられ、且つ、基礎基盤を変更する事無く技術革新ができる新しい形のブロックチェーンの必要が迫られてきています。

2. NULSとは何か？

NULSとは、カスタマイズ性に優れたモジュールや順応型のサブチェーンを可能にする、モジュールベースのブロックチェーンです。基本要素は大きく別けて、「マイクロカーネル」と「機能別のモジュール機能」の2つあります。マイクロカーネルはネットワークの基本を定義し、機能別のモジュールはブロックチェーンの様々な機能に区分されています。これらはプログラミングの理想である、「高い凝集力」と「低い相互依存性」を目標として開発されました。更に、システム稼働中にホットスワップができる為、いつでもモジュールの追加・削除が可能です。

NULSの分散システムの本質は、信頼性の高い技術であるだけでなく、ユーザー独自のニーズに合わせるられるビジネスモデルにあります。実装の簡略化はNULSの基本構成によって、暗号理論、コンセンサスメカニズムと保管方法はユーザー側（開発者側）から不可視にすることで、ユーザーは実際に何を作りたいのかという事に専念出来ます。

また、メインチェーンの基本構造に基づき、ユーザーのニーズに合わせてカスタマイズ可能なモジュールコンポーネントが用意されています。「コンセンサス方法」「保管方法」「仲裁方法」「アカウントのシステム」「匿名システム（ルール）」や「サブチェーン特有の許可設定」を自由に設定できます。サブチェーンは公開チェーンだけではなく、非公開や限定公開も可能です。

3. NULSはなぜ開発されたのか？

ブロックチェーンには、データベースのサイズ制限、シンク口の難易度や技術的なアップデートを分散型システム上での実装が可能か否かという制約があります。

その為、実社会における問題を解決するとともに、開発者に負担をかけないブロックチェーンの存在が必要でした。開発者のニーズに合わせてカスタマイズが可能なモジュールを使用することで、制限のない最大限のポテンシャルの製品を開発することが出来ます。このような問題の解決に加え、ブロックチェーン技術の商用利用を拡大する為、NULSは誕生しました。

4. NULSの目的

市場の調査・分析の結果、ブロックチェーンの開発や成長の妨げになる数々の課題が浮上しました。現在、IT分野において優秀な人材を探すだけでなく、ブロックチェーンの経験が豊富な人材は更に希少です。そしてこれらの人材には限りがある為、需要と供給によって報酬（給与）は高くなり、開発費が高額になっていきます。この問題はすぐには解決されないものであり、開発者の増加と同時に技術理解が更に深まる必要があります。

既存のブロックチェーンは機能に制限があり、クロスチェーンの情報交換は未だ模索中の状況です。企業や団体は、信用性の低いプライベートチェーンやコンソーシアムを使用しません。NULSはこの問題に対し、確かな解決策を提供します。

A. 使いやすさ

開発者から多少の複雑性を取り除くことで、NULSを開発する為のハードルを下げます。シンプルなプログラミング環境を用意することで、経験があまりない開発者に配慮するとともに、経験豊かな開発者への拡張をも可能にすることが、最終的なゴールです。

B. 数々のアプリケーションに対応

アプリケーション層では、開発者がプラットフォーム上に用意された機能を使用することが可能です。容易に基本的なタスクに対応が可能で、スマートコントラクト、マルチチェーンやモジュール部分を使用できます。

C. 高性能

NULSは、パフォーマンスの重要性を理解しているとともに、社会により広まることで生じる現在のブロックチェーンに懸念される問題を解決するために専念します。マルチチェーンシステムの並行拡張を使用し、メインチェーンとサブチェーン間、合わせて一秒間で数百万件の取引が可能です。

D. 平衡的透明性とデータの匿名性

データのセキュリティや匿名性は、企業や団体にとって最も重要なことです。そして、企業や団体は一般的にオープンソースであるブロックチェーンの透明性を懸念し、この新技術を使用する事を躊躇します。NULSはオープンソースですが、データアイソレーションとクロスチェーンデータの監査を駆使し、サブチェーンデータの匿名性を保護します。これらのデータの透明性と匿名性のバランスによって、オープンソースであるにも関わらず、NULSは企業に対して魅力的だと言えます。

5. NULSの実利モデル

NULSトークンはシステム全体を促進する為に利用されます。NULSベースのアプリを支え、アプリケーションコストの支払い、サブチェーン上のデジタルアセットの両替、NULS開発のサポート、マイナーへの賞金の支払いや運用における各手数料の支払いに使われます。

A. NULSの4つの配給区分

a. エアドロップ

トークンの4割（4000万）はERC20トークン保有者にエアドロップされます。

b. 開発費

トークン全体の2割（2000万）は開発費に使用されます。メインネットのオンライン開始以降、これらのトークンの5%（100万）は20ヶ月間、毎月アンロックされます。

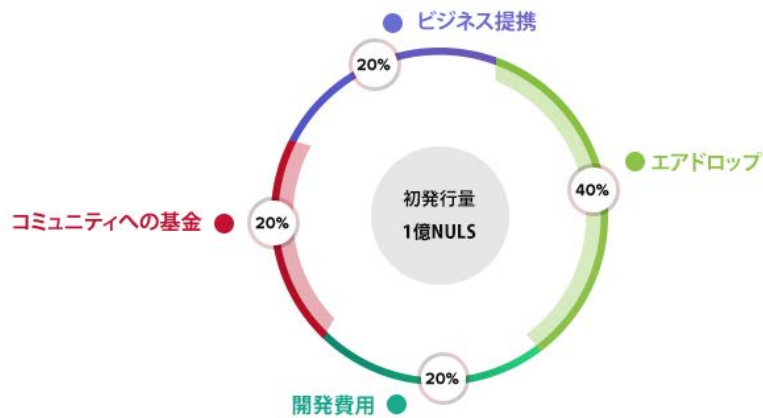
c. コミュニティへの基金

トークンの2割（2000万）はコミュニティの構築に使われますが、年間、最大で400万トークンまでの使用に限られます。

d. ビジネス提携

トークンの2割（2000万）はビジネス提携に使用されるとともに、高品質なNULSベースのサードパーティプロジェクトのサポートにも使用されます。年間、最大で400万トークンまでの使用に限られます。

NULS 配給メカニズム



B. ネットワークメンテナンス

500万NULSは毎年、マイナーへの賞金とネットワークの保証の為に、プルーフ・オブ・クレジットコンセンサス (POC) を通じて発行されます。

6. サブチェーンの運用

健康なシステムの構築の為、すべてのNULSサブチェーンは一定量のNULSトークンの支払いが請求されます (金額現在未定)。これは、正式なNULSサブチェーンであるという事を証明する為です。具体的に請求される金額は市場価値によって変動し、合理的な範囲内でコミュニティの投票によって決定されます。

A. サブチェーンベースの通貨と高度な両替

メインチェーンに使用される通貨は「NULS」であり、それぞれのサブチェーンは各自の基本トークンをサポートすることが可能です。これらは「NULSアセット」として考えられ、サブチェーンはこれらの契約トークンを「借用証明アセット」

(IOU) として発行が可能です。NULSシステムは、これらのスマートアセットとNULSトークン同士の変換を提供します。

サブチェーンがこれらのスマートアセットの発行を希望した場合、一定量のNULSの支払いが必要です。スマートアセット発行の際、ユーザー自身がスマートアセットとNULSトークンとの変換比率を設定します。

NULS資本プールとスマートアセットプールは自動的に作成され、変換比率は一定ですが市場価値によって変動します。

サブチェーン上のスマートアセットの価値が上昇した場合、価値の真価にあわせてNULS資本プールはより多くのNULSを必要とします。より多くの良質なサブチェーンプロジェクトがNULSを使用すればするほど、NULSの真価も上昇していきます。

7. NULS技術のデザイン



A. コンセンサスメカニズム - プルーフ・オブ・クレジット (POC)

NULSを構築しているモジュール型デザインは、新機能のモジュールの挿入やコンセンサスメカニズム既存の軸となるモジュールの交換が可能です。ユーザーはサブチェーンのルールをニーズに合わせてカスタマイズ出来ます。

メインチェーンはNULSチームによって新開発されたプルーフ・オブ・クレジット (POC) プロトコルを使用します。プルーフ・オブ・ステークのように、ユーザーが一定量のトークンを確保することで初めてノードとしてネットワークに承認されます。具体的な金額等はコミュニティの投票によって決定されますが、現時点では未定です。

ユーザーがノードを停止した時点から、それらのトークンは開放されます。

B. イエローカード警告

ユーザーが何らかの理由（ネットワーク接続問題やコンピュータ異常など）でインターネット未接続時にブロックを生成した場合、ネットワークルール違反として処理されます。しかし、システム全体に影響をきたす為、一定時間（72時間など）トークンを凍結する警告が発行されると同時にクレジット評価が減少します。

C. レッドカード警告

「敵意のある攻撃」「二重使用攻撃」「システム自体の強制分割（強制フォーク）」がされた場合、NULSネットワークはこれらを検知し、脆弱性や不正利用などからシステムを保護します。すべての不正ノードは更に長期間（一ヶ月など）トークンが凍結され、クレジット評価は更に減少します。これにより、最低確保金額を達成できない為、ネットワークに参加ができません。

8. クレジット評価

クレジットシステムは、各ユーザーのネットワーク上での保安全性・完全性を保証する為に導入されています。クレジット評価は、各ノードの挙動に合わせてアルゴリズムにより自動的に-1と1の間に決定されます。

クレジット評価の方式

クレジット基数 = 容積係数 + 義務係数

容積係数：過去累計ブロック生成数によって算出

義務係数：違反等の累計数と正確に生成されたブロックの累計数によって算出

9. コンセンサスリワード

NULSシステムのバランスや公平性を保証するため、コンセンサスリワードは、累計の賭けトークンと全ノードによって提示されたクレジット評価によって算出されます。

A. サブチェーン上のコンセンサスメカニズム

NULSのサブチェーンは基礎基盤を提供しており、各ユーザーが構築したサブチェーン上に新たなアプリケーションの作成、配置が可能です。

構成要素として、NULSの各ユーザーのトークンやサブチェーンを容易にカスタマイズすることができると同時に、ユーザー自身がどのようなコンセンサス（POW,DPOS,PBFT,POOL）で運用を行うかの選択が可能です。

B. モジュールの構造

NULSの構造デザインは、テクノロジーの進歩は今後も急速に進み、静的な技術は取り残されるという思想から生まれました。NULSはLinuxカーネルのモジュール性を導入することによって、柔軟性が高い機能的なブロックチェーンを実現しました。全てがモジュールである為、最新の技術アップグレードを容易にブロックチェーンに追加することが可能です。

Nuls モジュール設計



NULSモジュール構造

NULSカーネル：NULSカーネルは、「モジュールマネージャー」「サービスバス」「イベントバス」からなります。

カーネルは以下の機能を管理します

モジュールコンポーネント：「スマートコントラクト」「アカウント」「ストレージ（保管）」「アカウント」「コンセンサス（合意）」「プロセッサー」

NULS内蔵モジュール

サービスモジュールパック：「RPCサービスモジュール」

プロセッサーモジュールパック：「イベントプロセッサーモジュール」→「スマートコントラクトプロセッサーモジュール」

基本モジュールパック：「コンセンサス（合意）モジュール」→「ネットワークモジュール」→「保管（記憶）モジュール」→「ニュースモジュール」→「アカウント」→「アカウントブック」

C. NULSモジュールとモジュールマネージャー

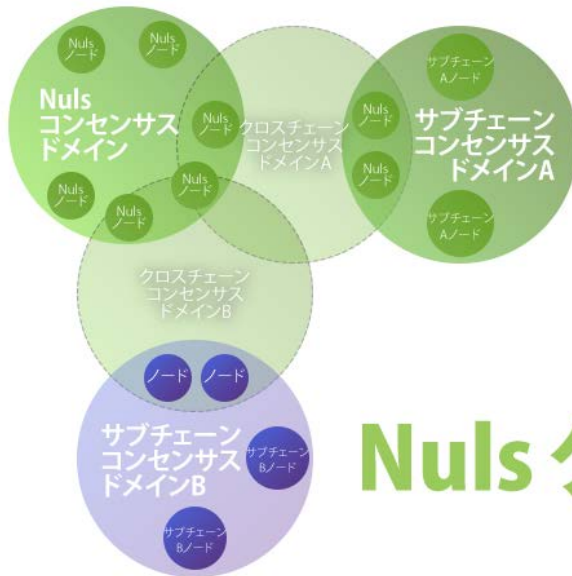
モジュールマネージャーとは、オンライン／オフライン問わず、全てのモジュールが管理されている場所です。モジュールがオンラインに切り替わると、他のモジュールとの通信が可能になり、様々な行動を実行する事ができます。専門的な観点では、NULSは「開放/閉鎖原則」を念頭に開発されました。拡張のために開放しますが、変更・修正は閉鎖されます。

D. マルチチェーンシステム

ブロックはクロスチェーンコンセンサスで承認され、NULSはメインチェーンとサブチェーン間を循環する事が可能です。サブチェーンはメインチェーンに報告をし、メインチェーンはヘッダーを審査と承認をします。

E. クロスチェーンのコンセンサスドメイン（C3D）

メインチェーンとサブチェーンの一部のノードは、クロスチェーンのコンセンサスドメイン（C3D）を構成します。それぞれのノードはお互いにクロスチェーン上の取引を一致させて他のノードに伝送し、同じチェーンのノードへと拡散します。

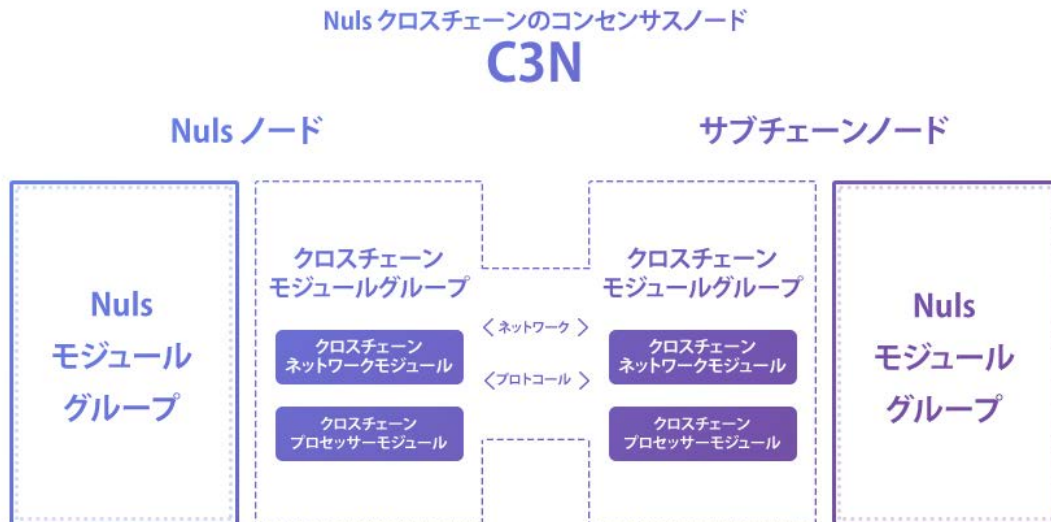


Nuls クロスチェーン コンセンサス

- メインチェーンのコンセンサスドメイン (メインチェーンのノードが包囲)
- サブチェーンAのコンセンサスドメイン (サブチェーンAのノードが包囲)
- サブチェーンBのコンセンサスドメイン (サブチェーンBのノードが包囲)
- 重なった区域：クロスチェーンのコンセンサスドメインA
- クロスチェーンのコンセンサスドメインB

F. クロスチェーンのコンセンサスノード (C3N)

クロスチェーンのコンセンサスに参加したノードは、「クロスチェーンネットワークモジュール」や「クロスチェーンプロトコルモジュール」という、2つのチェーン上で運用可能なモジュールを使用する必要があります。



NULSのノード

メインチェーンのモジュールパック：メインチェーン理論を操作します
 クロスチェーンのモジュールパック：NCMネットワークコントロールモジュール、プロセッサモジュールコミュニケーション、プロトコル
 サブチェーンのモジュールパック：サブチェーン理論を操作します

G. 安全性

クロスチェーンのコンセンサスプロトコルは2つのポリシーを使って、ネットワークの安全を保証します。

- ドメインの一元化を阻止する為にクロスチェーンコンセンサスの最低必要条件を配備
- 1つのクロスチェーンノードが継続的に情報を発信をしないための動的調整 (交代)

10. NULSスマートコントラクト

NULSはスマートコントラクト仮想マシン（NULSVM）を搭載しており、構造上、外部サービスモジュール（RPCモジュールなど）と基礎構造モジュール（ネットワークモジュール、ストレージモジュールやアカウントモジュール）の間に位置します。スマートコントラクトは高位レベルアプリケーションに使用され、解釈プログラムによって解釈された後、ストレージモジュールで保管し、NULSVMモジュールによって計算が行われます。複数の高位プログラミング言語をサポートしており、開発者が希望する言語で開発を行い、仮想マシンがアプリケーションを読めるように解釈プログラミングを通じてコンパイルをします。

11. オープンソースコミュニティ

NULSはコミュニティに支えられているオープンソースなプロジェクトです。オープンソースにする事によって、開発者間の信用・透明性を向上させ、強いコミュニティを確立します。コミュニティの力で、包括的な開発資料と開発者の支えとなる完成されたツールを提供します。NULSのエコシステムへの貢献者や素晴らしいプロジェクトをサポートする為、NULS財団は、コミュニティ基金として合計2000万NULSの基金を設立しました。NULS財団コミュニティはシンガポールにて登記されています（NULS FOUNDATION PTE. LTD. 201729333G）。コミュニティに支えられた開発環境によって革新的なプロジェクトを促進させると同時に、簡易的なツールを提供し、開発そのものを加速させる事がNULSの主要な目標です。

12. NULS開発ロードマップ

ロードマップ



ICE WATER STEAM

- ☞ POWモジュールとPOSモジュールを含む、機能的なモジュールを更に完成させる
- ☞ 最低5つのサブチェーンがNULSに参加
- ☞ 最低15個のアプリケーションがNULS上で動作
- ☞ 技術ソリューションを最低3つの業界へ提供

テクノロジー

更なるコンセンサスマジュール埋め込みを完成させ、自己進化型ネットワークとストレージモジュール（容量がエクサバイト分のストレージ）を掌握
 複数の業界にかけて、基本となる技術ソリューションを形成
 ビッグデータや人工知能（AI）などの分野で汎用できる
 ブロックチェーンを使った新しいシステムを確立する

エコロジー

成熟したオープンソースコミュニティを形成し
 大規模のアプリケーションサブチェーンを作成

ICE WATER STEAM

- ☞ 最低30個のサブチェーンがNULSに参加
- ☞ 最低50個のアプリケーションがNULS上で動作
- ☞ ビッグデータ等、NULSを基盤とした新しいシステムを最低20個の業界へ技術ソリューションを提供

テクノロジー

企業や農業の双方において、生産・管理が完成されたソリューションを提供。
 完全な技術プラットフォームからなるブロックチェーンインテグレーション。
 人工知能（AI）とビッグデータが1つのシステム上に動作する。

エコロジー

ブロックチェーン、ビッグデータ、人工知能（AI）分野を統合したオープンソースのコミュニティを形成
 総合的価値のドッキングと
 コラボレーションプラットフォームを提供

13. 結論

NULSチームは現在のブロックチェーンにおける問題を認識しています。ハッカー、バグ、悪意のあるノードや不誠実な個人によって、信用という幻想は幾度となく脅威に晒されてきました。「信用をシンプルに」というNULSのミッションは有用性重視のブロックチェーンのネットワークを強化するとともに、企業とブロックチェーン技術採用の間を埋めます。それでも、技術レベルが高いブロックチェーン開発者が不足しているという壁は、今後のブロックチェーンの拡張の妨げになる事は否めません。
 NULSは、「企業、開発者と支援者の為のシステムを築くソリューション」の実現を目標とします。