



# INTRAMO

## ホワイトペーパー

INTRAMO

THE KEY TO GROWTH IS TO INTRODUCE HIGHER  
DIMENSIONAL CONSCIOUSNESS INTO OUR CONSCIOUSNESS



「成長の鍵は、私たちの意識により高い次元の意識を導入することです。」

- 老子(紀元前604-531年)

2008年のビットコインの発明は、暗号通貨の出現を象徴していました。次の年は、ブロックチェーン技術の劇的な発展を目撃しました。イーサリアムの立ち上げは、暗号通貨を支える複雑なビジネス慣行への道を開きます。

しかし、全体的な勢いは現在、いくつかの重要な課題に直面しています。その中で

- 1) スマートコントラクト向けのルールベースの意味解析および構文解析エンジン。
- 2) スマートコントラクトの安全性を証明するための正式な検証ツールキット。
- 3) 取引モデルの識別およびセキュリティチェックに使用するAIベースの検出エンジン。ディープラーニングに基づくダイナミックセキュリティ検証および強化
- 4) プラットフォーム。

Intramoは、下記の課題を解決するために最新の人工知能技術を利用する新世代のブロックチェーンになることを目指しています。ブロックチェーンと人工知能技術の融合により、INTRAMOは、トランザクション速度の大幅な向上、一般ユーザーへの優れたアクセシビリティをサポートする革新的な暗号通貨を構築することができました。悪意のある攻撃に対するセキュリティの強化と柔軟性の高い運用ができます。

一、 Intramoの目標	4
1.1 スマートコントラクトの自動生成	4
1.2 安全なスマートコントラクト	4
1.3 高速取引	5
1.4 柔軟なブロックチェーン管理	5
1.5 付加価値のあるマイニング	5
二、 Intramo技術革新	6
三、 Intramoのキーテクノロジー	8
3.1 ランダムなネットワーク縮小に基づくハイブリッドPoS+PoWコンセンサス	9
3.2 ディープラーニングに基づくスマートコントラクトコード生成	10
3.3 人工知能のセキュリティ検証と拡張	11
• 3.3.1 構文解析と意味解析	11
• 3.3.2 スマートコントラクトの形式的検証	12
• 3.3.3 人工知能ベースのスマートコントラクト検証	13
• 3.3.4 ディープニューラルネットワークに基づく動的検証とセキュリティ化	14
3.4 柔軟性の高いブロックチェーンラック	15
• 3.4.1 Intramoのマルチチェーン構造	16
• 3.3.2 ブロックチェーンパラメータの自然な進化	17
3.5 マルコフ連鎖モンテカルロ計算の証明	18
四、 Intramoの経済学	21
4.1 発行メカニズム	21
4.2 トークンの配布	21
五、 Intramo結論	22
六、 免責事項	23
6.1 免責事項	23
6.2 リスク警告	23

# 一、Intramoの目標

今日のブロックチェーンが直面している課題を実現する必要があります。

暗号通貨は本当に現実のものになる可能性があります。AIテクノロジーは過去10年間で前例のない成長を遂げ、課題に対するすぐに使えるソリューションを提供していると信じています。MATRIXは、ブロックチェーン技術の潜在的な力を解き放つスマートチェーンを目指しています。このセクションでは、MATRIXの目標について簡単に説明します。

## 1.1 スマートコントラクトの自動生成

スマートコントラクトは、大規模なビジネス行為を処理する基本的な機能をブロックチェーンに提供しますが、ユーザーは特定のレベルでビジネス行為を処理する必要があります。

プログラミング言語。Intramoを使用すると、スマートコントラクトを設計するためにプログラミングの専門知識は不要になります。Intramo独自のプログラムコード生成技術により、スマートコントラクトの抽象的な記述を自動的に実行可能プログラムに変換できます。Intramoは、ユーザーがコマンドコード言語を使用して契約のコア要素(入力、出力、取引条件など)を入力するだけで済みます。ディープニューラルネットワークに基づくコードジェネレーターは、スクリプトを同等のプログラムに自動的に変換できます。

## 1.2 安全なスマートコントラクト

スマートコントラクトプログラムは、ホストシステムやサードパーティのライブラリによって提供される関数を呼び出すことができます。さらに、分散フレームワーク内の異なるコンピューターで実行されているプログラムは、実行時間を保証しません。このオープン性と分散化は、ブロックチェーンの本質的な精神を体現していますが、セキュリティの脅威のさまざまな原因も生み出しています。実際、セキュリティの欠如はスマートコントラクトを悩ませています。Intramoブロックチェーンには、4つの主要コンポーネントで構成される強力なAIセキュリティエンジンが搭載されています。

- 1) スマートコントラクトのためのルールベースのセマンティック及び構文分析エンジン
- 2) スマートコントラクトの安全な内容を証明するための正式な検証ツールキット
- 3) トランザクションモデルの識別とセキュリティチェックのためのAIベースの検出エンジン
- 4) ディープラーニングに基づく動的なセキュリティ検証および強化プラットフォーム。

### 1.3 高速

今日、すべてのパブリックチェーンは、長いトランザクションレイテンシと低いトランザクションスループットの問題に直面しています。具体的には、ビットコインがトランザクションを完了するのに30分以上かかりますが、イーサリアムのトランザクションスループットはわずか10送信/秒 (TPS) です。実際、ブロックチェーンはトランザクションを検証するためにP2Pネットワークに依存しています。トランザクションはネットワーク内のすべてのノードにブロードキャストするため、ネットワークに参加するノードが増える限り、合計遅延を増やす必要があります。Intramoは、すべてのノードが他のノードへのデリゲートとして投票されるデリゲートネットワークを動的に選択することで、この問題を解決します。すべてのプルーフオブワーク (PoW) 処理は、委任されたネットワーク内でのみ分散され、ノード数が少ないため、遅延が小さくなります。ノードを選択する確率はプルーフオブステーク (PoS) に比例するため、選択プロセスはランダムです。イントラモのオンラインバージョンは、100,000 TPSのスループットをサポートします。

### 1.4 柔軟なブロックチェーン管理

Intramoは、柔軟性の高いブロックチェーンアーキテクチャを目指しています。柔軟性は2つあります。まず、プライベートチェーンをパブリックチェーンにシームレスに統合するために、アクセス制御とルーティングサービスを提供します。このような機能は、多くの業界および政府のプレーヤーの承認要件を満たしながら、必要な情報をパブリックチェーンからプライベートチェーンに、またはその逆に流すことができます。第二に、Intramoは、強化学習フレームワークを使用して、進化チャンネルにおけるパラメータ (コンセンサスメカニズムやトランザクション割り当てなど) を最適化します。最適化パラダイムにより、ハードフォークのリスクなしに、ほぼ最適なパフォーマンスを得るためにパラメータを動的に更新できます。

### 1.5 付加価値のあるマイニング

おそらく、暗号通貨の最も非難される部分は、マイニング計算におけるエネルギーの「浪費」です。暗号通貨には物理的な価値がある必要がありますが、デジタル通貨の世界では、マイニングプロセスは意味がありません。この問題は現在、世界の計算能力の70%以上がビットコインやその他の通貨のマイニングに費やされているという事実によって悪化しています。Intramoは、ベイズ推論の重要なツールであるマルコフ連鎖モンテカルロ (MCMC) 計算を実行する新しいマイニングメカニズムを導入しています。MCMCに基づくベイズ計算は、遺伝子制御ネットワーク、臨床診断、ビデオ解析、構造モデリングなど、多くのビッグデータアプリケーションで重要な役割を果たします。このように、MCMCのコンピューティングノードの分散ネットワークは、現実世界の計算集約的な問題を解決する機能を提供し、物理世界と仮想世界の価値の間の架け橋を構築します。

## 二、Intramo技術革新

Intramoプロジェクトは、ビッグデータと計算高速化を使用して価格を予測する人工知能に基づいています。Intramoプロジェクトは、予測システムと取引モデルを構築するためのトップAI開発者と定量分析を通じて投資家に投資アドバイスを提供します。さまざまな仮想通貨のテクニカル分析も提供され、合計28のチャート分析モデルが合計ユーザーに使用されます。

トークンは、ユーザーがトランザクションにアクセスし、テストを実施し、トークンを獲得できるようにするプラットフォームのLearn 2 Earn機能にも使用できます。Intramoは、取引モデルの構築、価格変動の予測など、ユーザーの参加を通じてユーザーに報酬を与えます。

表1は、Intramoの基本技術をまとめたものです。これらのテクノロジーのおかげで、Intramoは異なり、新世代のブロックチェーンを開拓しています。

表1：Intramo的技術革新

カテゴリ	科学	創新目標
基礎協定	1. ネットワークを表すランダムにクラスター化された投票	トランザクションの遅延を短縮
	2. 個別の制御チェーンを導入する	パブリックチェーンとプライベートチェーン間の相互作用とセキュリティ制御の展開を実現
	3. 進化的パラメータの最適化	ブロックチェーン設計を外部の使用パターンと環境に適応させる
スマートコントラクトの生成	スマートコントラクトのプログラム自動生成 プログラム設計の障害を打破し、一般のユーザーがスマートコントラクトにアクセスできるようにします	プログラミングの障壁を取り除き、一般ユーザーがスマートコントラクトにアクセスできるよう
安全	1. 形式検証および深層学習に基づく監査、スマートコントラクトの知的審査、契約要素の関係審査、契約の形式検証、およびトランザクションの仲裁を含む。	潜在的な脆弱性と悪意を特定する
	2. バイナリコード検査	潜在的な脆弱性と悪意を特定する

	3. クレジットスコアに基づく信頼できるゲートウェイと (ORACLE)、パブリック ユーザークレジット スコアリング、マルチチェーン ベースのデータ ルーティングなど)	ネットワークのレピュテーションレコードを維持する
	4. 動的なセキュリティ検証と敵対的生成ネットワークによるスマートコントラクトの強化	高強度の攻撃に対する堅牢性の確保
	5. 主に使用される保証付き契約エスクローで	長期的なデリバティブ取引を可能にする
カテゴリ	テクノロジー	イノベーションの目標
商業	1. パターンマッチング	データ交換とマルチパーティトランザクションの識別を可能にするマッチングコントラクト
	2. 権限ベースのインデックス作成、プライバシーベースのユーザートランザクション追跡、および複数のユーザー行動に基づくインテリジェントなグループ化をサポートするトランザクションデータ検索エンジン	データ交換とマルチパーティトランザクションの識別を可能にするマッチングコントラクト
マイニング	BayesianとPOW計算としての深層学習	マイニングは普遍的な価値を生み出します

# 三、Intramoのキーテクノロジー

AIは、Intramoスマートブロックチェーンを作る上で重要な役割を果たします。さらに、Intramoは、ブロックチェーンテクノロジーの広範な最適化と拡張の産物でもあります。このセクションでは、Intramoによって行われた主要な技術的ブレークスルーを確認します。

## 3.1 ランダムなネットワーク縮小に基づくハイブリッドPoS+PoWコンセンサス

今日のブロックチェーントランザクションにおける過度の遅延の根本的な原因は、P2Pネットワークの伝送オーバーヘッドがノード数に応じて拡張できないことです。この問題は、すべてのトランザクションがそうであるように、P2PベースのPoWコンセンサスに固有のものであります。

ネットワーク全体にブロードキャストします。実際、ノードが追加されている限り。最近提案された雷電ネットワークは、上記の問題を解決するように設計されていますが、支払者、受信者、および送信ノード用のプライベートチャンネルを作成するだけで、コンセンサスに達するとトランザクションに到達します。このようなプロセスは、特にチャンネルが水中にあり、ブロックチェーンの外部で発生するため、悪意を持って攻撃された場合、セキュリティに欠けています。

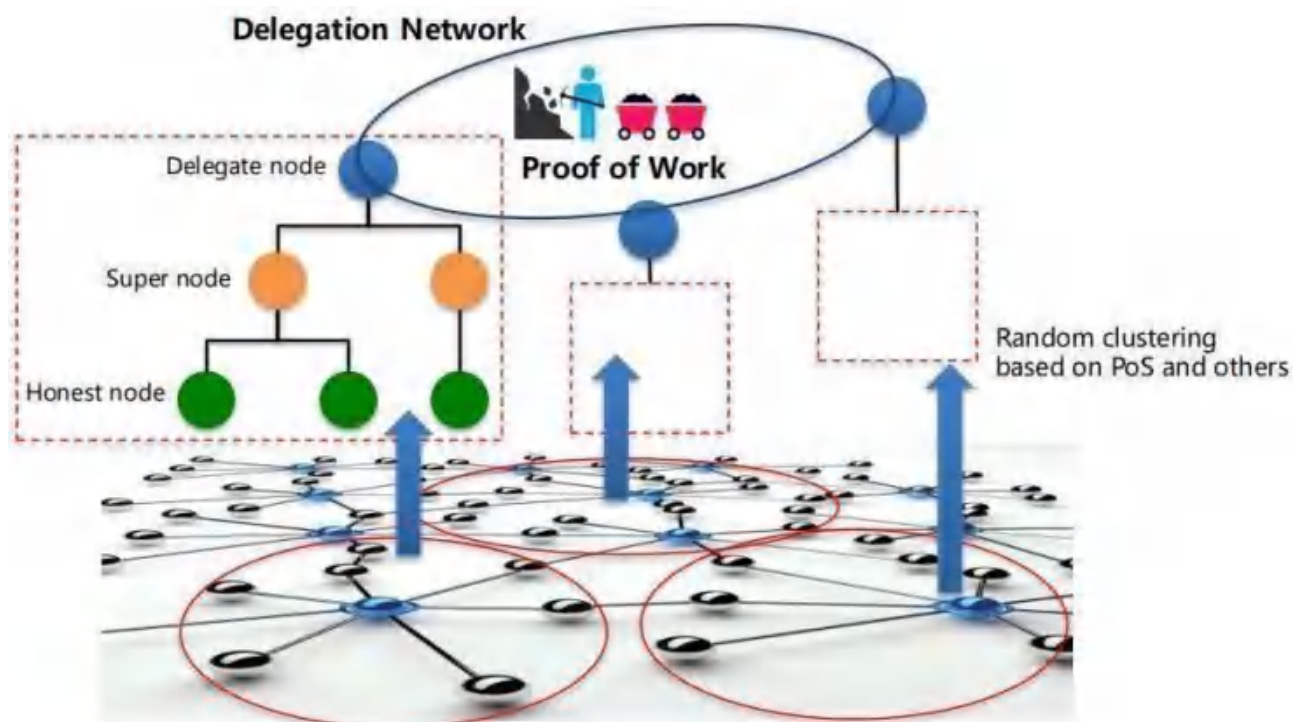


図1：ランダムクラスタリングに基づくPoS+PoWコンセンサス



すぐに使用できる効果的なソリューションは、ブロードキャストのオーバーヘッドを制御できる階層をP2Pネットワークに導入することです。重要なアイデアは、ネットワークをより小さなネットワークに縮小し(つまり、階層を作成し)、少数の契約ネットワーク、正直なノード、スーパーノード、委任されたノードのプルーフオブワーク、PoSに基づくランダムクラスタリング、およびその他の委任されたネットワークノードでPoW計算を実行することです。

独自の演算の基本的な考え方を図 1 に示します。この階層は、集中管理なしで分散ランダムクラスタリングプロセスによって作成されます。クラスターが完了すると、各ノードに独自の委任があります。選択された代表は、代表ネットワークと呼ばれる新しいネットワークを形成し、ノード数を調整できます。トランザクションは、委任された内部ブロードキャストネットワークPoW内の代表ノードにのみ割り当てられ、そのようなノードの1つはさらに分割できます。作業を小さなジョブに分割し、それらのジョブを投票するノードに割り当てます。クラスタリングは反復的に実行されることに注意してください。ノードがプロキシとして選択される確率は、そのPoSおよびその他の要因に比例します。

Intramo的分散ランダムクラスタリングに基づく整合性の計算は、次のように設計されます：

1. ノードはPoSまたはその他の要因に基づいています。
2. ノードは、ノードをクラスターとして参加するように要求し、ログインに使用される構成証明証明書への接続を要求する要求をネイバーに送信します  
チェックリストと入金リクエスト。他のノードがクラスターへの参加に同意すると、証明書が検証に使用され、コミットされた所属としてマークされます。彼らが同意しない場合、彼らは「競争相手」としてマークされ、セットから情報を受け取りません。
3. クラスターに参加した後、ノードは隣接ノードの接続ノードを計算し、特定のルールに基づいて候補のセットを選択します。ランダム方式では、最適な候補が選択され、適切なメッセージが他のノードに配信されます。
4. ノードに十分な数のセカンダリノードがある場合、そのノードはフルロードとしてマークされます。これらのノードは、他のクラスターをマージするために競合します。
5. ノードは、ネイバーに参加を求める招待をネイバーに送信します。マルチシグネチャメカニズムを通じて、マルコフ連鎖プロセスの初期化に使用できるコンパニオンシードを一緒に生成します。独立した第三者は、両当事者によって公開されたシード鍵、公開鍵、秘密鍵、およびMarkov計算の結果を見て、誰が勝つかを判断します。両当事者は結果を確認して署名する必要があり、結果は記録保持のために公開されます。
6. ノードは、他のノードが「完全にロードされる」(つまり、ノードの数が255に達するか、前のラウンドを超える)か、隣接する領域に直接移動する他のすべてのノードが完全にロードされるまで、他のノードをマージし続けます。その後、「検疫」としてマークされます。

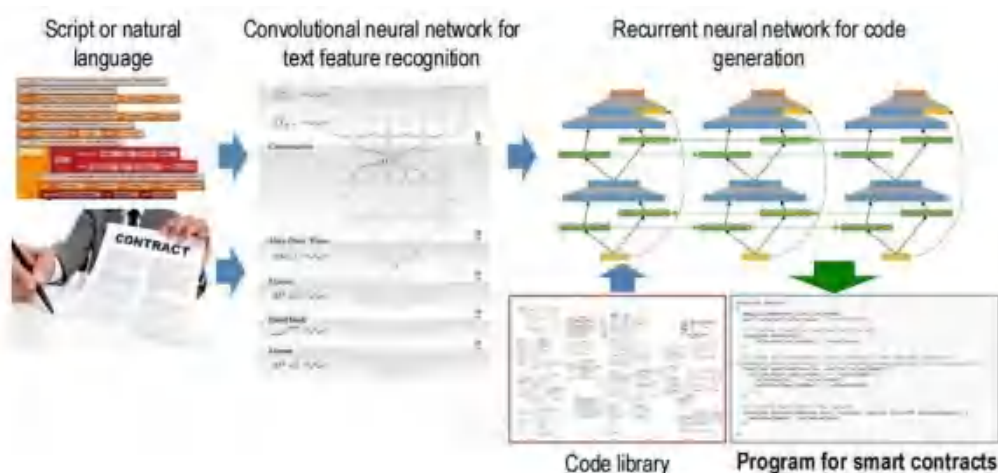
1. ネットワーク内に「完全にロードされた」ノードと「分離された」ノードのみがある場合、次の吸収ラウンドが開始されます。「フルロード」は「分離された」ノードのみを吸収し、その逆も同様です。「完全にロードされた」ノードは、「スーパー」ノード(対応するクラスターに $2^{16}$ を超えるノードがある、または前のラウンドのクラスター $N/128$ のノードの総数を超えることを意味します)または「孤立したスーパー吸収ノード」(ノードの数が32768未満であるか、残りの「フル」ノードが128未満であることを意味します)。

2. 255を超える「スーパー」ノードまたは「分離スーパー吸収」ノードがある場合、次の吸収ラウンドが開始され、ノードはコアノードになります。コアノードの数がノードの総数 $N/128$ を超えると、吸収プロセスが終了します。上記のプロセスは、存在するクラスターが255未満になるまで続行されます。これらのクラスターは「エージェントノード」になります

### 3.2 ディープラーニングに基づくスマートコントラクトコード生成

Instramo大きな利点は、スマートコントラクトのユーザーが知る必要がなくなったことです。プログラミング言語を使用してコーディングする方法。実際、マトリックスでは、ユーザーが契約の目的、つまり入力、出力、および取引条件をスクリプトとして入力するだけで済みます。ディープニューラルネットワークに基づくコードジェネレーターは、基本的なトランザクションパターンを識別し、ターゲットのスマートコントラクトの動作をキャプチャするプログラムに変換します。

将来的には、純粋な自然言語を入力フロントエンドとして使用する予定です。



深層学習技術の最近の開発は、自動コード生成の実現可能性を証明しています。

まず、畳み込みニューラルネットワーク (CNN) の成熟により、言語とスクリプトから高品質の特徴を選択できるようになりました。

第二に、リカレントニューラルネットワーク (RNN) は、任意のシーケンスを生成できるチューリング完全コンピュータであることが数学的に証明されました。これらのディープニューラルネットワークは、契約目的を分析し、対応するプログラムを生成するための重要な手法を提供します。

スマートコントラクトのコード生成プロセスを図2に示します。

コントラクトの目的をキャプチャするスクリプトは畳み込みニューラル作業に供給され、潜在的なトランザクションパターンとデータコンテンツを識別するために多数のラベル付きサンプルを使用してトレーニングされています。

発見されたパターンはシーケンスに編成され、リカレントニューラルネットワークに渡されます。RNNのパラメータは、典型的なインテリジェントモードでトレーニングされます。入力パターンを、スマートコントラクトのさまざまな設計パターンを含むターゲットプログラミングコードライブラリに変換します。

アクセシビリティが大幅に向上するだけでなく、イントラモのコード生成技術は、自動化されたセキュリティ検証および強化技術と簡単に統合できます。

実際、プロセス全体が反復的な改善のためのクロズドループとして機能する可能性があります。Intramoブロックチェーンの運用中、基盤となるモデルを継続的に更新して、コード生成の品質を向上させることができます。

### 3.3 人工知能のセキュリティ検証と拡張

Intramoはブロックチェーンのセキュリティを前例のないレベルに引き上げることを目指しています。全体的なセキュリティフレームワークは、次の4つの主要コンポーネントで構成されています

1. ルールベースのスマートコントラクトの意味論的および構文分析エンジン。
2. スマートコントラクトのセキュリティを証明するための正式な検証ツールキット、
3. トランザクションモデルの識別とセキュリティチェックのためのAIベースの検出エンジン
4. ディープラーニングに基づく動的なプラットフォームセキュリティの検証と強化。

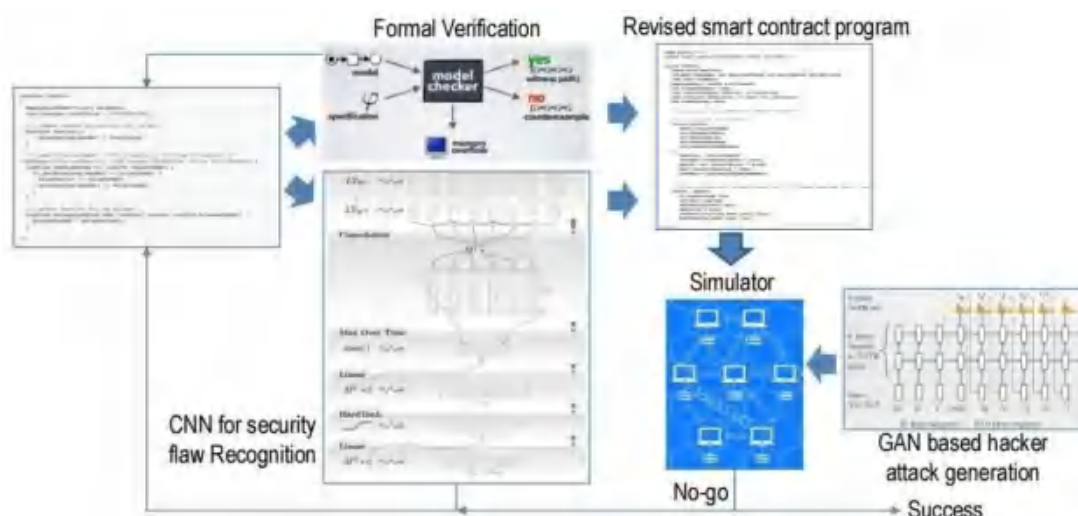


図3：ディープラーニングベースのスマートコントラクトプログラムのセキュリティ検証と強化

#### 3.3.1 構文解析と意味解析

スマートコントラクトプログラムを考えると、Intramoの内部コンパイラはBNFベースのASTを内部表現として構築します。

バイトコードアーカイブにコンパイルされたスマートコントラクトの場合、Intramoは最初にバイナリコードを逆アセンブルし、対応するINT0を生成します。

ドメインの知識と履歴経験に基づいて構築されたルールベースに基づいて、コンパイラは再帰的な降順解析を使用して、ASTにセキュリティの脆弱性がないかチェックします。

構文レベルでは、Intramoのコンパイラは対応する有限状態マシンとデータフロー図をプログラムから識別します。次に、ルールベースのチェックとコードリビジョンを実行します。

典型的な例は次のとおり：

- a) 不完全な条件による施行の問題を防ぐために、すべての契約条件を補足します。
- b) 呼び出されたすべてのパブリックメンバーと機能を分析して、契約の露出を判断します。
- c) 手順が完了しているかを確認して、条件記述が完全であることを確認します。Intramoのコンパイラは、意味レベルで文脈の検査を提供し、規則を満たさないか、安全でない操作を確定します。

典型的な例は次のとおり：

- (1) 外部環境にさらされなければならないオブジェクトとメソッドは、その必要性和潜在的な欠陥について検査されます；
- (2) ORACLEのコントラクトの分岐または処理が完了しているかどうか、およびコントラクトを呼び出すときに他の異常な操作がないかどうかを確認します；
- (3) 異なる呼び出しによる異常なシーケンスを回避するために、異なるオプションで同じ条件を確認します。

### ・3.3.2 スマートコントラクトの形式的検証

上記の静的構文解析および意味解析は、人的要因によって引き起こされる論理的な欠陥を特定することができます。ただし、ランタイムのロジックの問題は検出できません。たとえば、ターゲット契約が複雑な制約下にある場合、ユーザーは契約条件を定義できます。

さらに、コントラクトは分散環境で実行され、各ノードは一意の実行シーケンスを認識するため、セキュリティの脆弱性が発生する可能性があります。その結果、コントラクトの異常な実行により、他のプログラムが内部状態を変更する脆弱性が残る可能性があります。

Intramoブロックチェーンには、スマートコントラクトの安全なコンテンツを検証するための正式な検証フレームワークが装備されています。このフレームワークは関数型プログラミング言語に基づいており、

SMTソルバーを統合し、さまざまなモデルとツールを備えています。さまざまなソフトウェアや暗号化プログラムの検証に使用します。

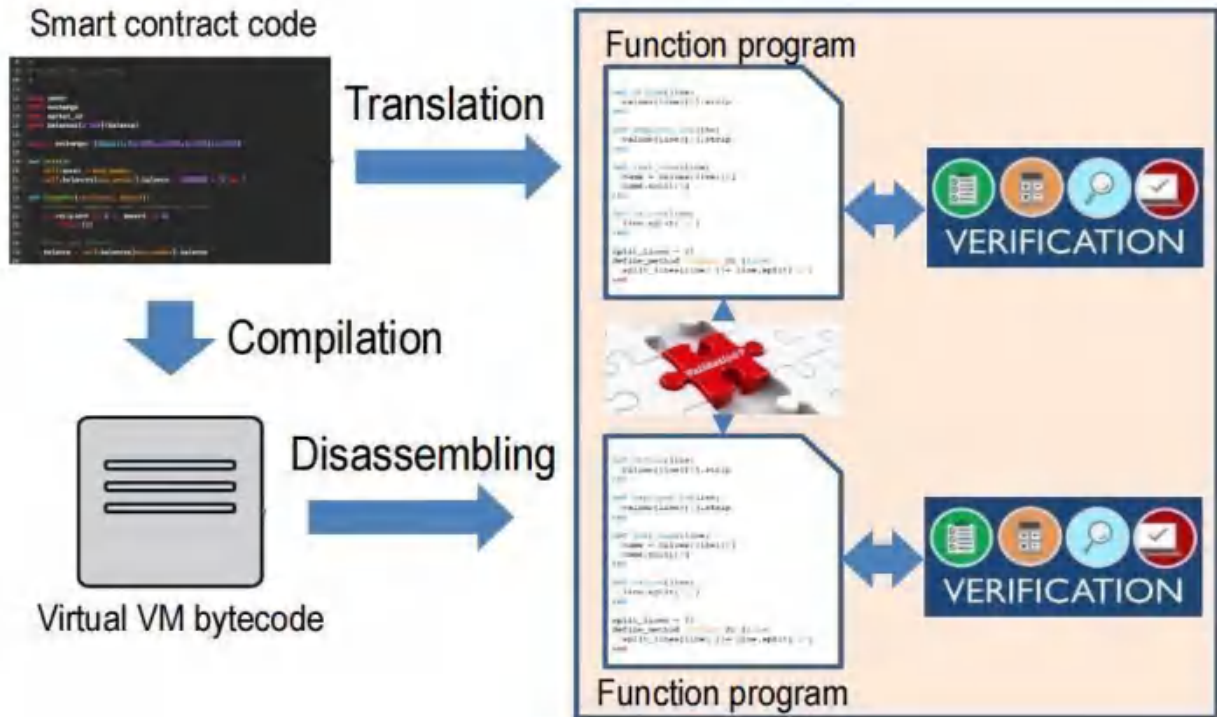


図4：スマート契約の正式検証

図4は、スマートコントラクトの正式な検証プロセスを示しています。検証ツールチェーンは、ソースコードとバイトレベルのコントラクトを処理できます。ソースコードは、関数型プログラミング言語と同等のものに翻訳されます。関数型プログラミングモデルは、非表示のロジックを公開し、後続の正式な操作を簡略化するために採用されています。INTRAMO 仮想マシンで実行するバイトコードは分解され、同等の機能プログラムに変換されます。等価性チェックおよびその他の整合性チェックは、2つの機能プログラムに対して実行できます。関数プロシージャを使用すると、一連のコンテンツチェッカーと定理証明者を適用して、さまざまな安全なコンテンツを検証できます(たとえば、send() 関数の戻り値がチェックされているかどうか)。

### 3.3.3 人工知能ベースのスマートコントラクト検証

上記の正式な検証では、明示的な正式なルールによってキャッチできる脆弱性とバグが明らかになりました。一方、考えられるすべてのシナリオをカバーするセキュリティコンテンツの完全なセットを定義することは困難です。Intramoにはディープラーニングベースのフレームワークがあり、スマートコントラクトの隠れた意図を発見し、セキュリティの脆弱性の複雑なパターンを検出します。

Intramoは畳み込みニューラルネットワークを使用してテキストの特徴を抽出し、興味深いパターンを検出します。これらのパターンは、構文パターンまたは構造パターン(または両方の組み合わせ)にすることができます。前者は通常、文法および機能的特徴を含み、後者は構造的な特徴を含みます。

CNNは、手動でトークン化されたイーサリアムのオープンソーススマートコントラクトについてトレーニングされています。

Intramoの主な特徴は、人工知能を使用してプログラムの構文を自動的に認識し、典型的なモデルを検出し、セキュリティ要件を満たすコンテンツを自動的に生成することです。スマートコントラクトプログラムを指定すると、IntramoのAIエンジンは類似性の部分一致と完全一致を自動的に検出して、コードの動作モデルを予測します。このようなモデルに基づいて、AIエンジンは、詳細な形式検証に関連する一連の制約を生成します。

### 3.3.4 ディープニューラルネットワークに基づく動的検証とセキュリティ化

これらの問題を解決するために、は、2つIntoramoの動的方法、すなわち敵対的生成ネットワーク (GAN) に基づく方法を採用しています。

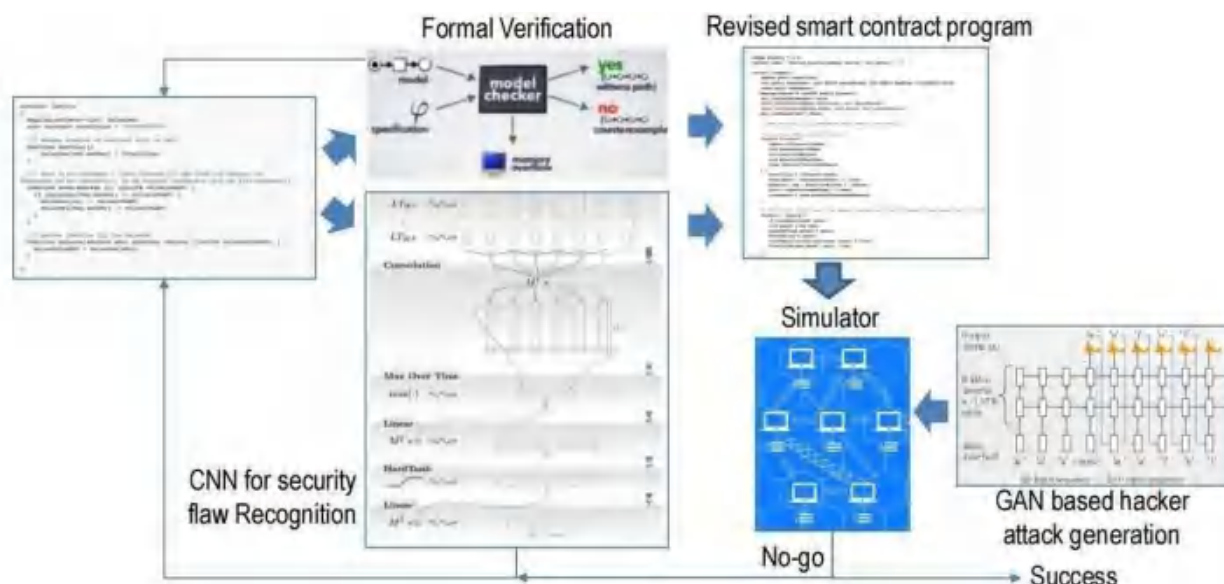


図4：スマート契約の正式検証

#### 3.3.4.1 敵対的生成ネットワークに基づくセキュリティ検証

Intramoは、最近開発された敵対的生成ネットワークを使用して、動的なセキュリティ認証を可能にします。図5に示すように、動的検証プロセスは、閉ループとしてコード生成フレームワークに結合できます。GAN フレームワークは 2 つの RNN で構成されています。1つのRNNはスマートコントラクトの既存のプログラムを変更するために使用され、もう1つのRNNは特定の確率分布のランダムサンプルから ハッカープログラムを生成することを学習します。スマートコントラクトプログラムが生成されると、対応するハッキングコードとともに「サンドボックスシミュレーションネットワーク (制御されたパイプラインで実験を行うことができるブロックチェーンをシミュレートするネットワーク)」に展開されます。これら2つのネットワークのコスト関数はリンクされているため、システム全体がナッシュ平衡に達したときに、全体最適を達成できます。この時点で、改訂されたスマートコントラクトスキームは最高レベルのセキュリティを備えています。

#### 3.3.4.2 分散型並行性に基づくダイナミックモデルの検証

上記の一般的なセキュリティ検証および強化技術に加えて、Intramoは以下のカスタマイズされた攻撃ツールを導入しました。

### コントラクトシーケンス攻撃

この攻撃は、スマートコントラクトの実行が非同期であり、動的に変化するという事実を利用して、います。コントラクトが静的に安全であっても、コントラクトが動的で不変になるように設計されていない限り、動的攻撃に対して脆弱です。イントラモは、機械学習技術を使用して、このような攻撃から契約を保護します。これらのテクノロジーには、関係契約トランザクションを識別するための契約セットの関係チェックが含まれます。Intramoは、このような攻撃の異常な名簿を特定するのに役立つ非同期エミュレータも提供しています。

#### ①タイムスタンプ依存関係攻撃

この攻撃の根本的な原因は、鉱夫の過度の注意です。Intramoは、AIを使用してタイムスタンプの依存関係や文字化けした数値の依存関係を動的にチェックし、このような動作を回避します。

#### ②エラー処理の例外と再入性攻撃

これらの攻撃は、基本的にスマートコントラクトへの関数呼び出しによってスローされる例外によって引き起こされます。Intramoは、ディープニューラルネットワークを使用して、そのような脆弱性につながるコーディングパターンを見つけます。

### 3.4 柔軟性の高いブロックチェーンラック

Intramoは、ブロックチェーンの管理と運用において優れた柔軟性を実現することを目指しています。図6は、Intramoのリファレンスアーキテクチャを示しています。点線のボックスに示されているように、Intramoブロックチェーンは6種類のネットワークノードで構成されています。Intramoノード、クラウドアクセスノード、クラウドストレージノード、Intramoトラステッドゲートウェイ、外部データソースストレージノード、AIサービスノード

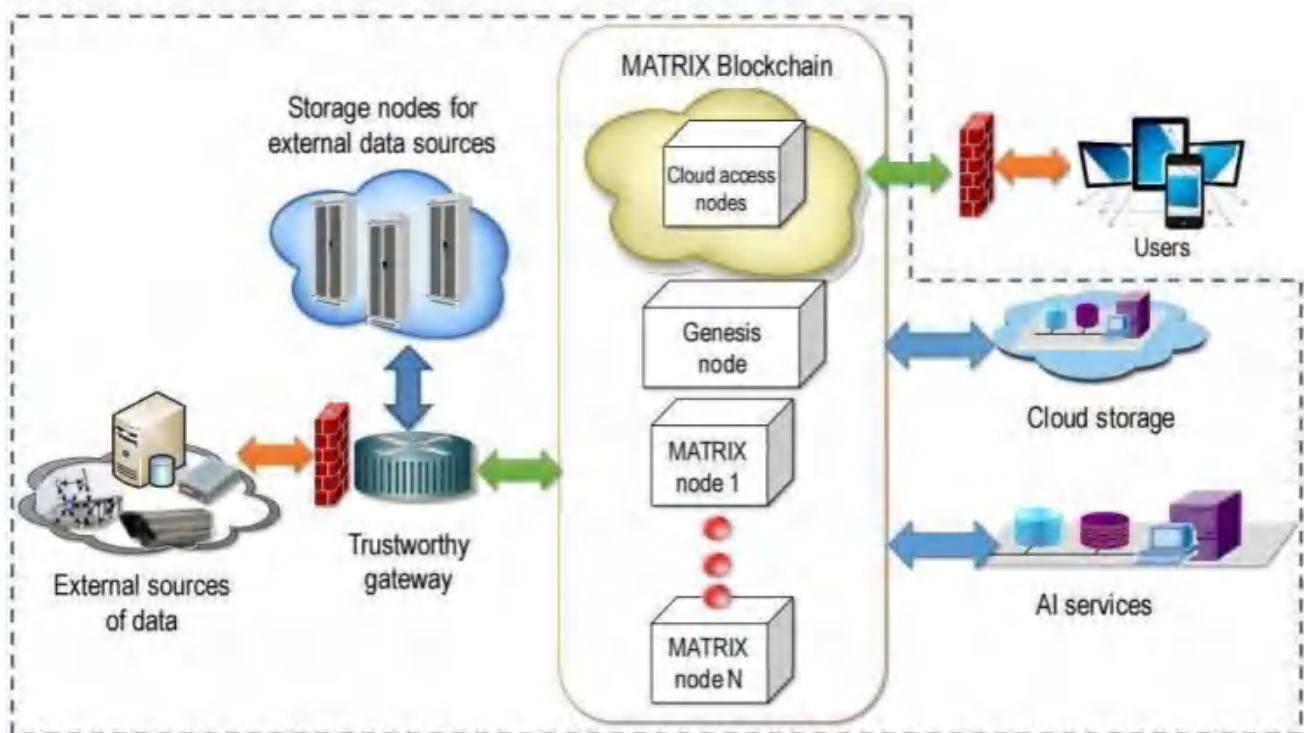


図6： Intramoのシステム構造と導入モデル

分散型協調制御チェーン(以下、制御チェーンと呼びます)は、ブロックチェーンの分散型および分散型の原則に完全に従うように設計されています。

標準Intramoノードは、分散協調制御チェーンと少なくとも1つのデータチェーンを形成します。各ノードには実行が必要です。マシンの計算能力をシミュレートします。分散協調制御チェーン(以下、制御チェーンと呼ぶ)は、標準Intramoノードによって設計され、分散協調制御リンクおよび少なくとも1つのデータチェーンを形成する。各ノードには、仮想マシンを実行するためのコンピューティング能力が必要です。

クラウドアクセスノードは、Intramoのクラウドサービスへのモバイルデバイスアクセスを容易にするように設計されており、Intramoに接続されているすべてのデバイスが十分なコンピューティングパワーを持つことができます。イントラモブロックチェーンからのブロックデータは、リアルタイムでクラウドストレージノードにコピーされます。クラウドストレージはコンセンサスのためではなく、ユーザーがオフラインでデータを簡単に表示できるようにするためです。ユーザーは、検証、データマイニング、およびその他の目的でトランザクションレコードを取得できます。

・intramo トラストド・ゲートウェイは、外部データ・ソースと通信するための重要なインターフェースです。デバイスは、Intramoが要求するすべての外部データソースを取得し、その信頼性を判断します。このデータを使用する場合、intramo ノードはデータの整合性をチェックして、各データソースの信頼レベルと各外部ノードの信用格付けを決定します。

・Intramoの信頼済みゲートウェイも P2P トポロジで編成されています。Intramoを介して確実に取得されたデータプール内の外部ソースからのストレージノードゲートウェイ。データは、チェックインする前に AI ベースの検証プロセスに合格する必要があります。プールにはユーザーの個人データも保存されますが、このデータは暗号化され、許可されたユーザーのみがアクセスできるようになります。プール内のすべてのデータは、その内容にアクセスしてテンパリングされていることを証明することなく、署名をチェックすることで検証できます。AIサービスノードには、システム全体の最適化を支援する機能と、Intramo上で様々な人工知能サービスを開始する機能の2つがあります。

Intramoをサービスプロバイダーとして起動して外部ユーザーにサービスを提供することも、内部ユーザーにサービスを提供するようにIntramoノードをスケジュールすることもできます。AIサービスノードは、接続されたハードウェアに依存してコンピューティング能力を提供します。

#### ・3.4.1 Intramoのマルチチェーン構造

パブリックチェーンとプライベートチェーンを同じプラットフォームで運営する必要性が強いIntramoは、マルチチェーン統合をサポートするブロックチェーンです。これにより、完全にパブリックなパブリックチェーンと、複数の安全なアクセスおよび制御メカニズムと調整されたプライベートチェーンの統合と相互運用性が可能になります。図7は、Intramoの技術を搭載したマルチチェーンプラットフォームを示しています。これは、制御チェーンと複数のデータチェーンで構成されています。

Intramoのパブリックチェーンとプライベートチェーンのサポートは、主に制御チェーンを通じて実装され、指定されたアクセス制御とセキュリティメカニズムを実現します。制御チェーンは、アクセス制御、データ・ストレージ・セキュリティ、およびマルチユーザー・セキュリティの制御ブロックで構成されます。各データチェーンブロックのデコードパイプラインとそのパラメータ割り当ては、制御ブロックの割り当てによって決まります。P2Pネットワークのプロビジョニングパラメータを定義する制御ブロックもあります。制御チェーンのおかげで、Intramoはブロックストレージキー、ノードセキュリティキー、およびユーザーセキュリティキーで構成される3層のセキュリティメカニズムを採用しています。グループキーとノードキーを使用して送信された情報を暗号化し、プライベートチェーンの形式でセキュリティキーの配布、管理、および安全な認証をサポートします。



複数の相互運用可能なチェーンを統合するというアイデアにより、Intramoは実世界規模のビジネスアプリケーションをサポートする自由度が大幅に向上します。たとえば、ビットコイン対応データチェーンとイーサリアムデータチェーンを持つことが可能になりました。2つのチェーンは、Intramoの安全なスマートコントラクトを通じてデータとトークンを交換できます。

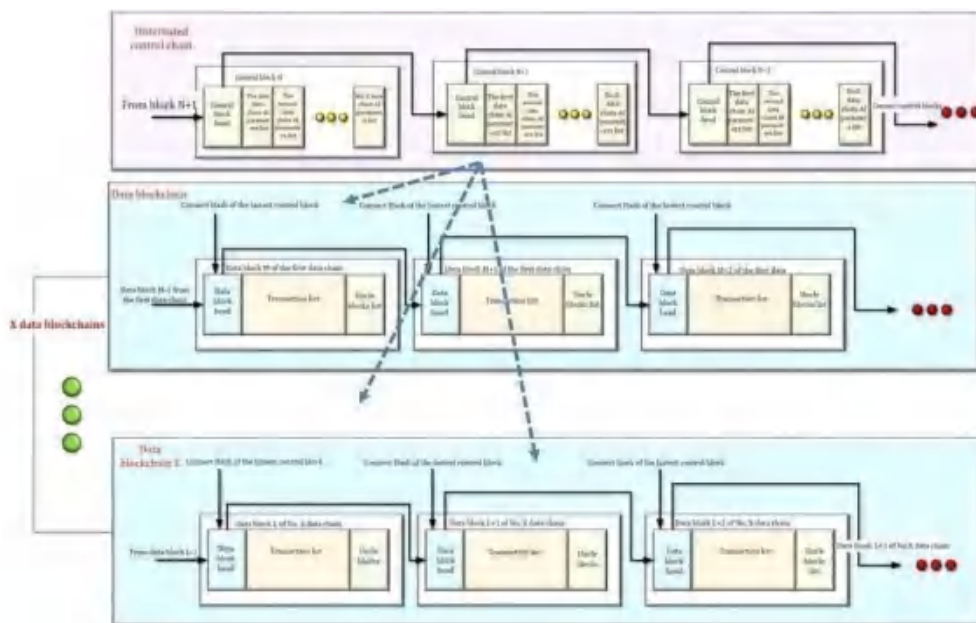


図7： Intramoのマルチチェーン構造

### 3.3.2 ブロックチェーンパラメータの自然な進化

ブロックチェーンには通常、ブロックサイズ、許可計算、コンセンサスメカニズム、マイニング計算など、多くのパラメータがあります。これらのパラメータの割り当ては、ブロックチェーンの全体的なパフォーマンスに大きな影響を与えます。多くの場合、すべてのケースに最適なパラメータセットを選択することは不可能です。ただし、これらのパラメータの大幅な変更は、暗号通貨のハードフォークに重大なリスクをもたらします。マルチチェーン統合の導入は、異なるチェーンのコンセンサスメカニズムやその他のパラメータが大きく異なる可能性があるため、問題を複雑にします。強化学習ベースのパラメータ最適化エンジンは、Intramoブロックチェーンに組み込まれています。いわゆるバリューネットワークは、さまざまなパラメータの長期的なリターンを微調整することを継続的に学習します。学習後、ネットワークは、特定のブロックチェーンの現在の構造とコンテキストで最適なパラメータ調整の決定を生成できます。図8は、イントラモの自然な進化を示しています。イントラモチェーンは自己最適化を学習するため、プロセス全体が自然進化として指定されます。

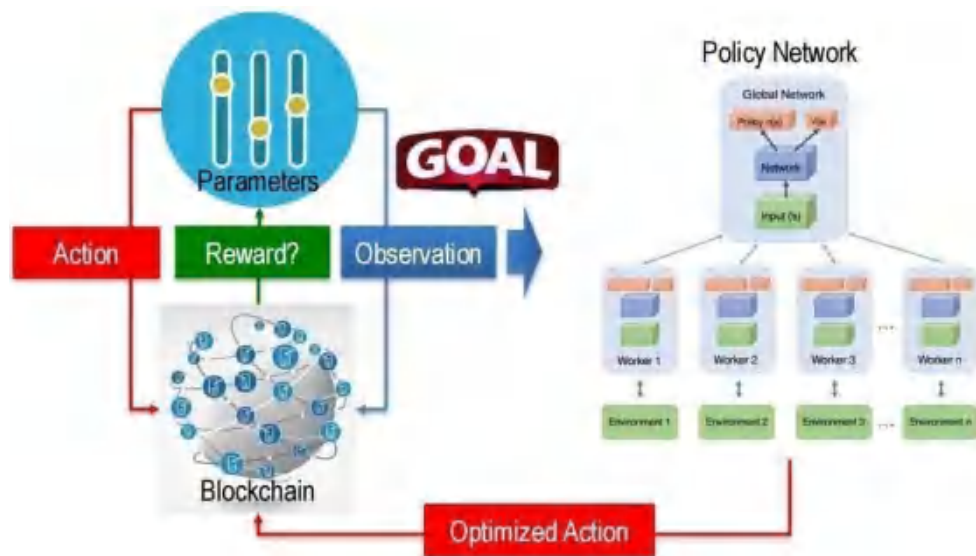


図8： Intramoのマルチチェーン構造

### 3.5 マルコフ連鎖モンテカルロ計算の証明

Intramoは、ハイブリッドPoS + PoWコンセンサスメカニズムを採用し、従来のハッシュコンピューティングに代わる付加価値コンピューティングの導入に革命をもたらしました。アイデアは、マルコフ連鎖モンテカルロ (MCMC) 計算をプルーフオブワークとして使用することです。MCMCは、個別化医療、財務モデリング、人間の認知モデリング、ソーシャルネットワーク分析などの科学および工学アプリケーションで幅広いアプリケーションを提供しています。そのため、マイニングプロセスは実際のアプリケーションで使用でき、付加価値を生み出すことができます。実際、MCMCベースのマイニングは、仮想世界と物理世界の資産間のより強力な架け橋を提供すると信じています。

MCMCはマルコフ連鎖を構築し、ターゲット確率密度からサンプルを選択します。20世紀に発明された最も影響力のある算術の1つとして、実世界のデータを使用したベイズ推論への道を開きました。図9の上半分は、事後分布(すなわち、与えられた観測データの仮想分布)をサンプリングするためのよく知られた微分メトロポリスヘイスティングス(MH)計算の擬似コードを示しています。MCMCには、マイニングワークロードとしての使用に適した一連の基本特性があります。まず、計算負荷が高くなります。複雑な分布の収束には、数千万のサンプルが必要になる場合があります。構造学習の問題では、多数のグラフトポロジーのサンプリングが必要であり、数日かかる場合があります。

スーパーコンピューターでも行われます。第二に、収束後のサンプルの分布は先験的に未知です。このような機能により、最終結果を改ざんして不正行為を行うことが非常に困難になります。第三に、最終結果は不明であるが、最終収束への近接度を評価することが可能である。図9の下半分は、サンプリング・トレースを示しています。図9の影付きのリングは、ターゲットの事後分布を表しています。

### Metropolis-Hastings MCMC

Starting with  $\mathbf{X}^{(0)} := (X_1^{(0)}, \dots, X_p^{(0)})$  iterate for  $t = 1, 2, \dots$

1. Draw  $\mathbf{X} \sim q(\cdot | \mathbf{X}^{(t-1)})$ .
2. Compute
 
$$\alpha(\mathbf{X} | \mathbf{X}^{(t-1)}) = \min \left\{ 1, \frac{f(\mathbf{X}) \cdot q(\mathbf{X}^{(t-1)} | \mathbf{X})}{f(\mathbf{X}^{(t-1)}) \cdot q(\mathbf{X} | \mathbf{X}^{(t-1)})} \right\}.$$
3. With probability  $\alpha(\mathbf{X} | \mathbf{X}^{(t-1)})$  set  $\mathbf{X}^{(t)} = \mathbf{X}$ , otherwise set  $\mathbf{X}^{(t)} = \mathbf{X}^{(t-1)}$ .

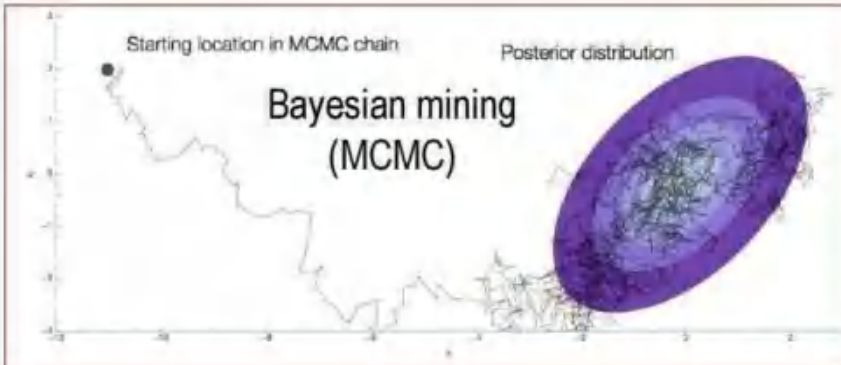


図9：マルコフ連鎖モンテカルロ計算

MCMC コンピューティング モードは、CPU または GPU に対応していません。 実際、MCMC には、乱数生成やサンプリング確率分布など、さまざまな確率計算が含まれます。 現在のコンピューターはこの種の計算をサポートしていないため、多くのオーバーヘッドが発生します。 以前の作品では、効率的なMCMCコンピューティングのためのベイジアンコンピューティングアーキテクチャを開発しました。 全体的なハードウェア アーキテクチャを図 10 に示します。 多重化をサポートするために、複数のランダムマルチプロセッサに編成されています。 1つ以上のランダムマルチプロセッサを割り当てて、ベイズ推論の単一のタスクを実行できます。 ランダムマルチプロセッサには、8つのサンプリングユニットのセットが装備されています。 これらのサンプリング ユニットのセットは、SIMD チャンネルで呼び出すことができることに注意してください。 サンプリング部は、乱数バッファと、所定の共通分布セット（一様分布や二項分布など）のランダムサンプルをプロットするランダム論理回路で構成されています。 商用IPハートは、実数乱数を生成するために使用されます。 A. 所定の MCMC プログラムに基づいて、プログラマブル コントローラは並列サンプリングを調整するように設計されています。

このアーキテクチャには、サンプルメモリが内蔵されており、実際にはサンプル操作を操作するためのハイブリッドコンピューティング/メモリモジュールです。各ランダムマルチプロセッサには、共通データに高速にアクセスするための一時メモリもあります。上記のアーキテクチャは、マイニングハードウェアのプロトタイプとして使用され、アプリケーション固有の集積回路として実装できます。

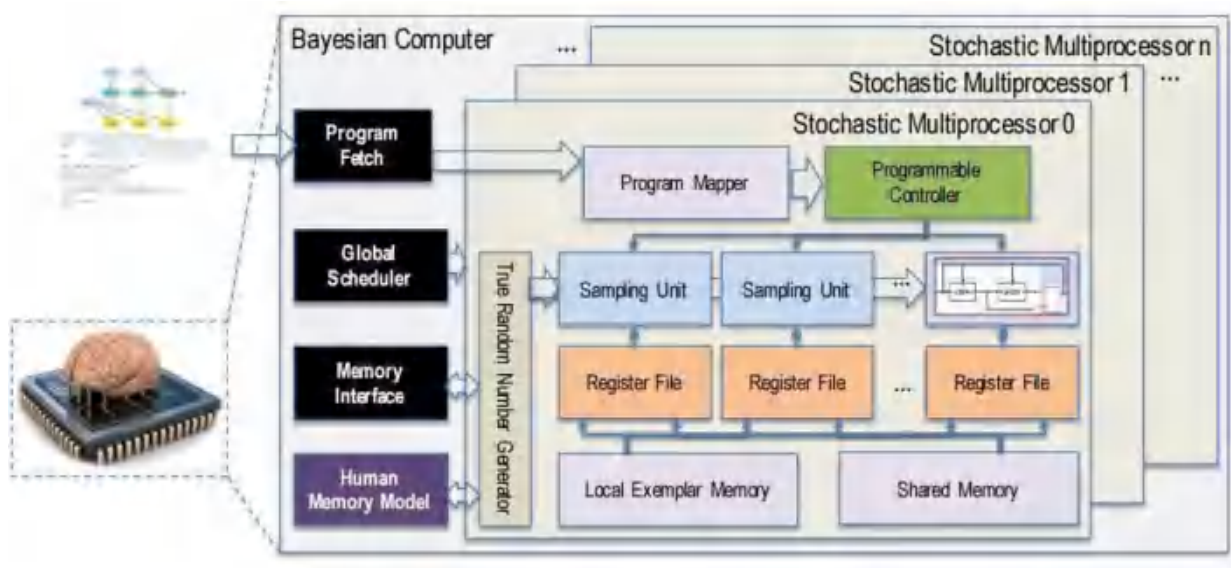


図10：マルコフ連鎖モンテカルロコンピューティングのためのハードウェア

## 四、Intramoの経済学

### 4.1 発行メカニズム

プロジェクト名：Intramo

トークン名：INTO

発行総額：1.5億枚

### 4.2 トークンの配布

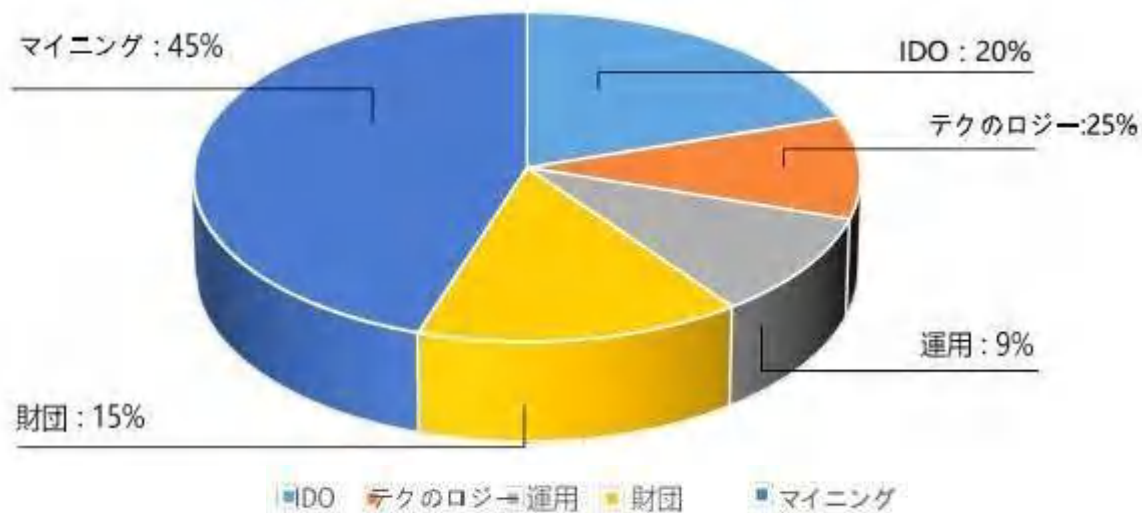
IDO：20%（すべて市場IDOによって生産され、ロックアップはなく、すべてオンラインになる前にリリースされました）

テクノロジー：10%（4年間ロックアップし、その後、完全に解放されるまで毎年2%が解放されます）

操作：10%（財団による監査と不定期の配布を行い、具体的なリリース率はコミュニティで発表されます）

財団：15%（ポジションを3年間ロックアップし、四半期ごとに1%をリリースし、主に広報処理と、プラットフォームに貢献するユーザーと機関への報酬に使用されます）

マイニング：45%（ユーザーデータによるマイニング）



## 五、Intramo結論

Intramoは、古代中国の賢者の精神を体現するために最先端の技術を取り入れています。中国の偉大な哲学者老子はかつて、「成長の鍵は、私たちの意識により高い次元の意識を導入することです」と述べました。「私たちはブロックチェーンと暗号通貨の世界に人工知能をもたらしています。ブロックチェーン技術はすでに世界を1つにつなぐため、IntramoのAIスマートブロックチェーンは、過去を理解し、未来を予測する比類のない能力を提供します。

## 六、免責事項

### 6.1 免責事項

このホワイトペーパーは情報提供のみを目的としており、上記の情報または分析は投資決定を構成するものではなく、このファイルは投資アドバイス、投資意図、または投資勧誘を構成するものではありません。本ホワイトペーパーは、いかなる種類の有価証券の売買の申し出、または売買の勧誘を構成するものではなく、またそのように解釈されるべきでもなく、いかなる種類の契約またはコミットメントでもなく、Intramoは、INTOおよびその他の暗号通貨およびブロックチェーンシステムの開発、保守、運用には多くのリスクが伴い、その多くは財団の管理が及ばないと考えています。このホワイトペーパーに記載されている他の内容に加えて、各INTO購入者は、以下に説明するリスクを熟読し、理解し、慎重に検討する必要があります。投資家はINTOトークンのリスクを明確に理解する必要があり、投資に参加すると、プロジェクトのリスクを理解して受け入れ、対応するすべての結果または結果を個人的に負担する用意があります。ユナイテッドメディカルチェーンチームは、ユナイテッドメディカルチェーンプロジェクトへの参加によって引き起こされた直接的または間接的な資産損失を負担しないものとします。INTOの各購入者は、Intramoがオンライン仮想空間にのみ存在し、具体的な存在を持たず、特定の国に属さない、または特定の国に関係していないという事実に特別な注意を払う必要があります。

### 6.2 リスク警告

INTO (デジタル資産交換機) の購入に参加するには、イントラモのホワイトペーパーを注意深く読み、イントラモの技術的特徴、グリーンシードのリスクリターン特性を十分に理解し、イントラモプログラムはいかなる状況においても交換されたデジタル資産のリターンまたは現金を提供しないことを理解してください。Intramoチームは、ホワイトペーパーで開示されているように、トークンによって調達されたデジタル資産を合理的に利用し、定期的の開示します。イントラモチームの献身、勤勉さ、コンプライアンスにもかかわらず、潜在的な政策リスク、景気循環リスク、流動性リスク、情報セキュリティリスク、公共福祉チェーン変動リスクなど、購入者にとって損失のリスクは依然としてあります。買い手は、自らのリスクテイク能力を十分に考慮し、合理的な判断を下し、慎重な判断を下す必要があります。