

修士論文

IoT 環境における分散台帳技術の性能分析

指導教官 林 冬恵

京都大学大学院情報学研究科
社会情報学専攻

渡辺隆弘

2018 年 12 月 18 日

IoT 環境における分散台帳技術の性能分析

渡辺隆弘

内容梗概

概要

目次

1	はじめに	3
2	背景	5
2.1	Internet of Things	5
2.1.1	IoT 環境において求められる要件	6
2.2	分散台帳技術	7
2.2.1	Blockchain	8
2.2.2	Ethereum	11
2.2.3	IOTA	12
2.3	IoT 環境における分散台帳技術	14
3	定性的な指標	16
4	定量的な指標	19
4.1	速度	19
4.1.1	ノード間遅延	19
4.1.2	承認時間	19
4.2	コスト	19
4.3	スケーラビリティ	20
4.3.1	キャパシティ	20
4.3.2	ノード規模耐性	20
4.3.3	処理達成率	20
5	定量的な分析	21
5.1	シミュレータの設計	21
5.2	分析	21

6 考察	22
7 まとめ	23

第 1 章 はじめに

近年、「いつでも、どこでも、何でも、誰でも」ネットワークに繋がる「ユビキタスネットワーク社会」が構想されてきた。接続機器として代表的なものとして、従来はパソコンやスマートフォンが挙げられるが、センサーデバイスの普及に伴い、車や家電といった物理機器、建物もネットワークに接続されるようになった。このように様々なデバイスがネットワークに接続されるようになると、それらのデバイス間での情報交換やデータの収集、それに基づく自動化が行われ、新たな付加価値を生むようになる。このような仕組みは Internet of Things(IoT) と呼ばれる仕組みであり、急速に発展している [Atzori et al., 2010][Gubbi et al., 2013a].

IoT は医療、スマートホーム、運送など幅広い分野での適用が検討されているが、収集、処理するデータの増加に伴い、深刻なセキュリティ、プライバシーの問題を引き起こすことが指摘されている [Dorri et al., 2017a]. この問題を解決するために Blockchain(BC) を採用することが検討されている。BC は Bitcoin[Nakamoto, 2008] の中核を為す分散台帳技術のことである。BC はセキュアな取引を保証するが、IoT 分野に適用するにあたり以下のような問題点が存在する。

- 取引の合意形成のアルゴリズムに基づく高いリソース要件
- ブロックサイズに基づくスケーラビリティの悪さ
- 合意形成、および二重支払いを防ぐためのアルゴリズムに基づく遅延

これらは IoT 環境が、現在 BC が利用されている分野とは異なる特性を持つ環境であるためである。IoT 環境に用いられるシステムは、膨大なデータ量やネットワークノード数に対応するスケーラビリティ、プライバシー保護のためのセキュリティ、障害耐性、処理のリアルタイム性などが求められる。そこで、上記の問題を解決するために IoT 環境に適用する目的の分散台帳技術の研究が行われている。スマートホームを題材とし、BC をベースとした新しいアーキテクチャを構成した研究 [Dorri et al., 2017a] では、BC を用いた場合と比べ、パケットと処理のオーバーヘッドを大幅に短縮する

ことを実証している。また、他の例には、BC をベースとしない、有向非循環グラフ (DAG) を用いた Tangle と呼ばれるグラフ構造に基づく IOTA という新たな分散台帳技術を開発し、取引の速度、規模のシミュレーションを行う研究 [Popov, 2016][Kusmierz, 2017] が挙げられる。

IoT 環境を想定した分散台帳技術について研究が行われる一方で、それらの技術を評価する明確な指標は存在しない。BC の性能を評価する研究 [Croman et al., 2016] などは存在するものの、IoT 環境を想定した際にこれらの評価軸を用いることが適切であるとは言えない。本研究は、既存の種々の分散台帳技術を IoT 環境に適用する際、どのような評価指標を用いることが適切であるか議論を行い、その指標に基づき複数の分散台帳技術の性能比較を行う。

本研究の貢献は以下の通りと考える。

- IoT 環境における分散台帳技術の評価指標を提案する。
- 提案した評価指標に基づき既存の分散台帳を評価し、IoT 分野に適用することが適切であるとされる技術の特徴を提示する。

本稿の構成は以下の通りである。第 2 節では、IoT の概略および BC などの既存の分散台帳技術の紹介を行う。第 3 節では、評価指標を提示し、その妥当性についての議論を行う。第 4 節では、定量的な指標を提示する。第 5 節では、4 節で提示した指標に関して分析を行い、その結果を示す。第 6 節では得られた結果から、IoT 環境における分散台帳技術の適用可能性や技術特性などについて議論する。

第 2 章 背景

本章では，IoT についての導入と，本研究で題材とする分散台帳技術についての説明を行う．その後，IoT に分散台帳技術を適用する研究の外観と，その重要性について述べる．

2.1 Internet of Things

Internet of Things(IoT) とは，様々な物理機器などにセンサーやソフトウェアを組み込むことで，情報交換やデータの収集を行えるネットワークを構築する仕組みである．[Vermesan et al., 2009] では，アイデンティティ，物理的属性，および仮想パーソナリティ，知的インターフェースを使用し、情報ネットワークにシームレスに統合されている物理的，もしくは仮想的な”モノ”に存在する標準および相互運用可能な通信プロトコルに基づく，自己構成能力を備えた動的なグローバルネットワークインフラストラクチャとして定義されている．

IoT は、物理的な世界と仮想的な世界を橋渡しすることで，スマートな都市，スマートな工場，資源管理、交通機関、健康、福利厚生など、多くのアプリケーション分野に影響を与える．しかし、ソフトウェアアプリケーションの中で IoT を活用することは、ネットワーキングからアプリケーション層まで，特に超大規模，極端な異質性，IoT の動的性などの大きな課題を抱えていることが指摘されている [Bouloukakis et al., 2016]．また，世界中において配備されているセンサーの数は急速に増加しており，加速度的に増大していくとされる．相互に接続されたデバイスの数は 2013 年の時点で 90 億個であり，2020 年には 240 億個に到達するとみられている [Gubbi et al., 2013b]．これらのセンサーは膨大な量のデータを生成しつづけるが，セキュリティ面に対して十分な対策はなされていない．現在の IoT において，セキュリティとプライバシーを提供する方法を提案するにあたり，3 つ課題が存在すると Dorri ら [Dorri et al., 2017a] は指摘している．1 つ目はリソースの面である．IoT のネットワークにおいてデータを収集するセンサーなどの末端のデバイスは，高度で複雑なセキュリティメソッドを備えていないという問題

がある。2つ目は、プライバシーの問題である。IoTにおいて収集されるデータは個人が特定されるようなデータが含まれることが想定される。種々のデータを収集しながらユーザーのプライバシーを保護しなければならない。3つ目は中央化である。クライアントサーバモデルをはじめとする中央集権的なモデルはIoTには不適切であることが多いと指摘されている。中央集権型のモデルを適用した際、単一障害点、多対一トラフィック、スケーラビリティなどの問題を抱えるとされる。

2.1.1 IoT 環境において求められる要件

IoT 環境のシステムに求められる要件は次のようなものが挙げられる。

- ・ 膨大なデータとノードの増加に対応するスケーラビリティ
- ・ プライバシー保護の観点でのセキュリティ
- ・ サイバー攻撃に対し強いこと
- ・ リアルタイムな処理

2.1 節で述べたように、センサーによって収集されるデータ量は膨大なものになる。また、ネットワークに接続されるセンサーの数や種類が急速に増加していくことが考えられるため、拡張性に富む設計であり、大量のデータを問題なく処理することができるスケーラビリティを有することが求められる。

IoTにおいて収集するデータは、工場内のデータや住居内のデータ、個人の身体情報などの機密性が高い情報も含まれる。情報を収集しつつ、これらのプライバシーを保護することのできるシステムが必要である。

また IoT は、都市インフラ、交通などシステムの安定性が求められる分野に利用されることが検討されている。サイバー攻撃や、サーバートラブルに対し強いシステムであることが求められる。

一方、既存のクライアント・サーバモデルでは、中央のサーバの処理速度が全体のボトルネックになることや、中央のサーバがトラブル、攻撃などの被害にあった際にシステムが停止してしまうことといった問題点が指摘されている。

これらを解決するために、中央集権型のシステムではなく、分散データベースを用いることが提案されてきた。分散台帳技術は、既存の IoT 環境のシステムに比べ、セキュリティの面や、攻撃やトラブルに対する耐性に優れる。一方で、現在実用されているブロックチェーンなどの分散型アーキテクチャは処理に時間がかかること、トランザクションの処理速度が遅いこと、トランザクションあたりの手数料が大きいことなどの理由からこれらを直接 IoT 環境に適用することは困難だとされている。

2.2 分散台帳技術

分散台帳技術 (Distributed Ledger Technology) はデータを中央で管理するのではなく、分散させ管理するデータベースであり、複数の端末が同じ情報を保持することで改竄や攻撃への耐性を高め、管理者が存在せずに信頼性を確保するものである。

分散台帳技術のうち代表的であるブロックチェーンは、取引の記録を分散させ、ネットワークの参加者に相互に確認させることで、取引の整合性を高めている。

分散台帳技術のメリットは、不正取引や改ざんが非常に困難である点、またシステムダウンに強い点である。従来の中央集権型のシステムは、管理者が存在し、管理者側に悪意のある人間が存在した場合に不正な取引や改ざんが行われる可能性があるために、管理者の信頼性というものが必要があるが、管理者が信頼できるかどうかユーザーが判断することは困難である。一方で分散台帳技術においては、管理者が存在しないため、管理方式に対してユーザーが安心しやすい。また、中央集権型のシステムの場合、管理者側のサーバーやコンピュータにトラブルが生じた際システムを稼働できない状態に陥る危険性があるが、分散型のシステムの場合は、一部のノードにトラブルが生じていてもシステムを稼働し続けることができる。

どのような目的、分野で活用されているか、どのような問題を解決するために生まれた技術か？Blockchain in government: Benefits and implications of distributed ledger technology for information sharing を参考にする。

本研究において分析対象とするいくつかの分散台帳技術を紹介する。

2.2.1 Blockchain

Blockchain(BC) は Bitcoin[Nakamoto, 2008] の中核を為す分散台帳技術である。ブロックと呼ばれるトランザクション (TX) の集合を一定時間おきに生成し、それを鎖のように連結させていくことでデータを保管するデータベースである。右に行くほど新しいブロックであり、鎖状に連結される。トランザクションと呼ばれるユーザ間での取引は 10 分おきにブロックという単位にまとめられ、台帳の最新のブロックの直後に連結される。台帳にブロックを追加するためには Proof of Work(PoW) と呼ばれる作業が必要となる。この作業は多くの計算資源を要求するため、データを保証する根拠となる。PoW を行い、ブロックを追加することができたユーザには報酬が与えられ、この一連の作業はマイニングと呼ばれる。BC の各ブロックは、直前のブロックの内容のハッシュ値と、取引データを含んでいる。そのため、台帳の一部を改竄するには、その後のブロックの内容を全て書き換える必要があり、BC の改竄は実質的に不可能とされている。

Bitcoin のシステムを例として、BC において利用される用語について説明する。

トランザクション トランザクションとは、ブロックチェーンにおける取引記録のことである。トランザクションには、タイムスタンプと、インプット、アウトプットが含まれており、Bitcoin のシステムにおいては、あるユーザーが別のユーザーへ送金したコインの額と、その時間が記録されている。BC 内のトランザクションのアウトプットには、未使用状態の UTXO(Unspent Transaction Output) と呼ばれるアウトプットと、使用済みのアウトプットの 2 種類の状態がある。

ブロック ブロックは、一定時間のうちに生成されたトランザクションの集合からなるデータである。1 つのブロックにはその親のブロックのハッシュ値が含まれており、ブロックを鎖状に繋げてデータを保存していく形式から Blockchain と名付けられている。最初のブロックからあるブロックまでの距離を表現するのに「高さ」、新しく追加された最後のブロックを「トップ」または「先端」と表現する。ブロックチェーンの

ブロックは、自身のヘッダの「previous block hash」のフィールドを通して1つ前のブロックを参照しており、参照されているブロックを親ブロックと呼ぶ。親ブロックのハッシュ値を自身のヘッダに持っており、このハッシュ値の連なりを辿っていくと、最終的には genesis ブロックと呼ばれる最初に生成されたブロックに達する、ブロックの構造は以下表2.1のようになっている。

サイズ	フィールド名	内容
4 バイト	ブロックサイズ	次のフィールドからブロックの最後までデータサイズ
80 バイト	ブロックヘッダ	ブロックヘッダ
1~9 バイト	トランザクションカウンタ	ブロックのトランザクション数
可変サイズ	トランザクション	ブロックに記録されるトランザクションのリスト

表 2.1: ブロック構造

マイニング マイニングとは、BC において新たなブロックを生成するための行程である。BC のネットワークに参加しているノードはこの作業を行い、マイニングに最初に成功したものがブロックチェーンにブロックを追加することができ、トランザクションを発行する際の手数料を報酬として得ることができる。Bitcoin においてマイニングは 10 分間に 1 度行われる。マイニングは、ブロックヘッダの中のナンス値と呼ばれる値について、ブロックのハッシュ値がある値よりも小さくなるような適切なナンス値を見つけるもので、適切なナンス値の条件を変動させることで、マイニングにかかる時間を一定に保っている。この適切なナンス値を見つける計算は Proof of Work(PoW) と呼ばれる。チェーン中のブロック内のトランザクションの一部を改ざんしようとした際、そのブロックのナンス値を再計算しなくてはならないばかりではなく、そのブロック以降の全てのブロックに対して同様の計算をしなくてはならないため、ブロックの改ざんは不可能に近いとされる。

BC を用いたシステムの挙動を Bitcoin のシステムを例にして順を追って説明する。

1. トランザクションの発行... ビットコインを 1 つ以上のソースアカウントから 1 つ以上の宛先アカウントに転送することでトランザクション

が作成される。送金者は、データ構造としてのトランザクションを作成し、インターネット経由で、Bitcoin ネットワークに接続されている全てのノードに送信する。送金者は、マイニングを行う際に自分のトランザクションをブロックに取り込んでもらうために、手数料を支払う必要がある。この場合、インプットの総額とアウトプットの総額の差額が手数料となる。

2. トランザクションの伝搬... 発行されたトランザクションは、ネットワークのノードからノードへと回送されることでネットワークの隅々までデータとして届けられる。トランザクションは、そのトランザクションを受け取ったノードで内容の生合成の検証をされ、内容が不整合であれば、他のノードへの回送は行われない。
3. 検証... ブロックの作成を行う主体のことをマイナーと呼ぶ。マイナーは自身が受け取ったトランザクションをメモリープールと呼ばれる領域に格納し、マイニングに成功すると、メモリープールの中のトランザクションをブロックに格納していく。Bitcoin において、ブロックサイズの上限は 1MB であり、この上限までしかトランザクションは格納することができない。
4. ブロックの追加... 計算の競争に勝利したマイナーは新しいブロックを作成することができ、この新しいブロックはネットワークにブロードキャストされる。各ノードは、送信されてきたブロックの内容をそれぞれ検証し、問題がない場合自身のノード内の BC に接続する。新しいブロックが Bitcoin ネットワークの全てのノードにおいて BC に接続されると、ブロック内の全トランザクションも非可逆な記録として定着する。ブロードキャストされたトランザクションの伝播には大きなレイテンシが存在する。また、世界中にマイナーは点在しているため、ブロックがほぼ同時に生成されたり、ブロック内のトランザクションもマイナーごとに異なる可能性がある。あるトランザクションがブロックに取り込まれてから最新のブロックが接続されるまでのブロックの数である確認数が 6、つまりあるトランザクションが格納されているブロックに 6 つ新しいブロックが接続されるとトランザクションは非可逆であるとみなされる。

2.2.2 Ethereum

Ethereum¹は次世代のスマートコントラクトと非中央集権型アプリケーションのプラットフォームと表現されている，独自 BC 上でアプリケーションを配置し，実行できるプラットフォームである．Ethereum はスマートコントラクトを記述する Solidity という言語に代表されるチューリング完全なプログラミング言語を持ち，ユーザは Ethereum 上の BC に任意の分散型アプリケーションやスマートコントラクトを記述し実行することが可能である．

スマートコントラクト スマートコントラクトは，1994 年に Nick Szabo により「契約を実行するコンピュータ化されたトランザクションプロトコル」として定義された [Szabo, 1994]．また，担保，譲渡といった契約条項をコードに翻訳し，自己執行可能なハードウェア，あるいはソフトウェアにそれらを埋め込むことを提案した [Szabo, 1997]．これにより，仲介者の必要性を最小限に抑え，信頼性のある取引が可能となる．ブロックチェーン上のスマートコントラクトでは，契約をプログラムで定義し，条件に合致した際には仮想通貨などのデジタル情報で取引を行い，契約が正当に履行されたかの確認も自動化して実行する．決済や権利の取引の自動化にスマートコントラクトを活用できれば，これらの取引のプロセスを P2P で実行でき，仲介者が不要となるため，自律的で透明性の高い取引が行うことが可能となると期待されている．ブロックチェーンを利用したスマートコントラクトは，過去の実行履歴がブロックチェーン上に記載されるため，取引の改ざんを防ぐことが可能である．金融・証券や，生活・産業など契約と密接に関連する業務への適用が検討されている．

Ethereum で使う通貨は「Ether(イーサ)」と呼ばれる．Ethereum での送金，コントラクトの実行には「Gas(ガス)」と呼ばれる手数料が必要となる．また，Ethereum はコンセンサスアルゴリズムとして Bitcoin と同じ PoW を用いている．Bitcoin では最も長いブロックチェーンを有効なチェーンとみなすのにたいし，Ethereum では最も多く計算量が投下されているブロックチェーンを有効なチェーンとする GHOST(Greedy Heaviest Observed Subtree) プ

¹<https://www.ethereum.org/>

ロトコルが採用されている。これは、Bitcoin のブロック生成時間が 10 分間なのに対し、Ethereum のブロック生成時間は 15 秒と短く、チェーンのフォークが頻繁に起こるためである。

Ethereum のコンセンサスアルゴリズムは、Proof of Stakes(PoS) にアップデートされることが計画されている。PoS においてブロック生成に参加している人々はバリデーターと呼ばれる。バリデーターがステイクしている通貨の量に応じて、ブロックごとに抽選でブロックを生成する権利が与えられ、ブロックを生成したバリデーターに生成報酬が与えられる。

ブロックガスリミット Ethereum の特徴として、Bitcoin のようにブロックサイズの上限が明確に定められていないことがある。マイナーはブロックガスリミットと呼ばれる値を、投票によってマイブロックごとに変動させることができ、この概念が Bitcoin におけるブロックサイズに似た役割を果たしている。Ethereum ではトランザクションの処理を行うために Gas を支払うが、1 ブロックに取り込むことのできる Gas の上限がブロックガスリミットである。

2.2.3 IOTA

IOTA²は M2M マイクロペイメントのために開発された仮想通貨の基盤となる分散台帳技術である。IOTA は BC を IoT に適用する際に課題とされる、スケーラビリティとトランザクションフィーを解決するために開発された。第三者の関与なしに、マシンが相互にサービスを提供し、電気、ストレージ、データといったリソースをトレードすることを想定し、これらのために軽量で、スケーラビリティに富んだ分散台帳が必要であると述べている。ユースケースとして、オランダにおいて IOTA を用いて課金と支払いができる充電スタンドが設置されている。これは自律的に電気自動車の充電を行うための通信や支払いを担い、メーターの値を台帳に保存することで信頼性が高い管理を保証するものである。

IOTA は BC とは異なり、Tangle と呼ばれる分散台帳アーキテクチャを用いている。Tangle は有向非循環グラフ (Directed Acyclic Graph) に基づいており、BC のようなブロックの概念は存在しない。IOTA において、ネットワークの参加者は BC と異なり、台帳に任意のタイミングでトランザク

²<https://www.iota.org/>

ションを追加することができる。この際、Tangle に追加されているトランザクション (TX) のうち、2つを選択して PoW を行い、それらのトランザクションの正当性を証明することで、自分のトランザクションをネットワークに追加することが可能になる、図2.1の場合、8 のトランザクションをグラフに追加するために 5, 6 の2つのトランザクションを検証したということを表している。また、単位時間あたりのトランザクションが増加しても未承認のトランザクション（グラフの左端のトランザクション）の数は発散せず一定であり、安定性があるとされている [Kusmierz, 2017].

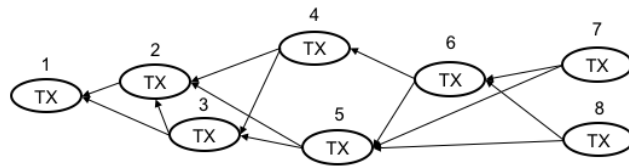


図 2.1: IOTA 概略

Tangle について詳細な説明を与える。Tangle は IOTA に利用されている有向非循環グラフであり、発行されたトランザクションは Tangle 上で集合を形成する。新しいトランザクションが到着すると、前の2つのトランザクションを承認する必要がある。これらの承認は有向エッジによって表される。トランザクション A とトランザクション B の間に有向エッジがなく、A から B までに少なくとも長さ2の有向パスがある場合、A は B を間接的に承認する、と定義されている。ノードはトランザクションを発行するために、以下のことを行う必要がある。

- アルゴリズムに従って、承認する2つの他のトランザクションを選択する。
- ノードは2つのトランザクションが矛盾していないかどうかを確認し、矛盾しているトランザクションは承認しない。
- 承認されたトランザクションのいくつかのデータと鎖状に繋がったナンス値のハッシュがある条件を満たすような、ナンス値を見つける作業を行う。これは Bitcoin の BC で行われる Proof of Work と同様なものである。

Tangle において、トランザクションが承認されるには、「全ての未承認のトランザクションから直接的あるいは間接的に承認される」ことが必要となるが、これは容易に確認することができる。

IOTA は、BC や Ethereum と異なり、ブロックを生成することがなく、トランザクションの発行者自身が PoW を行い報酬として台帳に自身のトランザクションを追加する権利を得る。そのため、トランザクションを発行するために BC や Ethereum では必要となった手数料が必要ではない。このため、1 回あたりの取引の金額が少額になることが想定される IoT 環境において適しているとしている。また、BC や Ethereum のように一定の間隔で承認が行われるのではなく、並列して行われるため、ネットワークに大量のトランザクションが追加されるほどトランザクションは承認されやすくなり、スケーラビリティにも富むとされている。

2.3 IoT 環境における分散台帳技術

IoT 環境では、現在より膨大な量のデータのやりとりが行われるようになる。Croman らは、現在の BC の性能評価を行い、理論的に最大 1 秒あたり 7 トランザクションの処理が可能であるものの、実際の BC における測定では 1 秒あたり 3.3 トランザクション程度の性能であると述べている [Croman et al., 2016]。一方で、現在の VISA の支払いストリームは毎秒平均で 2000 トランザクションの処理が行われており、BC のスケーラビリティとの大きな乖離が指摘されている。また、BC は仕様上、10 分に 1 度まとめてトランザクションの合意を行うため、リアルタイムの処理を行うことはできない。IoT、金融などのシステムではリアルタイムの処理が要求されるため、この点においても現状の BC を転用することは困難であると指摘されている。

また、[Decker and Wattenhofer, 2013] では、台帳を共有するネットワークのメッセージ交換がオーバーヘッドになることを指摘している。各ノードが新規ブロックを受け取るまでの遅延は平均で 12.6 秒であり、ブロックサイズが大きくなればなるほど、遅延時間も比例して大きくなるとしている。

Dorri らは、IoT 環境としてスマートホームの環境を想定し、既存の BC をベースにした新たな軽量なアーキテクチャを提案し、セキュリティ、プライ

バシーに対し BC ベースのアーキテクチャの有効性について分析を行った [Dorri et al., 2017b]. また, パケットオーバーヘッド, 時間オーバーヘッド, エネルギー消費の観点から提案アーキテクチャを評価, 議論した.

詳細化, 実際の IoT 環境の特徴, DLE の特徴を踏まえて

一方で, IoT 環境の分散台帳技術において求められる要件は, 既存の分散台帳技術に求められる要件と重要視される点が必ずしも等しくないと考えられる. 前節で提示した評価指標において, 本研究は IoT 環境における分散台帳技術の評価指標を作成することを考慮すると, 性能効率性, スケーラビリティの 2 点がより重要視されると考えられる. これは, IoT 環境においては Bitcoin などのシステムに比べ即時的な処理が要求されること, ノード数, データ数が非常に膨大になることが想定されるためである.

第3章 定性的な指標

本研究は，IoT 環境に分散台帳技術を適用する際，それらの性能を比較するための適切な評価指標を提示し，既存のアーキテクチャに対し比較を行い，どのようなアーキテクチャが IoT 環境に適しているか考察する．既存研究において，BC の性能評価，IoT への適用可能性や具体的なシナリオにおける評価などは議論されてきたが，IoT 環境に分散台帳技術を適用する際どのような性能評価が必要であるかという点の議論は未だ不十分である．分散台帳技術の評価を行うにあたり，ネットワーク，サービスコンピューティングなどの観点も含め，以下表3.1のような評価項目が考えられる．

一般的な性質の分析は主に，それらの構造的特徴を捉えるものである．シミュレーションによる分析に対し，種々のシステムの差異がアーキテクチャ，アルゴリズムなどのどの要素によって生じ得たものか検討する際に要求されるものである．図3.1の関連技術の項目が各分散台帳技術の性能，特性差を生むものであるため，一般的な性質の分析指標としてこれらの項目を取り上げる．

- ネットワーク環境
- ブロックサイズ
- トランザクションサイズ
- コンセンサス方式
- ブロック生成時間

ネットワーク環境は，具体的にはユーザが自由にネットワークに参加することができるかということを指す．IoT 環境においては，ノード数が増大していくことが考えられるため，管理者によってネットワークへの参加者が制限されるシステムは適さないと考えられる．しかし，管理者がネットワークに参加するユーザを事前に制限することは，PoW を簡素化できるセキュリティを生むために，処理速度を向上させることができるというメリットもある．ブロックサイズは，台帳のブロック 1 つあたりの容量を指す．ブロックサイズが大きくなれば，1 回のブロック生成によって承

大項目	概要	小項目	関連技術
性能効率性	システムの応答時間および処理時間並びにスループット速度が要求事項を満足する度合い	処理性能	ブロックサイズ トランザクションサイズ コンセンサス方式 ブロック生成時間
		ネットワーク性能	ネットワーク環境 ノード分散
		ブロック確定性能	コンセンサス方式 ネットワーク環境
		参照性能	ノード分散 ネットワーク環境 ブロック構造
スケーラビリティ	処理速度を向上させられる度合い，保持するデータ量の増大に対する拡張性の度合い，対応可能ノード数など	スループット向上性	ブロックサイズ トランザクションサイズ コンセンサス方式 ブロック生成時間
		ネットワーク性能向上性	ノード分散 ネットワーク環境 P2P プロトコル
		容量拡張性	ブロックサイズ トランザクションサイズ コンセンサス方式 ブロック生成時間
		ノード数拡張性	データ容量 コンセンサス方式
信頼性	運用操作可能及びアクセス可能な度合い	可用性	単一障害点の有無 コンセンサス方式
セキュリティ	アクセスすることを認められたデータのみアクセスできる度合い	機密性	アクセス管理 データ秘匿化
	行為が引き起こされたことを証明することができる度合い	否認防止性	コンセンサス方式

表 3.1: 評価軸

認されるトランザクションの数が増え，単位時間あたりのトランザクションの処理速度が増大する．一方で，ブロックサイズが増加すればするほど，ブロックがネットワークを伝播する際の遅延は大きくなる．トランザクションサイズは1取引あたりのデータ量を表す．トランザクションサイズが小さくなれば，1ブロックあたりのトランザクション数が増加し，単位時間あたりのトランザクションの処理速度が増大する．一方トランザクションサイズの減少はハッシュ等の簡略化を引き起こし，セキュリティ面での低下をもたらす．コンセンサス方式は，新たなトランザクションを台帳に追加する際にどのような合意形成の方法を取るかを指す．コンセンサス方式によって，合意形成に必要な時間，必要となるリソース，セキュリティなどが変化すると考えられる．ブロック生成時間は，あるブロッ

クが生成されてから次に新たなブロックが生成されるまでに要する時間である。ブロック生成時間が短くなれば、単位時間あたりにより多くのトランザクションを処理することが可能になる。一方で、ブロック生成時間を短くするということは PoW に要する時間を短くすることと同義であり、検証の時間が短くなればなるほどセキュリティの低下を引き起こす。

第 4 章 定量的な指標

本章では，分散台帳技術を評価するための指標のうち，定量的な指標について定義し，詳細に説明する．

4.1 速度

速度 (遅延) は，主に分散台帳技術の処理性能に大きく関わる点である．現状利用されている分散台帳技術を用いたシステムと比較し，IoT 環境ではより高い処理性能が求められるため，遅延やトランザクションの処理にかかる時間は短ければ短いほど良い．

本研究においては以下の 2 点について評価する．

4.1.1 ノード間遅延

ノード間遅延は，あるノードにおいてトランザクションが発行されてからそのトランザクションがネットワーク内の全ノードに伝搬し，全ノードから確認できるようになるまでにかかる時間と定義する．

4.1.2 承認時間

承認時間は，発行されたあるトランザクションが承認されるまでの時間と定義する．IoT 環境においては処理のリアルタイム性が求められる場合もあるため，承認時間が長くなると，システムとして適切ではない．

4.2 コスト

コストは，1 トランザクションを処理するためにどの程度のコストが必要であるかという，Cost Per Confirmed Transaction と定義される．1 トランザクションを処理するためのコストは以下の内訳からなる．

CPCT の話，論文からハードと PoW が大きく関係するということ

4.3 スケーラビリティ

スケーラビリティは処理するデータ量の増大及びネットワークの参加者の増大に対する拡張性の度合いである。生成されるトランザクションのスピードがどの程度であればシステムが正常に動作することができるか、データ量やネットワークの参加者が増大した際にネットワーク遅延がどの程度生じるかという点を指標とすることで、データ及びノードが膨大となる IoT 環境を想定した評価指標になると考える。

4.3.1 キャパシティ

キャパシティは、単位時間あたりに処理できるトランザクション数と定義する。現状、分散台帳技術を用いたシステムは、トランザクション数が大規模になる状況に適していない。あるシステムのキャパシティが大きければ大きいほど、トランザクション数が膨大になることが想定される IoT 環境において利用するシステムとして適切であると考えられる。

4.3.2 ノード規模耐性

ノード規模耐性は、ノードの規模が増大することに対してシステムの承認時間やキャパシティがどのように変動するかというものである。

4.3.3 処理達成率

処理達成率は、ある時点までに発行された全トランザクションのうち、どの程度の割合のトランザクションが承認されているかということを示すものである。ノード規模、秒間に発行されるトランザクションの数が増大しても、処理達成率に大きな変化が起きないシステムは、スケーラビリティがあると考えられる。

第 5 章 定量的な分析

本章では，4 章で提案した評価指標に基づき，既存の分散台帳技術の性能比較を行う．評価対象として，2 章で紹介した，Blockchain, Ethereum, IOTA の 3 つのシステムを用いる．

5.1 シミュレータの設計

5.2 分析

第 6 章 考察

第 7 章 まとめ

文献データベース

- [Atzori et al., 2010] Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805.
- [Bouloukakis et al., 2016] Bouloukakis, G., Georgantas, N., Billet, B., Bouloukakis, G., Georgantas, N., and Revisiting, B. B. (2016). Revisiting Service-oriented Architecture for the IoT : A Middleware Perspective To cite this version : Revisiting Service-oriented Architecture for the IoT : A Middleware Perspective.
- [Croman et al., 2016] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., et al. (2016). On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*, pages 106–125. Springer.
- [Decker and Wattenhofer, 2013] Decker, C. and Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pages 1–10. IEEE.
- [Dorri et al., 2017a] Dorri, A., Kanhere, S. S., and Jurdak, R. (2017a). Towards an optimized blockchain for iot. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pages 173–178. ACM.
- [Dorri et al., 2017b] Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. (2017b). Blockchain for iot security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, pages 618–623. IEEE.
- [Gubbi et al., 2013a] Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013a). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660.

- [Gubbi et al., 2013b] Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013b). Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660.
- [Kusmierz, 2017] Kusmierz, B. (2017). The first glance at the simulation of the tangle: discrete model.
- [Nakamoto, 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- [Popov, 2016] Popov, S. (2016). The tangle. *cit. on*, page 131.
- [Szabo, 1994] Szabo, N. (1994). Smart contracts. *Unpublished manuscript*.
- [Szabo, 1997] Szabo, N. (1997). The idea of smart contracts. *Nick Szabo’s Papers and Concise Tutorials*, 6.
- [Vermesan et al., 2009] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaecker, H., Bassi, A., Jubert, I. S., Mazura, M., Harrison, M., Eisenhauer, M., Doody, P., Peter, F., Patrick, G., Sergio, G., Harald, Sundmaecker Alessandro, B., Ignacio Soler, J., Margaretha, M., Mark, H., Markus, E., and Pat, D. (2009). Internet of Things Strategic Research Roadmap. *Internet of Things Strategic Research Roadmap*, pages 9–52.