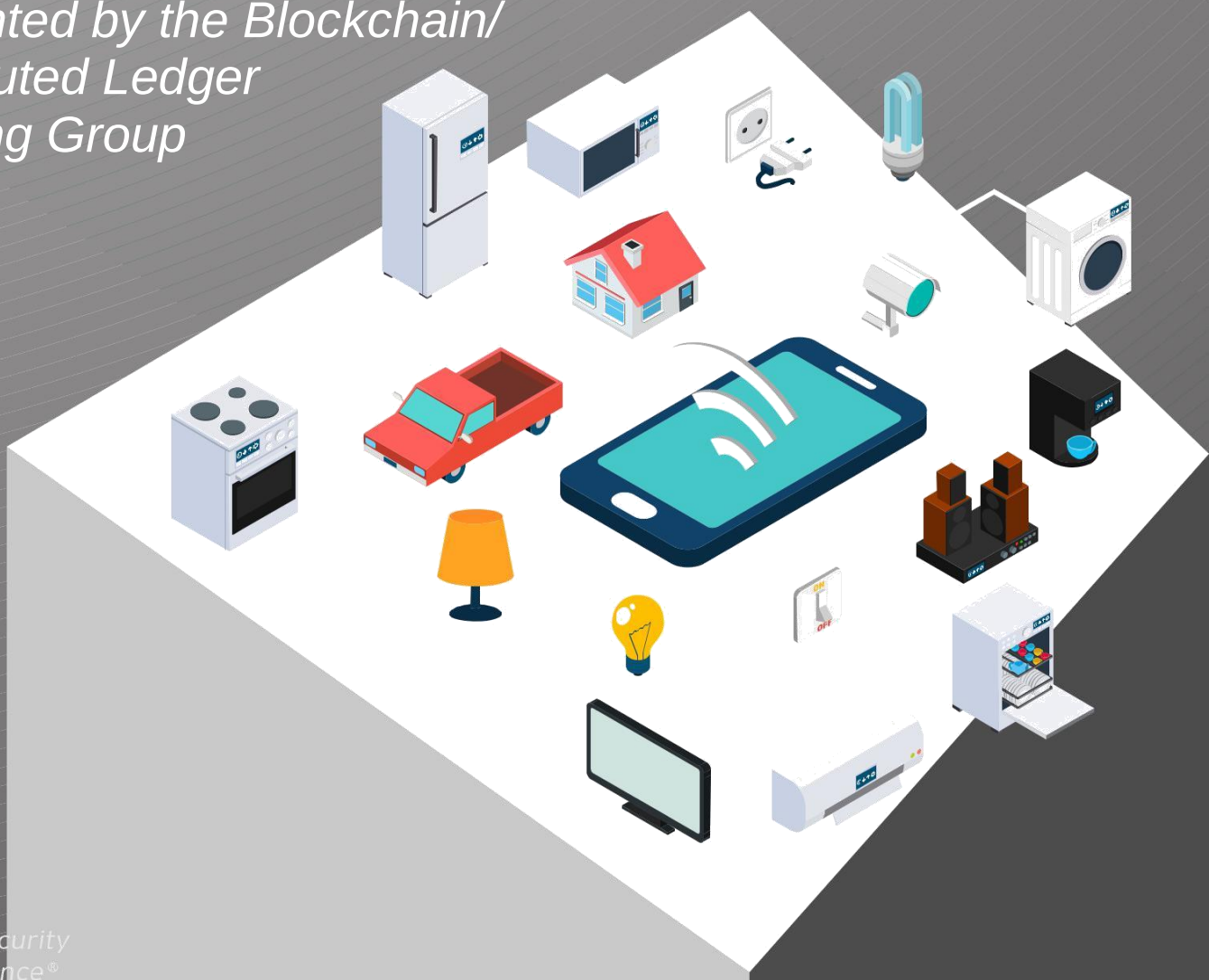
IoT セキュリティのためのブロックチェーン技術の活用

Presented by the Blockchain/ Distributed Ledger Working Group



CSA cloud security alliance®

ABOUT CSA

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at www.cloudsecurityalliance.org and follow us on Twitter @cloudsa.

目次

Initiative Lead:
Sabri Khemissa

Key Contributors:
Alex Brown
Giuliana Carullo
Elier Cruz
Kevin Fielder
Doug Gardner
Jas Khehra
Imre Kocsis
Paul Lanois
Ashish Mehta
Matt Murphy
Todd Nelson
Denis Nwanshi
Luc Poulin
Michael Roza
Brian Russell
Srinivas Tatipamula
Udo Gustavo von Blücher

CSA Staff:
Hillary Baron
Kendall Scoboria
John Yeoh

日本語版提供に際しての告知及び注意事項

本書「IoT セキュリティのためのブロックチェーン技術の活用」は、Cloud Security Alliance (CSA)が公開している「Using Blockchain Technology to Secure the Internet of Things」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2018 年 10 月 02 日	日本語版 1.0	初版発行

日本語版作成に際しての謝辞

「IoT セキュリティのためのブロックチェーン技術の活用」の日本語訳は、CSA ジャパンの「Blockchain ワーキンググループ」に参加するメンバーを中心とした、CSA ジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）

阿賀　誠
勝見　勉
唐澤　光彦
笹原　英司
滝江　勇介
西　　誉
守屋　有晶
諸角　昌宏

はじめに

過去 4 年間に、技術専門家、最高デジタル責任者（chief digital officer）、マーケティングマネージャ、ジャーナリスト、ブロガー、研究機関が、ブロックチェーン技術を使用したセキュアなトランザクション処理とストレージのための新しい分散モデルについて議論し、推進してきた。IDC FutureScape は、2020 年までに世界貿易金融の 20%がブロックチェーンを組み込むと予測している。

[1]. Coindesk は、ベンチャーキャピタルが過去数年間にブロックチェーンの新興企業に 18 億ドル以上を投資したと報告している。

[2]. セクター間のブロックチェーン技術の新しいユースケースを特定することに重点を置く Enterprise Ethereum Alliance など、コンソーシアムや提携が始まっている。

ブロックチェーンは、ブロックにグループ分けされた取引の公開および分散台帳で、次のことを約束している。

1. デジタル資産の所有権の移転に対するスピード、効率、セキュリティを向上する
2. 所有権の証明と取引の解消を行う中央の権威者を不要にする
3. 透明かつ公的に監査可能な台帳を提供することにより、不正行為や腐敗を減らす
4. 特定の条件に基づいて、信頼できるアクションを自動的に有効にし、安全にし、認証することで、契約を使用することの管理コストを削減する（「スマートコントラクト」）

ブロックチェーンの利用に関する重要な課題は、ブロックチェーン技術の統合から利益を得る関連するユースケースを特定する必要がある。Internet of Things（IoT）は長い間、セキュリティの弱点や課題があり、専門家や組織は IoT を安全にするためにブロックチェーンの使用を検討し始めている。IOTA や Trusted IoT Alliance などの組織は、ブロックチェーンを適用して IoT セキュリティに焦点を当て始めている。

IoT は、それ自体、消費者の行動やビジネスプロセスを変革している。分散エッジ IoT デバイスは、処理のためにデータを収集し、送信する。IoT システムは、このデータによって、高度なサービス、自動化機能、エンドユーザーのための経験を提供する。IoT システムは動的でかつ分散している。これらには、デバイス、モバイルアプリケーション、ゲートウェイ、クラウドサービス、分析と機械学習プロセス、ネットワークインフラ、Web サービス、ストレージシステム、フォグレイヤー、ユーザーが含まれる。これらのすべてのシステムは、台帳にトランザクションとして記録できるデータの書き込みと読み取りを行う。

Cloud Security Alliance の IoT ワーキンググループ（IoT WG）は、2014 年以降、IoT セキュリティのベストプラクティスを文書化することに注力してきた。IoT のセキュリティ問題にブロックチェーン技術を適用することによる潜在的な利点を考慮して、IoT WG は CSA の Blockchain/Distributed Ledger Technology ワーキンググループと一緒に、ブロックチェーンが IoT システムをセキュアにする方法について研究し文書化することを始めている。このように、この文書では、成熟度の異なる以下の 2 つの技術について説明する：

- **ブロックチェーン**： BitCoin、Ethereum、Litecoin、Dash など、急速に進化する暗号通貨のサポートを通して、デジタル経済全体に急速な変化と混乱をもたらした技術手段。暗号通貨の基盤としてのブロックチェーンの成功は、分散台帳技術を使ってシステムと技術を安全にすることを目的とした業界内での新しい研究を生み出した。2017 年には、多くのビジネスイニシアチブが、限られたプロトタイプと概念実証（proof-of-concept）の作成にフォーカスし、この複雑な技術を習得するためにほとんどの時間を費やしてきた。

- **IoT**： ビジネスプロセスやミッション処理の変革をサポートする急速に成熟した一連の技術。IoT は、消費者、輸送、エネルギー、ヘルスケア、製造、小売、財務などのセクターにわたって、様々なレベルで成熟している。IoT は、コネクティッド・カー、スマートビルディング、産業用制御システム、ドローン、ロボットシステムなどの物理デバイスに、エレクトロニクス、ソフトウェア、センサー、アクチュエータ、ネットワーク接続が組み込まれ、これらのオブジェクトがデータを交換できるようになる。

このホワイトペーパーでは、ブロックチェーン技術の概要を説明し、IoT 機能をセキュアにする技術としてブロックチェーンを使用できるようにする一連のアーキテクチャパターンについて説明する。これらのユースケースの技術的実装は企業によって異なるが、IoT セキュリティに対するブロックチェーンの具体的なユースケースの例についても調査している。

ブロックチェーン技術概要

ブロックチェーンサービス、または単に「ブロックチェーン」は、トランザクションをひとまとめにしてブロックに格納するトランザクションリポジトリである。"すべてのブロックには、前のブロックのハッシュが含まれている。これは、genesis ブロックから現在のブロックまでの一連のブロックをチェーンで接続していることになる"[3]。各ブロックの内容は、記録されたトランザクションのデータの完全性を保証するためにデジタル署名されている。

ブロックチェーンサービスには、次の 3 つの主要コンポーネントが含まれる：

(1) 自律ノードのネットワーク

独立したノードは、自律的に正当なトランザクションを生成し、分散台帳に登録する。トランザクションを検証するには、中央権限も信頼できる第三者も必要ない。ブロックチェーンサービス（ブロックチェーンプラットフォームとも呼ばれる）のすべてのノードが連携して、台帳の一貫性を維持する。

各ノードは、コンセンサスアルゴリズムと呼ばれるメカニズムを実行する。コンセンサスアルゴリズムは、一連のトランザクションの結果としてノードがブロックチェーンを更新する方法に同意するプロセスである。コンセンサスを達成することで、ネットワーク内のノードの大多数が同じ一連のトランザクションを検証することが保証される。

分散型コンセンサスの目標は、参加しているシステムの中で十分に多い数の台帳を（ある程度細かい時間間隔で）正確かつ最新のものに保つことである。コンセンサスメカニズムは、（a）遡及的に取引を変更すること（b）意味的に許可されていないトランザクションを実行する（例えば、「二重支出」および暗号非同期設定で非所有資産を転送する）。（c）正しいトランザクション要求の受け入れ、及び予約をブロックすること、などによって台帳の完全性を損なう可能性のある悪意のあるピアから守っている。

ブロックチェーンサービスの開発中に選択されたコンセンサスアプローチは、特定の攻撃を防ぐ。これらの攻撃緩和は事実上技術的なものではない。例えば、Bitcoin の "Proof of Work"では、ネットワーク内のハッシュパワーの 51%を制御することに経済的に不利な立場にある。マイニングハッシュレートの 51%を獲得することで、攻撃者がコインを 2 倍にしたり、最近の取引履歴を変更する可能性がある。また、ハッシュレートの 51%を取得し、悪意のあるトランザクションを伝播すると、暗号の信頼性が急速に低下し、悪意のある当事者の株式の価値が大幅に低下する。さらに、悪意のある当事者は、自分自身のために利益を生むために、マイニングのプロセスに向けて単純にハッシュパワーを利用することができる。

許可された（閉じた）システムでは、経済的阻害要因は存在しない可能性がある。 また、許可されたシステムでは、マイニングの難易度が低いため、ネットワーク内のトランザクションを高速化できる。これらの許可されたシステムには、レジリエンス・セーフガード、ハードウェア・ベースのウォレット、ネットワーク・マイナーへのアクセスを制限するアクセス制御、アイデンティティ管理、潜在的な規制当局への関与、訴訟、不正行為の犯罪調査を可能にする強力な監査機能を含む伝統的なサイバーセキュリティ管理システムを実装しなければならない。

3 つの主要なメカニズムがブロックチェーンのコンセンサスを提供する：

- ***ビザンチンフォールトトレランス（BFT）アルゴリズム***は、障害のあるノードに任意の動作（ビザンチンフォールト）が発生するような攻撃やソフトウェアエラーを回避するように設計されている。BFT [4]は、悪意のある不正行為（ビザンチン）ノードの参加にもかかわらず合意を提供する。しかしながら、このアプローチの欠点は、ブロックチェーンネットワークを形成するノード数のスケーラビリティの限界である[5]。実用的ビザンチンフォールトトレランス（PBFT）[5]を含む BFT への代替

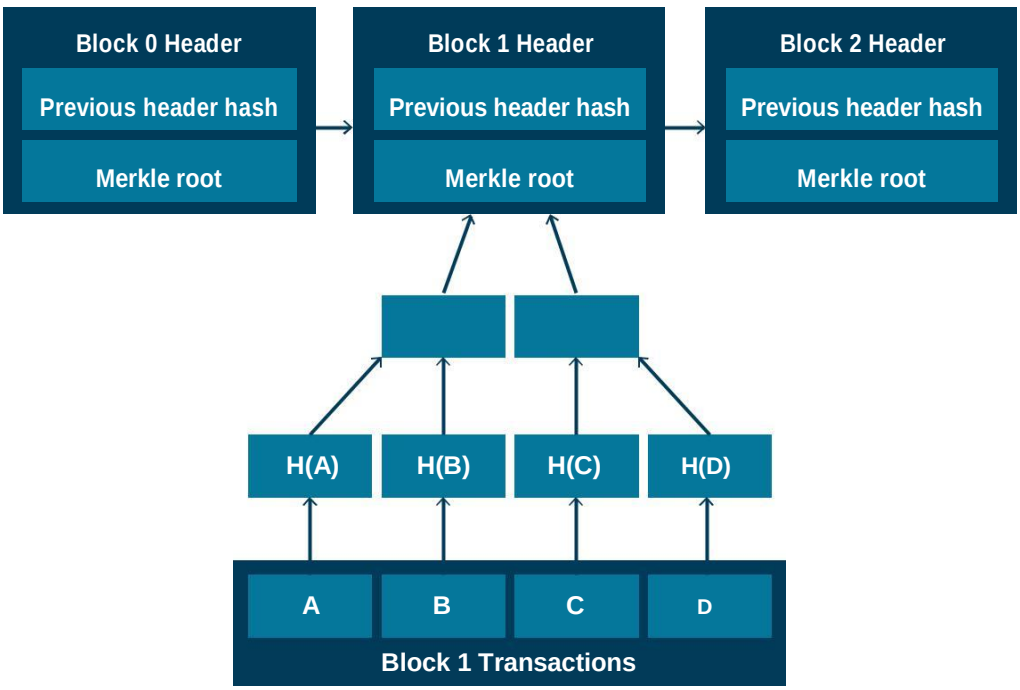
アプローチが提案されている。PBFT を現在利用しているブロックチェーンインプリメンテーションの例は、Linux Foundation Hyperledger fabric（0.6）と Ripple である。

- ***Proof-of-Work（POW）*** は、Bitcoin と Ethereum で使用され、コンセンサスを確立するための広く知られたメカニズムである。POW では、単一のノードが他のノードにその結論を提供することができる。この結論は、ネットワーク内の他のノードによって検証される。コンセンサスを達成するために、生成されたブロックを提出するノードは、計算上困難なタスク（ハッシュ関数に基づく「暗号的に困難なパズル」）である、実行した作業の証明も提供しなければならない。POW は優れたネットワーク安定性を提供する[6]。しかし、POW は、計算資源が消費されるために特にコストがかかる。「マイナー」は、成功したブロック生成の対価として付与される暗号通貨の報酬を得るために参加するように動機づけられる。
-
- ***Proof-of-Stake（POS）*** は POW と似ている。ノードがブロックを生成すると報酬が与えられる。しかし、このフェーズには少数のノードしか参加できない[7]。実際、蓄積された富（すなわち「ステーク」）に基づいて決定論的に次のジェネレータノードが取り出される。POS に基づくブロックチェーンのマイニングプロセスは、通常、“forgery” あるいは “minting” と呼ばれる。（訳注：どちらも「鋳造」を意味する）。PoS を開始したテクノロジは PeerCoin である。

(2) 取引の台帳

データベースはブロック（したがって「ブロックチェーン」）で構成されている。各ブロックには、有効なトランザクションのリスト、タイムスタンプ、および現在のブロックと前のブロックをリンクする情報が含まれている。各ブロックの先行ブロックへのリンクを連鎖すると、台帳が作成される。

台帳の中心は、可変サイズのデータを固定サイズの文字列にマップする数学的アルゴリズムである暗号ハッシュである。すべてのトランザクション A, B, C, D はハッシュされ H(A), H(B), H(C), H(D)になる。その後、次のハッシュが統合され H(hA|hB), H(hC|hD)になり、マークルツリーを構成する。先頭のハッシュまたはマークルツリーのルートは、ブロックヘッダーに統合される。



マークルツリーはブロックトランザクションをブロックヘッダーであるマークルルートに接続する

(3) 分散データベース

新しいトランザクションが追加されると台帳が作成され、システムのノード間で利用可能になり複製される（したがって、「分散型台帳」）。ネットワーク上のすべてのノードは、それぞれデータベースのコピーを持ち、すべてのトランザクションの履歴にアクセスできる。

特定の暗号通貨のブロックチェーンサイズは、IoT や台帳をホストしているデバイス内のストレージ容量の要件に左右される。以下の表は、2017 年 8 月 14 日時点で良く知られている暗号通貨のブロックチェーンサイズを示している[30]。

Cryptocurrency	Blockchain Size (snapshot 8/14/17)
Bitcoin	151.74 GB
Ethereum	98.94 GB
Ethereum Classic	20.12 GB
Litecoin	8.62 GB
Dash	3.69 GB

トランザクションの送信とブロックチェーンの構築

以下は、ブロックチェーントランザクションの一般的な処理フローである。トランザクションがノードに紐づけられると、ブロックチェーンサービスは通常次のように実行される[6]：

1. 新しいトランザクションがすべてのノードにブロードキャストされる。
2. 各ノードは、新しいトランザクションをブロックに取り込む。
3. 各ノードは、そのブロックのコンセンサスアルゴリズムで動作する（一般に、この処理はノード処理と消費電力の面で高くつく）。
4. ノードがコンセンサスアルゴリズム処理を完了すると、ノードはブロックと処理結果をすべてのノードにブロードキャストし、この作業の報酬を受け取る。（Bitcoin の場合、報酬は Bitcoin マイナーによって処理され、受け取られた取引手数料である。）
5. ノードは、その中のすべてのトランザクションが妥当な場合にのみブロックを受け入れる。
6. ノードは、受け入れられたブロックのハッシュを前のハッシュとして使用して、チェーン内の次のブロックの作成に取り組み、ブロックの受け入れを行う。

この技術は新しいものではなく、デジタル署名、暗号化ハッシュアルゴリズム、ピアツーピア接続、分散データベースなどが使われている。コンピューティング能力とインターネット速度の向上により分散コンピューティングが可能になるため、これらの個別の技術を効果的に組み合わせたブロックチェーン技術が、この状況において必要になる。

スマートコントラクト

スマートコントラクトは台帳にある自己実行コードである。スマートコントラクトを使用して、2 人の当事者が取引を行う。例えば、一方の当事者はサービスを提供することができ、他方の当事者はそのサービスに支払いを行う。スマートコントラクトはトランザクションのルールを実行し、違反に関連する罰則を課すこともできる。

IoT の環境では、デバイスはブロックチェーン上のコントラクトアドレスに基づいてスマートコントラクトとやり取りをするように事前設定できる。これらのデバイスは、お互いの間でトランザクションを開始することができる。スマートコントラクトはトランザクションの流れを監視し、資金を支払うか行動を許可する前に、規則に従っていることを検証する。

スマートコントラクトを利用する IoT システムの実装者は、誤った使い方の可能性を考慮した処理をコントラクト上で実装する必要がある。例えば、スマートコントラクト開発者が、スマートコントラクトの完了条項の検証まで資金を留保するエスクロー要件を実施することができる。その他のスマートコントラクトを利用するにあたってのセキュリティに関する考慮事項としては、以下のようなものがある：
・未完了トランザクションを、そのトランザクションの発行者以外が再実行することという競合状態を回避する必要性
・コントラクトの送信者と受信者の間で再帰呼び出しになっていないことを検証する
・スマートコントラクトの利用を、許可されたデバイスに限定する
詳細については、https://consensys.github.io/smart-contract-best-practices/を参照。

オフチェーンストレージソリューション

ブロックチェーン技術の実装を担当するソリューション開発者は、パブリックブロックチェーンネットワークに組み入れられた機密保護が存在しないことを認識する必要がある。プライベート・ネットワークや許可型ネットワークであっても、オンチェーン上で機微データの保存を可能にするための十分な機密保護ツールはない。従って、多くの組織は、ブロックチェーンがトランザクションとしてハッシュを記録している一方で、生成したデータの保存に使えるオフチェーンストレージソリューションを立ち上げる必要がある。そのソリューションは、あらゆる規制要件または業界ベストプラクティスに従った暗号化を具備する必要がある。

配備オプション

ブロックチェーンは、以下の 3 つに大別されます[11]。

- **非許可型(パブリック型)**：すべてのノードはトランザクションの読み取りや発行が可能であり、さらにコンセンサスプロセスに参加することもできる。POW コンセンサスアルゴリズムは非許可型に最も適している。
- **コンソーシアム型（例：部分許可型）**：事前に定義されたノードのみコンセンサスプロセスに参加出きる。トランザクションの読み取りや実行は、全ノードが実行できる場合もあるが、ノードが制限されている場合もある。BFT コンセンサスアルゴリズムは、Linux Foundation によって運営されているオープンソースの取り組みである Hyperledger のようなコンソーシアム型配備に最も適している[13]。

- **許可(プライベート)型**：コンセンサスメカニズムとは関係なく、信頼された組織のみが、ブロックチェーンに向けてトランザクションが発行可能である。プライベート型は、規制業種や同一法人に属する組織間に適している[11]。プロジェクト R3[19]や ChainCore[20]が金融機関に向けて提案しているような業界特化型の取り組みは、中央管理によって統治されているプライベートブロックチェーンになる可能性が高い。

Bitcoin[12]と Ethereum[14]は、分散アプリケーションをサポートすることで普及したパブリック型ブロックチェーンである。Ethereum は、IoT デバイス間で自律的にトランザクションを発行し合うことを可能とするスマートコントラクトを容易に開発するためのプログラミング言語である Solidity を備えている。BTC Relay[15]のようなソリューションは、Bitcoin による支払を Ethereum のスマートコントラクト上で決済する機能を提供している。

ブロックチェーンの実装は、ブロックチェーンネットワーク上で、暗号通貨や分散アプリケーション、スマートコントラクトのようなサービスを構築するためのフレームワークである。そのフレームワークは、使用される理論的概念とそれらの組み合わせ方法（例えば、コンセンサスメカニズム、電子署名、暗号化、通信特性）を記述している。フレームワークを実装するための技術要素を特定し詳述するかは実装者次第である。右上の図は、ブロックチェーンベースの IoT セキュリティソリューションを設計する際に考慮すべき技術要素を示している。

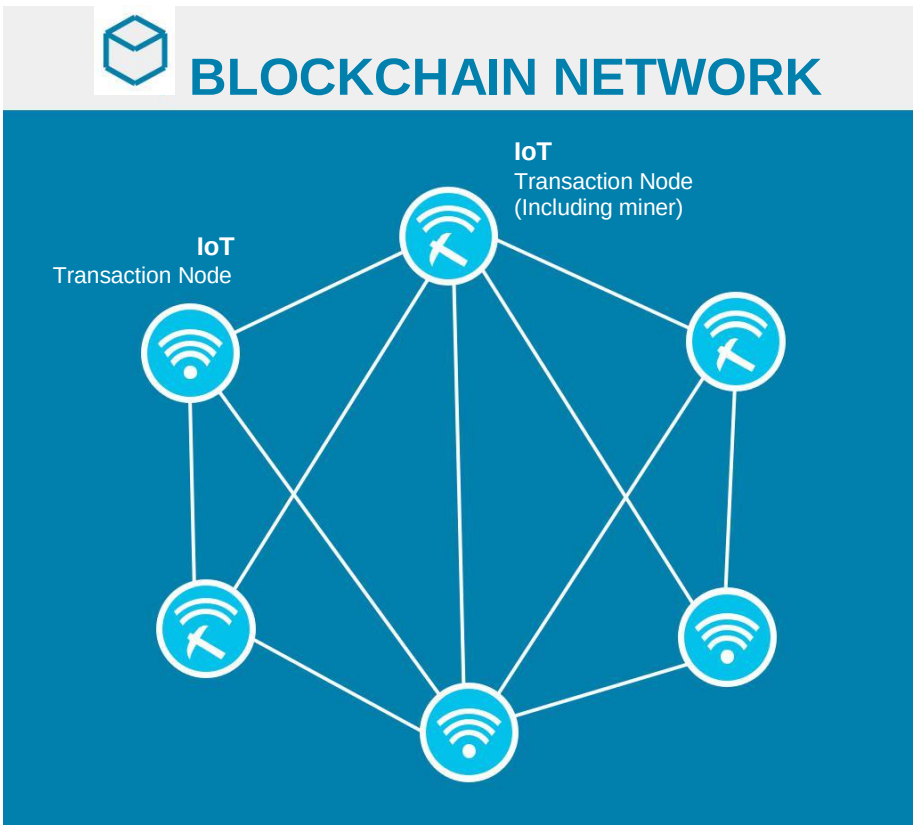
ブロックチェーンは複数の実装が可能であり、それぞれ、異なる利用方法やサービスを提案している。2-way peg[9]と呼ばれている、異なるブロックチェーンの機能へのアクセスを可能にする中継の方法によって、異なるブロックチェーンネットワーク間で、トラストレスに交換が出来るようになる。Rootstock[10]は、ビットコインとの 2-way peg を備えた、OSS のスマートコントラクトプラットフォームである。

ブロックチェーン技術に基づく IoT アーキテクチャ

ブロックチェーン技術を IoT に適応させるためには、ブロックチェーン技術に基づく IoT アーキテクチャパターンの検討が必要である。この定義されたパターンには、このセクションで説明するように、３つの要素が含まれることが必要である：

コミュニケーションモデル

コミュニケーションモデルは、ブロックチェーンソフトウェアのインストールについて、IoT ノードへ直接導入する場合と、クラウドに置いてアプリケーション・プログラミング・インターフェース（API）経由で IoT ノードに導入する場合とについて説明する。以下の図は、IoT エッジデバイスがトランザクションノードソフトウェアを保持し、台帳を格納し、ネットワーク全体でコミュニケーションを維持できるようにする堅牢な機能を備えている場合における、ブロックチェーン技術と IoT を組み合わせた一般的なモデルである。



各々の IoT ノードがブロックチェーン Transaction node として動作

IoT Transaction Nodes

前の図では、それぞれの IoT デバイスが台帳を保持し、マイニングを含むブロックチェーントランザクションに参加することができる。各デバイスには、秘密鍵が配備されているか、ネットワークトランザクションに参加するための秘密鍵を内部で自己生成する機能が含まれている。このエンドステートモデルは、ブロックチェーンサービスで有効にできる３つの基本機能を提供する：

- 自律的調整（例えば、コンセンサスや P2P メッセージング）を含む自立型 IoT デバイスネットワーク
- IoT デバイスが暗号機能を実行するトランザクションを作成できるトランザクションの台帳
- IoT デバイスに台帳の最新バージョンがある分散データベース

ただし、ハードウェアの制限により、現時点では IoT においてこのモデルを採用することは難しい。以下の課題がある:

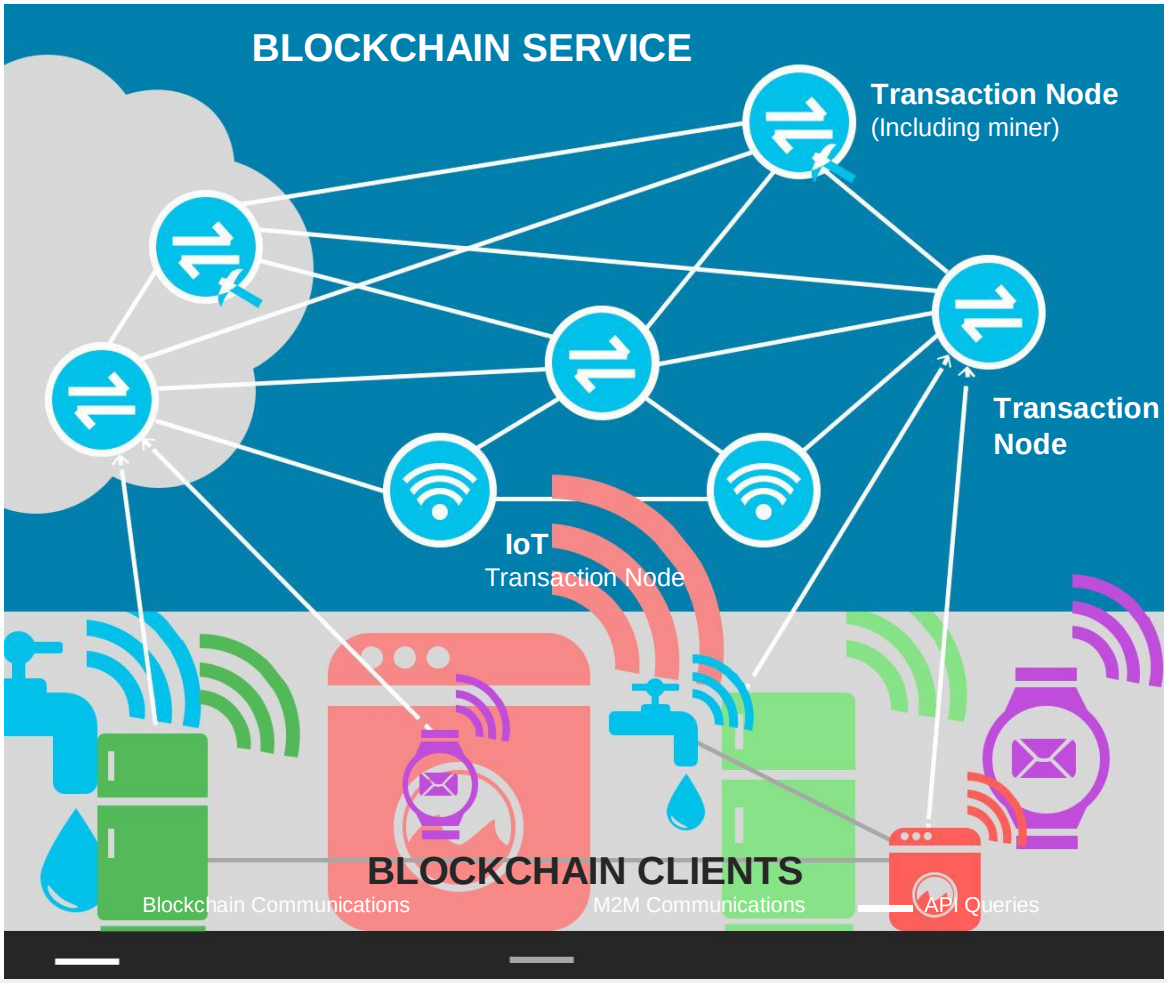
1. **低い処理能力**：ブロックチェーンサービスの処理には、処理能力の高い CPU、メモリおよび電力が必要である。ブロックチェーンプラットフォームにおける処理能力は主に、POW、スマートコントラクトの実行、暗号プリミティブ処理に消費される。
2. **小さいストレージ**：台帳に追加されるトランザクションの量が増え、少ないトランザクションデータでも維持するのが難しくなる。
3. **制限された接続**：IoT デバイスは帯域の小さいインターネットまたは無線アクセスを利用する可能性があり、これにより、台帳のダウンロードや同期中にパフォーマンスの問題が発生する可能性がある。

IOTA のようないくつかの企業は、小さなセンサーを「ブロックチェーン化」するための、以下を含む新しいアプローチを提案している：

- ハードウェア要件を軽減するためにマイニングプロセスを簡略化する
- IoT 通信に関連するマイクロトランザクションの実装
- 軽量な台帳を管理する

クラウド対応の IoT ブロックチェーンネットワーク

クラウド対応のブロックチェーンネットワークでは、トランザクションノードとマイニングノードが、クラウドとオンプレミスの両方に配置される。実装次第で、ノードは、エンタープライズ・サーバ、PC またはスマートデバイス（例えば、スマートフォンやタブレット）、クラウドベースの仮想サーバ、十分なハードウェアリソース（CPU、RAM、ストレージなど）を備えた IoT デバイスとすることができる。



限られたハードウェアリソースを持つ IoT デバイスは、ブロックチェーンクライアントとして機能する。この場合、分散台帳は保持されない。これらのクライアントは API を介して上流のクラウドベースのブロックチェーントランザクションノードと通信する。API は主として HTTP REST または JSON RPC のいずれかとなる。

IoT デバイスは、ブロックチェーンサービスで処理されるためにトランザクションノードに中継されたデータを収集するか、クラウド内で動作するブロックチェーンノードを指定することによってスマートコントラクトトランザクションに参加する。この流れにおいては、IoT デバイスは、依然としてデータに署名するための秘密鍵を備えている。署名されたデータは、処理のために上流のトランザクションノードに送信される。データを安全に送信するためには、IoT デバイスとトランザクションノード間の別の信頼関係が必要である。例えば、１対１の関係では、２つのデバイス（IoT デバイスとトランザクションノード）間のホワイトリスト作成と双方向認証を使用することができる。秘密鍵を安全に保存するためにはハードウェアセキュリティを使用する必要もある。

許可された領域（プライベートブロックチェーンサービス）では、マイニングノードへのアクセスは、許可されたオペレータに限定される場合がある。

コンソーシアム領域（部分的に許可されたブロックチェーンサービス）または許可された領域（プライベートブロックチェーンサービス）では、セキュリティを向上させるため、または規制遵守の目的で、メンバーはこのアーキテクチャパターンを実装することを決定できる。

ビットコインの実装では、このような機能を Simplified Payment Verification (SPV) という名前のシンクライアントを使用して提案している。これは、台帳の完全なコピーは保持しない。これらのシンクライアントは Bitcoin Client API（BCCAPI）を使用してノードと通信する。

メッセージは、複数の IoT デバイス間で交換することができる。これらのメッセージは、トランザクションに統合されたデータを含む。これらのトランザクションは、トランザクションノードとの交換に参加する IoT デバイスによって中継される。IoT デバイス間の通信プロトコルとメッセージフォーマットは、ブロックチェーン実装の範囲外である。これらの通信は Message Queue Telemetry Transport（MQTT）などの機器間通信のことである。

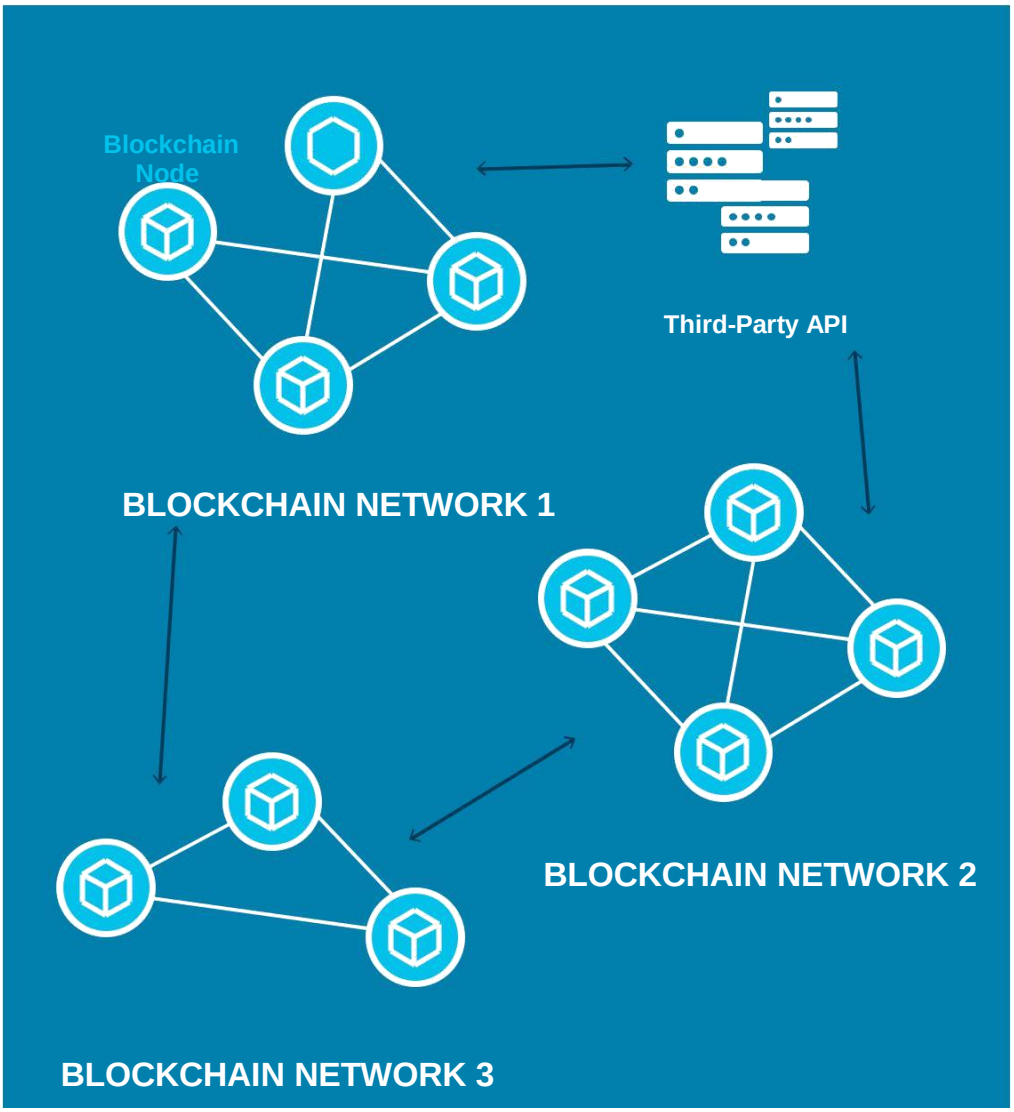
相互運用性を高めるための充実したエコシステム

ブロックチェーン技術を取り巻くエコシステムを開発することは、その採用を加速する機会になる。この潜在力のあるエコシステムは、IoT のブロックチェーンサービスへの統合を簡素化する機能を提供する。

- **サービスプロバイダ**：Blockcypher などのサービスプロバイダは、IoT とブロックチェーンサービスのクライアントおよびサービス間の通信を簡素化する API 機能を提供する。API の仲介は、ブロックチェーン技術の実装ではなく、サービスの価値に焦点を当てることにより、異なるブロックチェーンサービスと通信する IoT の開発が可能になる。
- **ソリューションプロバイダ**：Credits などのソリューションプロバイダは、プライベートブロックチェーンサービスを迅速に構築するためのフレームワークを提供する。これらのフレームワークはトランザクションノード上で動作する。各ノードは API を介してクライアントからアクセスされる。また、これらのフレームワークは、他のブロックチェーンサービスと連携する機能も提供する。

複数のブロックチェーンサービスの同居

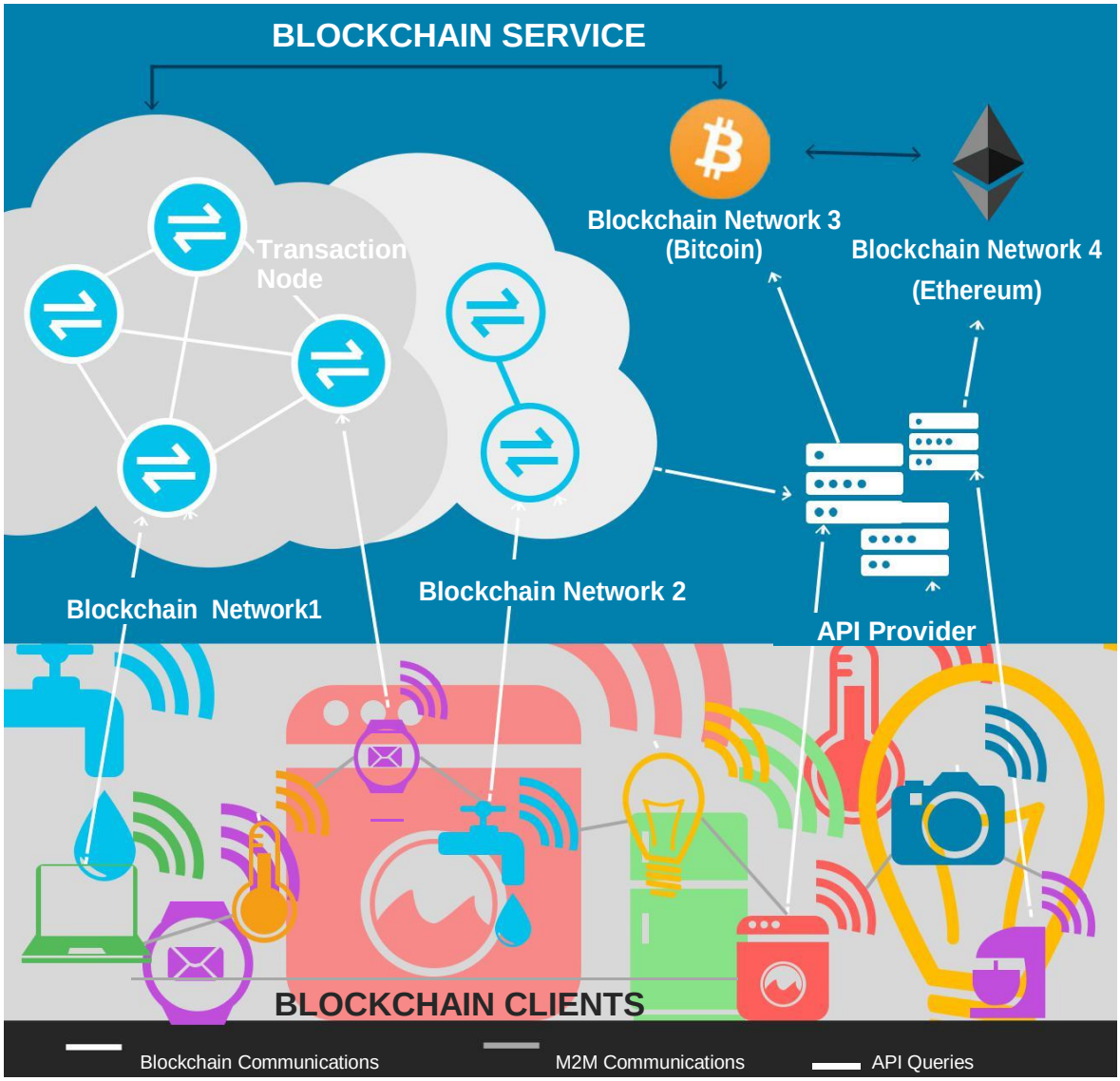
次のページの図に示すように、それぞれが異なった機能と通貨を持つ複数のブロックチェーンサービスにフォーカスした考え方があり、またその数は増え続けていく。これらのブロックチェーンサービスは補完的な機能を果たす。各ブロックチェーンサービスは、ネイティブに、またはサードパーティが提供する API を使用して、結合することができる。



各々のブロックチェーンサービスは異なったコンテキストで走る。たとえば、ホームネットワーク、企業ネットワーク、インターネットである。

ブロックチェーン技術に基づいた IoT アーキテクチャのパターン

CSA IoT WG およびブロックチェーン／分散台帳技術 WG は、複数のブロックチェーンサービス内にある IoT クライアントが協働できる以下のシステムを提案している。



ブロックチェーンサービス１：法人専用サービス：

- トランザクションノードは、クラウドにホスティングされた法人のコンピュータ、あるいはサーバである
- IoT ブロックチェーンクライアントは、企業エリア内に配備されたセンサーとスマートデバイスである

ブロックチェーンサービス２：消費者向けスマートホームサービス：

- トランザクションノードは、パソコンとその他のデバイス、またはクラウドサービスである
- IoT ブロックチェーンクライアントは、冷蔵庫、温度センサー、セキュリティカメラといったスマートデバイスである

IoT デバイスがブロックチェーンサービスのクライアントとなるアーキテクチャは、ブロックチェーン技術の実装に向けた産業界の取り組みに主に採用されている。

IoT セキュリティに向けたブロックチェーン技術の選択

ブロックチェーン技術は、IoT デバイスをセキュアにするのに役立つ。IoT デバイスは、パブリックブロックチェーンサービスを使用するか、クラウド内のプライベートブロックチェーンノードと安全な API を介して通信するように構成できる。IoT システムのセキュリティフレームワークにブロックチェーン技術を組み込むことにより、IoT デバイスは安全に互いを検出し、分散鍵管理技術を使用してマシン間のトランザクションを暗号化し、ソフトウェアイメージの更新とポリシーの更新の完全性と真正性を検証することができる。

このレポートで説明しているアーキテクチャパターンが実現すれば、それによって IoT デバイスは API を介してブロックチェーントランザクションノードと通信し、制約のあるデバイスであってもブロックチェーンサービスに参加できる。

セキュリティを確実にするために、特定のブロックチェーンサービスへ接続しようとする IoT デバイスのブートストラップ中、注意が必要となる。以下は、IoT デバイスのトランザクションノードへ参加することをサポートする IoT デバイスの検出の例である。IoT デバイスは、まずトランザクションノードとして追加されるための認可を証明するための資格情報を付与される必要がある。この資格情報の付与は、特定の IoT デバイスエコシステムの脅威に対して保護されている安全な環境で実施する必要がある。

このことを実現することを可能にするブロックチェーン技術と市場のイニシアチブを検討した結果、ブロックチェーン技術を使う IoT をセキュアにするために検討すべき以下の 5 つ機能が浮かび上がる：

1. スケーラブルな IoT の検出
2. 信頼できる通信
3. メッセージ認証/署名（Chain of Things [27]）
4. IoT の構成と更新
5. セキュアなファームウェアイメージの配布と更新

1.スケーラブルな IoT の検出

スマートシティと大企業の IoT の配備は、協働すべき数千～数万の IoT デバイスをアクティベーションすることになる[28]。多くの場合、これらのデバイスは自律的なマシンツーマシントランザクションによって、お互いに協調し合う。相互に作用するための正しい接続相手デバイス、正しいサービスをデバイスが発見できることも必要となる。IoT システムは、ブロックチェーンの実装が、パブリック、プライベートのどちらであってもスケーラブルな IoT の検出を利用できる。

たとえば Bitcoin では、ハードコードされた Named DNS Seeds のセットが、新しいユーザーやデバイスにブートストラップサービスを提供する。これらの DNS Seeds は、IoT デバイス内で事前設定できる。IoT デバイスはこれらのアドレスを照会し、完全なノードの IP アドレスを提供される。 IoT デバイスは、それ自体をノードに登録し、ネットワーク上の他の IoT デバイスのリストを要求する。 プロビジョニングされると、IoT デバイスは、ピアツーピア通信を開始し、ピア発見情報をネットワーク上の隣接デバイスに示すことができる。

Named DNS Seed アドレスを事前設定（ハードコーディング）することで、MITM（man-in-the-middle）攻撃を軽減する。 IoT デバイスは、複数の DNS Seed から情報を受信した後、登録するノードを選択する。ルートサーバの名前解決を保護し、DNS スプーフィング攻撃を軽減するためには、DNS Sec を使用しなければならない。

Named DNS Seed アドレスはファームウェアにハードコードする必要がある。このホワイトペーパーのケース５で、ファームウェアイメージの配布と更新を保護する方法を示す。

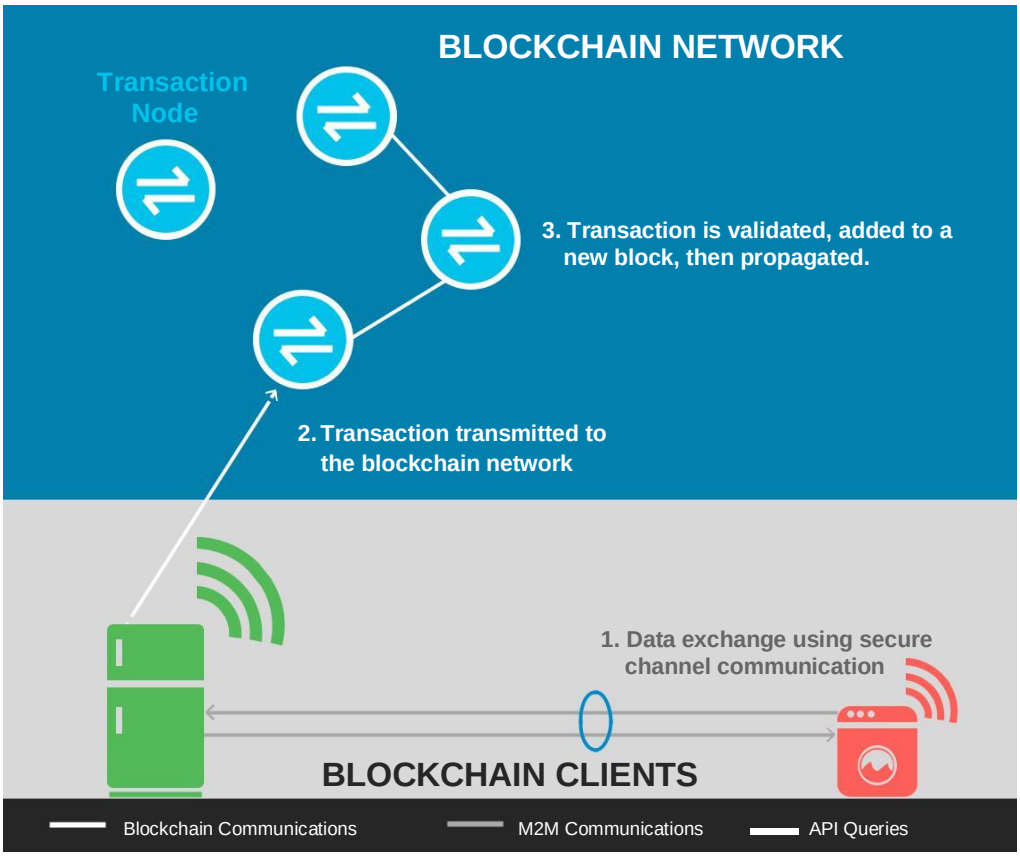
プライベートブロックチェーンサービスにおいても、ブートストラップと IoT デバイスのネットワークへの登録をサポートすることができる。トランザクションノードは、信頼できるノードリストを提供する前に IoT デバイスを認証する。IoT デバイスは参加のための資格情報を提供され、それには以下が含まれる

1. IoT デバイスに（予め）インストールされているセキュリティ資格情報、または、セットアップ中に内部的に自己生成されるセキュリティ資格情報は、ブロックチェーンの実装の一部となる安全なプロセスを使用して生成と提供を行う必要がある。
2. IoT デバイスの所有者、または設置担当技術者によって提供される資格情報は、その IoT の特定の資格情報を取得するため、セキュリティサーバへのデバイスの登録を実施する

どちらの場合でも、正しい IoT デバイスだけをブロックチェーンサービスに追加するのを確実にするために登録プロセスを実施する必要がある。すべての通信の記述は、機密性と完全性を確保するために認証され、暗号化されることが必要である。

ブロックチェーンにデバイス ID を登録する機能の詳細については、Trusted IoT Alliance を参照し、ブロックチェーンにモノの ID を登録するために開発されたブロックチェーン API を参照のこと。

2. トラステッドコミュニケーション

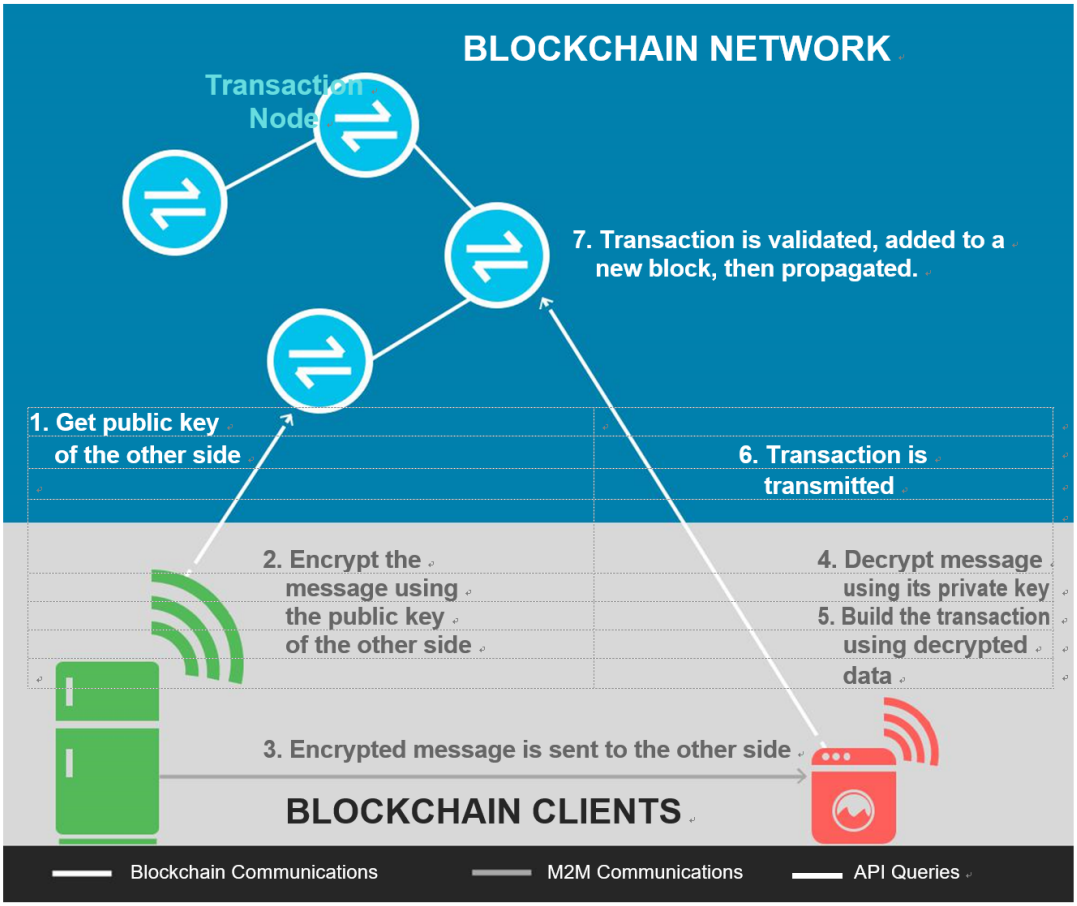


例えば、パブリックデプロイメントなど、いくつかの文脈では、IoT デバイスは、台帳に格納されるトランザクションを構築するために必要なデータを交換するための安全な通信チャネルの使用を必要とする。この台帳は、公開鍵の格納にも使用できる。

情報交換を機密にしなければならない場合、IoT 装置（送信側）は、ブロックチェーンサービスに格納された受信側 IoT 装置の公開鍵を使用し、IoT 装置（受信側）に暗号化メッセージを送信する。

この保護されたトランザクションを実現するために、IoT 送信側は、IoT 受信側の公開鍵をブロックチェーン台帳から取得するようにそのトランザクションノードに要求する。IoT 送信側は、IoT 受信側の公開鍵を使用してメッセージを暗号化する。

受信側だけが秘密鍵でメッセージを復号できる。コンテンツ暗号化鍵（Content Encryption Keys（CEK））やトラフィック暗号化鍵（Traffic Encryption Keys（TEK））などのトランザクションを保護するための鍵を作成するには、楕円曲線ディフィー・ヘルマン(Elliptic Curve Diffie Hellman（ECDH）)などの鍵共有アルゴリズムを使用する必要がある。



このユースケースでは、ブロックチェーンサービスは分散 PKI（distributed public key infrastructure）[29]として機能する。 公開鍵はトランザクション内に格納される。つまり、新しい IoT デバイスがプライベートブロックチェーンまたはパブリックブロックチェーンサービス（前のセクションを参照）に登録されると、新しいトランザクションが作成される。このトランザクションは、公開鍵を含む IoT プロパティで構成される。 IoT デバイスが証明書を更新する必要がある場合、再登録が行われる。失効した証明書をトランザクションとしてブロックチェーンサービスに追加することもできる。 台帳に記録された安全なトランザクション履歴は、IoT デバイス鍵の一貫性を提供する。

ブロックチェーン実装には、複数の種類の暗号鍵が使用される。ブロックチェーントランザクションを保護するために使用される鍵は、しばしばウォレット鍵と呼ばれる。このユースケースで説明された鍵はIdentity Key を表し、IoT デバイス間の通信を保護するためにトラフィック暗号化キー（TEK）またはコンテンツ暗号化キー（CEK）を生成するために使用できる。

- **IoT アイデンティティ鍵** ：IoT デバイス間のメッセージコンテンツおよびトラフィックフローの暗号化のためのキーマテリアルを生成するために使われる非対称鍵ペア
- ウォレット鍵：台帳に格納されたトランザクションを保護するために使われる：IoT アイデンティティ鍵も含まれる

3.半自動型 M2M（Machine-to-Machine）操作

IoT 技術の実現には、ひとつの設定したゴールに向けて、半自動的な方法の中で共に連携して動作するマシンの能力が重要となる。スマートコントラクト機能を使うことによって、ブロックチェーンは、これらの自律型トランザクションのセキュリティを実現する役割を果たすことができる。

スマートコントラクトは、ルール、罰則、契約条件を含むように書くことができる。エッジ IoT デバイスは、スマートコントラクトと対話し、ピアデバイスおよび/またはサービスとの契約を締結するための API を用いて構成することができる。各トランザクションは、実行前に契約条件を満たす必要があり、すべてのトランザクションはブロックチェーンに書き込まれる。

スマートコントラクトは、誰（どの IoT デバイス）がトランザクションに参加できるかのアクセス制限を実施できる。各トランザクションは、IoT ノードのウォレット鍵で署名され、ウォレット鍵はハードウェアセキュリティコンテナに格納されなければならない。ブロックチェーン上のトランザクション記録は、トランザクションが後で否認されないことを保証する（例えば、サービスプロバイダの IoT デバイスが利用者の IoT デバイスとのトランザクションに入る場合）。

4. IoT 設定とアップデートコントロール

より多くの IoT デバイスが、最初からクラウドサービスに接続されるにつれて、信頼があり安全な設定に関してブロックチェーンは有望な技術となる。以下に、３つのセキュリティアプローチを示す：

1. 台帳は、検証されたファームウェアの最新バージョンや設定の詳細など、IoT プロパティをホストできる。ブートストラップの間、IoT デバイスは、トランザクションノードに、設定を台帳から取得するように要求する。パブリック台帳の内容の分析により、IoT ネットワークのトポロジーが読み取られないように、設定は台帳内で暗号化される必要がある。
2. 台帳は、各 IoT デバイスの最新の設定ファイルのハッシュ値をホストすることができる。IoT デバイスは、クラウドサービスから毎晩（または設定された時間）最新の信頼できる設定ファイルをダウンロードし、トランザクションノード API を使用して、ブロックチェーンに格納されているハッシュ値を入手して照合する。これにより、管理者は定期的に不正な設定を消去し、新しい設定でネットワーク内の IoT デバイスを再起動することができる。
3. IoT デバイスのファームウェアイメージに、上記の#2 で説明したものと同じプロセスを適用できるが、IoT デバイスの側で、帯域幅の容量の追加が必要となる可能性がある。

5.安全なファームウェアイメージの配布と更新

ブロックチェーン技術は、クラウドサービスプロバイダから既知の信頼できる設定のダウンロードをサポートするのと同様に、IoT デバイスの信頼できるイメージングプロセスをサポートすることもできる。IoT デバイス開発者は、IoT デバイスファームウェアを作成することによって、独自のブロックチェーンを実装したり、パブリックブロックチェーンを使用したりすることができる。開発者は、そのデバイスファミリの最新の信頼できるイメージをハッシュし、そのハッシュをブロックチェーンにロードすることができる。この方法は、以下の 3 つの方法で IoT デバイスのセキュリティ強化をサポートする：

1. IoT デバイスは、新しいファームウェアイメージを定期的にダウンロードするよう API を介して設定することができる。ほとんどの IoT デバイスは、データを保持したりメモリに保存する必要がないため、必要に応じて上書きすることが可能である。たとえば、ベンダーのブロックチェーンに対してイメージハッシュを検証することで、イメージ更新プロセスを毎日または毎週に設定することもできる。
2. IoT デバイスは、ブロックチェーンベースのイメージ更新プロセスを使用して、ベンダーが提供するすべてのアップデートを検証できる。
3. IoT デバイスは、上記の方法 1 または 2 のどちらかを使用してすべての更新を検証し、また、デバイス所有者に（安全な方法を使用して）ファームウェア更新の承認を要求することができる。

IoT メーカは、ウェブサイトに公開するのではなく、台帳にファームウェアのデジタル署名を保存することによって、現行の標準的なソフトウェア署名の方法を改善する必要がある。更新を適用する前に、IoT デバイスは、新ファームウェアのデジタル署名を台帳から取得し、 メンテナンス用公開鍵を使用して検証する。このメンテナンス用公開鍵は、ファブリック/ハードウェアレベルに組み込むことができる（変更/更新機能なし）。

警告：製造元のメンテナンス用秘密鍵は、すべてのファームウェアを危険にさらさないように保護する必要がある。 秘密鍵を取得する攻撃者は、一見「有効な」デジタル署名を持つ悪質なファームウェアを利用する可能性がある。

製造元がすべてのデバイスの公開鍵を変更するプロセスには、莫大な労力が必要となる。

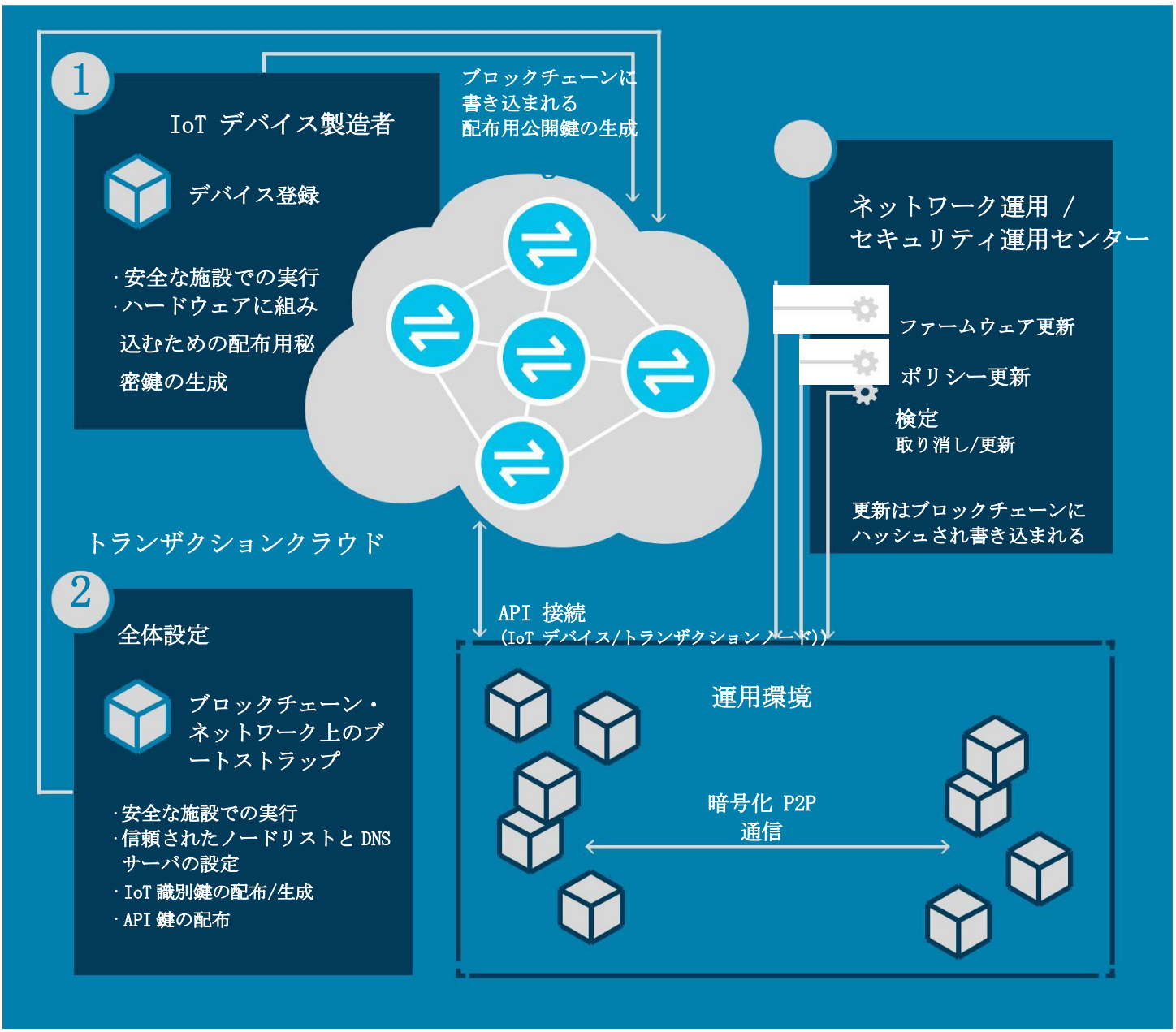
ファームウェアの評価に基づくアップデート（Chain of Things [27]）：

台帳のトランザクション履歴機能は、専門家のコミュニティからの新しいファームウェアの記述を取り込んでくることができるので、マルウェアに感染したファームウェアやバックドアが仕掛けられたファームウェアがインストールされることを回避し、ファームウェアの信頼性を向上させることができる。

IoT デバイスの所有者/管理者は、ファームウェアの評価が台帳の一定の賛成意見のレベルに達した時に IoT が自動更新するように設定する必要がある。ブロックチェーンサービスにおける IoT デバイスのこの「受け入れ(acceptance)」動作は、台帳のデバイスのファームウェア評価をベースにすることができる結果、次のような利点がある：

- ブロックチェーンサービスへの脆弱なデバイスの接続を抑止する
- IoT デバイスのセキュリティ更新プロセスを実施する
- ブロックチェーンサービスに必要な最小限のセキュリティ要件を定義する

IoT におけるブロックチェーンセキュリティサービスのまとめ



結論

IoT ソリューションを実装している組織は、IoT に対する固有の脅威を緩和するのに十分なセキュリティの技術と対処法を見つけ出すという課題に常にさらされている。ブロックチェーン技術は、これらの課題に対処する上で重要な役割を果たすことが期待される。

一部のセキュリティベンダーは、これらのサービスの提供を開始する可能性があるが、ブロックチェーンの実装によって提供される完全性と真正性のサービスをすぐに活用することが可能である。

この文書では、ブロックチェーン技術を使用して接続されたデバイスを保護しようとする際に考慮すべき機能について説明してきた。
しかし、IoT のハードウェアの制約から、数十万個以上の IoT デバイスのコンテキストでは、これらのデバイスの多くはトランザクションノード（トランザクションの生成、コンセンサスの提供など）として機能しない可能性があると結論付けており、安全なブロックチェーンの対象範囲外になる。
多くのデバイスは、ネットワークの上流のトランザクションノードからの API または特殊な仲介により、ブロックチェーンサービスによって提供されるセキュリティおよびその他の機能を有効に活用するこができる。これらの上流機能を使用して、IoT デバイス（構成および更新の制御、安全なファームウェア更新）および通信（IoT 検出、信頼できる通信、メッセージ認証/署名）を保護することができる。

この文書が、ブロックチェーンという機会を利用したビジネスリーダーや開発者を刺激し、IoT のセキュリティを確保するためにこの技術の機能を拡張していくことを期待している。

REFERENCES

[1] IDC FutureScape https://www.idc.com/url.do?url=/getfile.dyn?containerId=US42259417&attachmentId=47254824&elementId=54425583&term=&position=1&page=1&perPage=50&id=b28d2b1c-ddd5-4e60-a2c2-de3a4f7ee253

[2] Bitcoin Venture Capital https://www.coindesk.com/bitcoin-venture-capital/

[3] Blockchain https://en.bitcoin.it/wiki/Block_chain

[4] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. ACM Trans. Program. Lang. Syst., 4:382–401, July 1982. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf

[5] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst., 20(4):398–461, November 2002. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.6725&rep=rep1&type=pdf

[6] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” (2008): 28. https://bitcoin.org/bitcoin.pdf

[7] Vasin, Pavel. “Blackcoin’s proof-of-stake protocol v2.” (2014) https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[8] What is IOTA? https://iota.readme.io/v1.1.0/docs

[9] Trustless exchange and pegging of BTC in Ethereum https://medium.com/@ConsenSys/taking-stock-bitcoin-and-ethereum-4382f0a2f17#.h6nhib6ql

[10] Rootstock http://www.rsk.co/

[11] On Public and Private Blockchains https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[12] Bitcoin https://bitcoin.org/

[13] The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication http://vukolic.com/iNetSec_2015.pdf

[14] Ethereum https://www.ethereum.org/

[15] BTC Relay http://btcrelay.org/

[16] Ethereum Blockchain as a Service now on Azure https://azure.microsoft.com/fr-fr/blog/ethereum-blockchain-as-a-service-now-on-azure/

[17] Hyperledger https://www.hyperledger.org/

[18] IBM Blockchain on Bluemix https://www.ibm.com/blockchain/offerings.html

[19] Project R3 https://r3cev.com/

[20] Chain Core https://chain.com/technology/

[21] Thin Client Security https://en.bitcoin.it/wiki/Thin_Client_Security

[22]BCCAPI (Bitcoin Client API) https://en.bitcoin.it/wiki/BCCAPI

[23]Machine-to-Machine https://en.wikipedia.org/wiki/Machine_to_machine

[24]Blockcypher https://www.blockcypher.com/

[25]Credits http://credits.vision/

[26] Drivechains sidechains and hybrid 2-way peg designs http://www.the-blockchain.com/docs/Drivechains%20sidechains%20and%20hybrid%202-way%20peg%20designs%20-%20Sergio%20Lerner%20-%202016.pdf

[27]Chain of Things http://www.chainofthings.com/

[28]Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From 2016 http://www.gartner.com/ newsroom/id/3598917

[29]Decentralized Public Key Infrastructure http://www.weboftrust.info/downloads/dpki.pdf

[30]Cryptocurrency Statistics https://bitinfocharts.com/