報道関係者各位

新たなブロックチェーン基盤 BBc-1 (Beyond Blockchain One) Core v1.0 を公開

一般社団法人ビヨンドブロックチェーン

2018 年 5 月 23 日

デジタル通貨 Bitcoin を成立させるために発明され、「分散台帳技術 (Distributed Ledger Technology; 以下 DLT)」という概念の元となったブロックチェーン[1]は、マイニング[2]による改ざん困難性と、最も改ざんしにくい履歴[3]を全員が正史として採用するという「ナカモト・コンセンサス」により、通貨・証券をはじめとして、各種行政の手続きなど、社会の信用基盤をめぐって、中央の管理主体を不要とする新たな応用可能性の地平を拓いたことで評価に値します。しかし、この技術は、実時間性・秘匿性・スケーラビリティの課題や、暗号技術の危殆化への対応を含む、技術を進化させる上でのガバナンス上の課題、ネイティブ通貨の暴落による停止可能性など、さまざまな課題を未解決のまま持っています。一方、そうした課題を解決し、ビジネス応用に資するために開発されたはずの数々の DLT (多くはいわゆる「プライベートチェーン」と呼ばれる) は、そもそもブロックチェーンが達成していた改ざん困難性を失うなど、その存在意義すら疑われています。

一般社団法人ビヨンドブロックチェーン (東京都中央区) では、こうしたブロックチェーン技術を含む従来の DLT の諸々の課題を解決し、通貨やその他のフィンテック応用、各種証明機能といった社会信用基盤の自動化・高度化に寄与するべく、新たな基盤ソフトウェア[4]「BBc-1 (Beyond Blockchain One)」をオープンソースで開発して参りました。このたび、同ソフトウェアのうち DLT としての中核を成す BBc-1 Core の version 1.0 を発表・公開することになりましたのでお知らせいたします。

[1] 【ブロックチェーン】記録の内容や存在を誰にも否定できないように保存・維持し、その正当性を誰もが確認でき、また、正当な記録が投入されることを誰も妨げることができないことを目指した DLT。記録を集めたブロックを連鎖 (チェーン) させる構造を持つ。

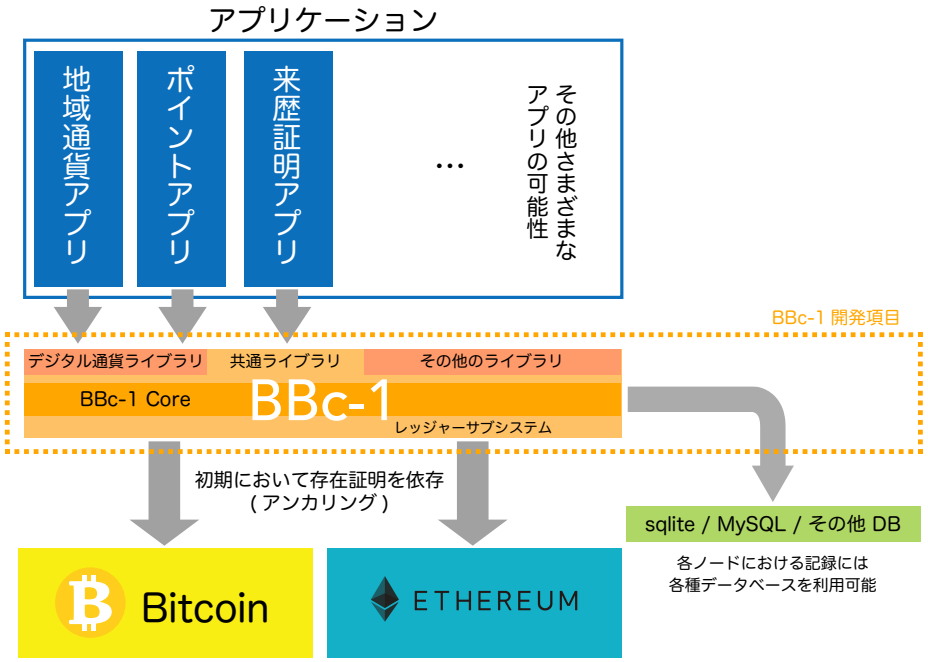
[2] 【マイニング】Proof of Work (作業証明) によって、数学的くじを当てるまでの作業のコストを払ったと証明できる者だけがブロックを生成するとともに新たなデジタル通貨の供給を受けられるという方式。生成されたブロックを改ざんするためには、同じだけのコストを払わなければならない。

[3] 【履歴】ブロックチェーンではマイニングの競争に勝ったと信じる者が自律的に履歴 (=チェーン) を形成していくため、頻繁に履歴が分岐する。ナカモト・コンセンサスでは、分岐した履歴のうち、最も改ざんしにくいもの (=作業証明に最も大きなコストが支払われているもの) を正しい履歴として採用する。

[4] 【基盤ソフトウェア】実際には BBc-1 ではトランザクション (送金やデータの更新などの不可逆的な操作) のデータ構造を含む通信プロトコル (通信規約) のみを定義します。そして当団体では、そのプロトコルを実装し検証可能にするための「参照ソフトウェア」を可読性の高い Python3 言語により開発しています。もちろんこのソフトウェアを実証実験や実運用に用いることが可能です。

BBc-1 Core とは？

BBc-1 (Beyond Blockchain One) は、ブロックチェーン技術を含む従来の DLT が持つ諸々の課題への長期的な解決策を用意し、かつ短期的に控える実証実験や、その後の実用化に至るまでのアプリケーション開発を支援するための新たな基盤ソフトウェアです (図 1)。このうち、BBc-1 Core は、DLT としての中核を成す部分で、次の特徴を持ちます。



- 初期には Bitcoin や Ethereum といった既存のブロックチェーンにアンカリング (証拠の埋め込み) をすることにより、トランザクションの証明機能を達成します。
- 中長期的には履歴交差[5]の考え方を応用した独自方式により達成します (機能は初期から提供します)。

図 1: BBc-1 のアーキテクチャ

1. 改ざん検知の機会が向上している。
2. システム上の「合意」を現実社会・実ビジネスのそれと一致させることができる。
3. 台帳における情報同士の関係性の記述力が高い。

これらの特徴のうち、2 (「合意」の考え方) と 3 (情報の記述力) については、ブロックチェーンを含む従来の DLT にはほとんど見られないものであり、BBc-1 のユニークな特徴となりますが、そのため他システムとの比較ができません。一方、1 (改ざん検知の機会向上) については、従来の技術から向上している面であり、以下にその内容を中心に、BBc-1 について従来の技術と比較しながら説明します。

[5] 【履歴交差】無関係なトランザクションやデータ同士の間に暗号学的ハッシュ関数やデジタル署名による連結を埋め込むことで、過去のトランザクションやデータの存在・非存在を証明する方式。

DLT の一般構造

DLT は「記録の内容や存在を誰にも否定できないように保存・維持し、その正当性を関わる誰もが確認でき、誰によっても運用を止められない」ことを目指す技術で、その構造は図 2 のように整理できます。

図 2: DLT の一般構造

図は、下から上に機能の階層が積み重なっている様子を示しており、各層で例として示されているのは Bitcoin のシステムにおける実現方法です。Bitcoin、その他のブロックチェーン、あるいはいわゆるプライベートチェーンに関わらず、DLT の機能を実現するためには、図のような構造が必要とされます。

履歴交差、および BBc-1 のその他の特徴

BBc-1 にて「存在性の証明」、すなわち、記録が改ざんされないことに基づいて、記録の存在・非存在の証明を行うことのために採用されているのが「履歴交差」です (図 3)。

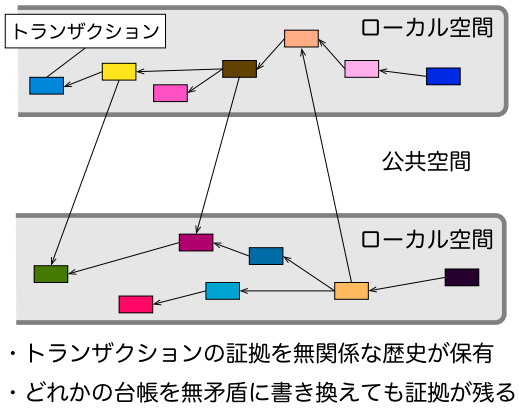


図 3: 履歴交差

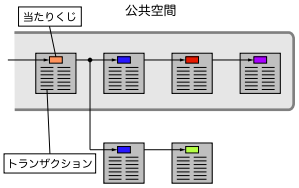
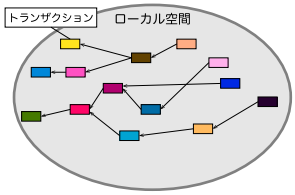
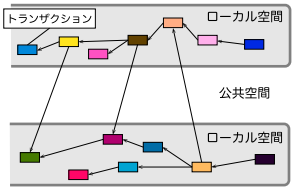
履歴交差は、一般に、無関係なトランザクションやデータ同士の間に互いの証拠を埋め込むことで、過去のトランザクションやデータの存在・非存在を証明する方式のことです。

BBc-1 では、この履歴交差を、プライベートに展開された台帳システム (ドメインと呼ばれます) 同士の間で実施し、トランザクションのダイジェスト[6]だけを持ち合うことで、情報を秘匿してプライベートな台帳を作りたいというビジネス上の要請と、公開性が無ければ存在性の証明が得られないという DLT の本質的要件を適合させた、ハイブリッドな設計 となっています。

また、BBc-1 では「唯一性の合意」の方法も特徴的です。BBc-1 には「サインリクエスト」という機構があり、合意が必要な (複数の) 相手のデジタル署名を収集した上でトランザクションをシステムに投入することができるようになっています。

DLT の比較

ブロックチェーン、プライベート DLT (いわゆるプライベートチェーン)、履歴交差に基づく BBc-1 の 3 種類の DLT を比較します。

プラットフォーム	Bitcoin, Ethereum 等	プライベート DLT 一般	BBc-1
メタファー	(民主的) 新聞モデル	社内報モデル	文献・古文書モデル
存在性の証明の方法 (抹消・捏造が不可)	作業証明 ; (コストで守る)	ない (内部無矛盾性)	履歴交差 (外部性で守る)
唯一性の合意の方法 (矛盾を解消する)	ナカモトコンセンサス (最大コストの歴史を選択)	冗長化された第三者 による分散合意	(冗長化された) 関係者 による (分散) 合意
イメージ	 ・作成時と同じだけくじを引かないと改変できない ・最もくじが引かれた歴史を有効とする	 ・トランザクションの関係と順序をローカルに表現 ・証明にはならない	 ・トランザクションの証拠を無関係な歴史が保有 ・どれかの台帳を無矛盾に書き換えても証拠が残る

- Ethereum は Ether のデポジットに応じた投票権 (Proof-of-Stake) による分散合意に舵を切ろうとしています。
  - それも (市場原理的) (民主的) 新聞モデルであり、コストで守ろうとしていることには変わりがありません。

(民主的) 新聞モデル　ブロックチェーンの「新聞モデル」(サトシ・ナカモトによる Bitcoin のオリジナルの設計文書にもブロックチェーンは「新聞の代わり」だと書いてあります) は、元々の考え方としては、公開され、広く共有されているデータが根拠になるため、改ざんができないというものでした。ただし、システムを「誰にも止めさせない」ためには、実際に新聞のようなサービスを誰かが提供するという風にはできず、参加する全員の力で「新聞のようなもの」を (民主的に) 作る、という考え方になっています。

そのために導入されたのが「作業証明」であり、記録するのに費やされたのと同じだけのコストを費やさなければ改ざんができず、より改ざんしにくくするために、より多くコストを払って記録された内容が正しい、という方式になっています。ここでは「広く共有されることで守る」という元々の考え方が「より多くのコストを払うことで守る」という考え方にすり替わっており、最近、日本発のデジタル通貨である Monacoin で発生した事

[6]【ダイジェスト】データに暗号学的ハッシュ関数を適用することにより得られる、256 ビットなどの決まった桁数の値で、元のデータが 1 ビットでも異なるとまったく別の値となり、ダイジェストから元のデータを推測できないという特徴を持つ。

件のように、多くの参加者がどう思うかに関わらず、多くのコストを払うことで歴史を書き換えることが可能になってしまっています。

社内報モデル　一方、プライベート DLT はいわば「社内報モデル」であり、権限を持つ内部者であれば台帳の書き換えが可能だと考えられるので、トランザクションの証明機能はそのままでは達成できません。

文献・古文書モデル　BBc-1 の「文献・古文書モデル」は、ちょうど古文書の存在を他の文献から参照されていることを以て確認していくように、特定の権威に依らず、独自に運用されているプライベート DLT 同士 (共謀していないという前提[7]) の間での記録の参照関係を利用して存在性を証明していくものです。

「コンセンサス」の考え方

ブロックチェーンを含む DLT を語るとき、何かと注目されるのが「合意 (コンセンサス)」の在り方です。DLT における「合意」は、生じうる矛盾を解消するためのものですが、ブロックチェーン、プライベート DLT 一般、BBc-1 では、それぞれ異なる意味を持っています。

ブロックチェーン　合意は全員参加であり、特に自発的な第三者としての検証者 (マイナー) が担っています。ブロックチェーンにおける合意の意味は、

- 「参加者の自律動作によって生じうる矛盾を解消する」ことであり、
- 自律動作によって 止まらない仕組みを達成 したことの後始末です。

プライベート DLT 一般　合意は任命された第三者としての検証者群により行われます。その意味は、

- 「主として故障により生じうる矛盾を解消する」ことであり、
- 耐障害性の実現 に向けた機構 (冗長化されたノードの状態を一致させる) です。

ここで、「耐障害性」はネットワークシステムにおいて長年研究されてきており、プライベート DLT に依らずとも、30 年以上の使用実績がある技術が存在することは特に申し添えておきましょう。

BBc-1　合意は関係者の間で取られます。特に責任者・債務者のデジタル署名が必要なようにアプリケーションを設計できます。その意味は、

- 「参加者の意思の不一致により生じうる矛盾を解消する」ことであり、
- 不利益の回避 と、システムの外で形成された合意の確認です。
- その上で、必要なら 耐障害性の実現 に向けた機構も持ちます。

[7]【共謀していないという前提】実際に共謀を困難にするため、BBc-1 の履歴交差は多数のドメイン間で実施される必要があります。まだ BBc-1 が広く利用されていない段階ではそのことの達成が難しく、そのため、既存のブロックチェーンへのアンカリングの機構を持ちます。

改ざんは防げるか → 改ざんは検知できるか、いつ検知するか

それでは、以上のような各種の DLT の特徴に基づいて、改ざんの困難性について見ていきましょう。

実は、ハードウェアによって書き込みから保護するのでなく、ソフトウェアシステムである限り、データの改変自体は可能です。ですので、大事なのは改ざんを検知できるか、そしていつ検知するかということになります。

従来のデータベースは、改ざんの機会を提供しないように、アクセス制御で守っていました。もし実際に侵入されたり、あるいは権限を持つ者による不当な書き換えが行われた場合は、ジャーナル (ログ) による検知に留まります。ログまで改変されていれば検知できません。

ブロックチェーンが、もし新しい考え方をもたらしたとすると、それは「データ同士を関連づけ、単純な改変では矛盾が生じるようにする」というものです。この場合、矛盾が残っていれば検知できますが、矛盾が残らないように改変されると検知できません。

それでは、ブロックチェーン (bitcoin の移転に用いる範囲内での Bitcoin、Bitcoin の応用システム、Ethereum)、プライベート DLT 一般、BBc-1 のそれぞれについて、記録が矛盾なく改変されるリスクを見てみましょう。

プラットフォーム	無矛盾に改変するコスト C	扱う価値 V	抑制条件 $C \geq V$	積極的検知
Bitcoin (基本)	マイニングコスト	bitcoin	成立	していない
Bitcoin (応用)		応用次第	不成立も可	
Ethereum	マイニングコスト	応用次第	不成立も可	していない
プライベート DLT 一般	見積もりにくい (比較的小)	応用次第	一般に不成立	していない？
BBc-1 (履歴交差)	見積もりにくい (極大)	応用次第	一般に成立	する

- 抑制条件 $C \geq V$ が不成立なら、合理的理由により無矛盾に改変され検知不可になり得る

ブロックチェーンの場合　ブロックチェーンは、無矛盾に改変されてしまうことから、マイニングのコストにより守られています。このコストは、ネイティブ通貨 (Bitcoin なら bitcoin、Ethereum なら Ether) の価格と均衡することが知られています。ネイティブ通貨の価格が相対的に高くなれば、マイナーが参入し競争が激化してコストが上昇し、ネイティブ通貨の価格が相対的に安くなれば、マイナーが撤退し競争が緩くなってコストが低下するからです。

このことから、bitcoin を取り扱う範囲での Bitcoin システムでは、マイニングコストをかけて bitcoin の価値を毀損することの合理的な理由がありません。

ところが、Bitcoin でも応用システムを作っていたり、Ethereum の場合については、マイニングコストを大きく上回る価値を扱う可能性が出てきます。その場合、その価値を毀損することによる利益が、マイニングコストを大きく上回るとすれば、実際にマイニングコストをかけて改ざんする合理的な理由があることになります。

プライベート DLT 一般の場合　プライベート DLT の場合は、改変のためには侵入が必要となり、コストが見積もりにくくなりますが、内部の管理者であれば無矛盾に改変するコストがゼロと考えられます。そのため、抑制条件は一般に不成立であり、合理的な理由で改ざんが行われるリスクを排除できません。

BBc-1 の場合　BBc-1 の場合も、改変のためには侵入が必要となり、コストが見積もりにくくなりますが、多くのドメインにおいて同時に内部の管理者であることはできず、容易な改ざんを可能にする条件を見つけることが極めて困難となります。そのため、抑制条件は一般に成立すると考えられ、表の中では唯一、応用システムにおいても合理的な理由により改ざんが行われるリスクを最小にできることになります。

ブロックチェーンの課題を乗り越える

BBc-1 では、以上のように改ざん困難性を担保したまま、従来のブロックチェーンが抱えていた問題を次のように解決します。

- 非実時間性 (確率的動作があり進行が読めない)

  ⇒ トランザクションの投入までに確率的動作が入らない

- 秘匿の困難性 (万人への検証可能性を担保すると秘匿できない)

  ⇒ ドメイン外へはトランザクションの内容を秘匿、内側でも暗号化可

- ワンネス (「分散」というより「複製」をしている)

  - スケーラビリティがない (全参加者が同じことをするのであれば参加者を増やしても性能が上がらない)

    ⇒ ドメインが増えることでスケールアップ、ドメイン内も将来的にスケール可能に

  - 進化のガバナンスが困難 (全員が一丸となる必要があるなら変われない)

    ⇒ ドメインごとの自治で新しいことを試せる (ドメイン内プロトコルは関知しない)

- インセンティブ不整合性

  - ネイティブ通貨の価値で支えられている (暴落するとすべての応用が止まる)

    ⇒ ネイティブ通貨は持たず、履歴交差は互助的に動作

むすび

BBc-1 は、ブロックチェーンハブ・コミュニティ[8]の優秀な研究開発者陣に恵まれ、17 年以上にわたる P2P・デジタル通貨の研究や、直近 4 年間のブロックチェーンの分析や実装の経験に裏付けられた、実用指向で確かな基盤技術と自負しております。

当非営利法人には、すでに大手メーカーを含む企業がメンバーとして参加し、地域ポイントから宇宙開発までをも含む、さまざまな応用に向けた検討と実証実験システムの開発が進行しております。ぜひ、多くの方々にご活用をご検討いただきたく、広く報道をいただければ幸いです。

GitHub URL　https://github.com/beyond-blockchain/bbc1
団体 URL　https://beyond-blockchain.org

[8] 株式会社ブロックチェーンハブ (https://www.blockchainhub.co.jp/) により創業が支援された各ベンチャー企業や、その活動に賛同する企業支援者、および開発者のコミュニティ。

団体概要	
名称：	一般社団法人ビヨンドブロックチェーン
形態：	非営利
目的:	従来のブロックチェーン技術がもつ諸々の課題を解決し、通貨や各種証明機能といった社会信用基盤の自動化・高度化に寄与する一連のビヨンドブロックチェーン技術の開発とその応用促進を通して、社会の様々な課題の解決に貢献すること。
設立：	2017 年 9 月
代表理事：	斉藤 賢爾
住所：	〒 103-0023 東京都中央区日本橋本町 4 丁目 8 番 16 号 千城ビル 5 階 BcH

お問い合わせ： pr@beyond-blockchain.org (担当： 斉藤)