

BBc-1 consensus consideration

revision 1

26 April 2019

本資料について

- BBc-1における「合意」とその意味について整理する
 - BBc-1が対象とする「合意」の考え方が理解できれば、BBc-1を利用しやすくなる
と期待している
 - パブリックブロックチェーンにおけるコンセンサスアルゴリズムとも対比する
- 作成日：2019/4/26
- 作成者：takeshi@quvox.net (t-kubo@zettant.com)

目次

| タイトル | ページ |
|--------------|-----|
| 合意とは何か | 4 |
| コンセンサスアルゴリズム | 8 |
| ビットコインにおける合意 | 16 |
| 誰と合意すべきか | 21 |

合意とは何か

「合意」とは何か

- 登録しようとする情報（トランザクション）に対して「間違いや偽りがないこと」を**確認し承認すること**
 - **情報＝取引契約**だった場合、取引内容に偽りがあれば、**当事者が損失を被るため、承認すべきではない**
 - **情報＝存在を表すもの**だった場合、**ある時点でその情報が確かにその形で存在していた**ことを承認しておくことで、存在証明が可能になる

「誰が」 合意に参加すべきか

- 下記いずれかのパターン
 - 登録する情報（トランザクション）が正しいものでなければ損失を被る可能性がある人
 - 登録する情報（トランザクション）が正しいものであることを主張したい人
- 正しいものでなければ損失を被る可能性がある人
 - 情報＝契約の場合、契約の当事者（2者またはそれ以上）は、契約内容に間違いや偽りがあると損失を被る可能性があるので、しっかり確認してその内容を承認する必要がある
- 登録する情報（トランザクション）が正しいものであることを主張したい人
 - 情報＝存在を表すものの場合、その情報の所有者や、存在証明をサービスとして提供する人が、「確かにそれは存在していた」と主張するために、その情報を承認する

何をもって合意とするか

- 情報（トランザクション）に署名を付与すれば、署名した本人はその情報を承認したこととする
 - 署名するために必要な「秘密鍵」は本人しか持ちえず、他人が勝手になりすまして署名されることはないため、「間違いなくその人が承認した」ことになる
 - したがって、承認できない内容であれば、絶対に署名を付与してはならない

BBc-1はこの意味の合意のみを取り扱う

コンセンサスアルゴリズム

コンセンサスアルゴリズムとは何か

- ほとんどのブロックチェーンプラットフォームには、コンセンサスアルゴリズム（合意アルゴリズム）が搭載されている
- コンセンサスアルゴリズム
 - システムに参加する複数のノード(=サーバ)間で状態を一致させるための方法
 - つまり、分散システムを動かす際に必要なアルゴリズム
- 状態は「情報」と読み替えられる
 - つまり、「システムに参加する複数のサーバ間で同じ情報を保持するための方法」

なぜコンセンサスアルゴリズムが必要か

- 複数のノードから構成されるシステム（＝分散システム）に様々な障害が起これと、「同じ情報を保持する」ことが実現困難になる
- 起こりうる障害に何らかの想定をおいて、それを克服する方法を考えた
 - それがコンセンサスアルゴリズム

想定する障害とは

- 最も難しい障害＝ビザンチン障害
 - ノードが急にダウンするかもしれないし、急に復旧するかもしれない
 - しかも、ノードは嘘をつくかもしれない（嘘の情報を流す）
- 次に難しい障害＝クラッシュ＆リカバリー障害
 - ノードが急にダウンするかもしれないし、急に復旧するかもしれない
- ビザンチン障害を対象としたコンセンサスアルゴリズム
 - BFT (Byzantine Fault Tolerant) と呼ばれるものたち（PBFTなど）
 - PoWやPoSは正確に言えばコンセンサスアルゴリズムには分類されないが目的は似ている
- クラッシュ＆リカバリー障害を対象としたコンセンサスアルゴリズム
 - PAXOS、RAFTなど

どの障害を想定すべきか

- パブリックブロックチェーン
 - 「何が起こるかわからない」という最も厳しい障害であるビザンチン障害を想定しておいたほうが良さそう
- プライベート/コンソーシアム型のブロックチェーン
 - 「嘘をつくかもしれない」というビザンチン障害の想定は本当に必要なのか？
 - 例えば、ビジネス上の契約で罰則を設けるなどすれば排除できるのではないか？
 - そもそも、嘘をつけるのか？

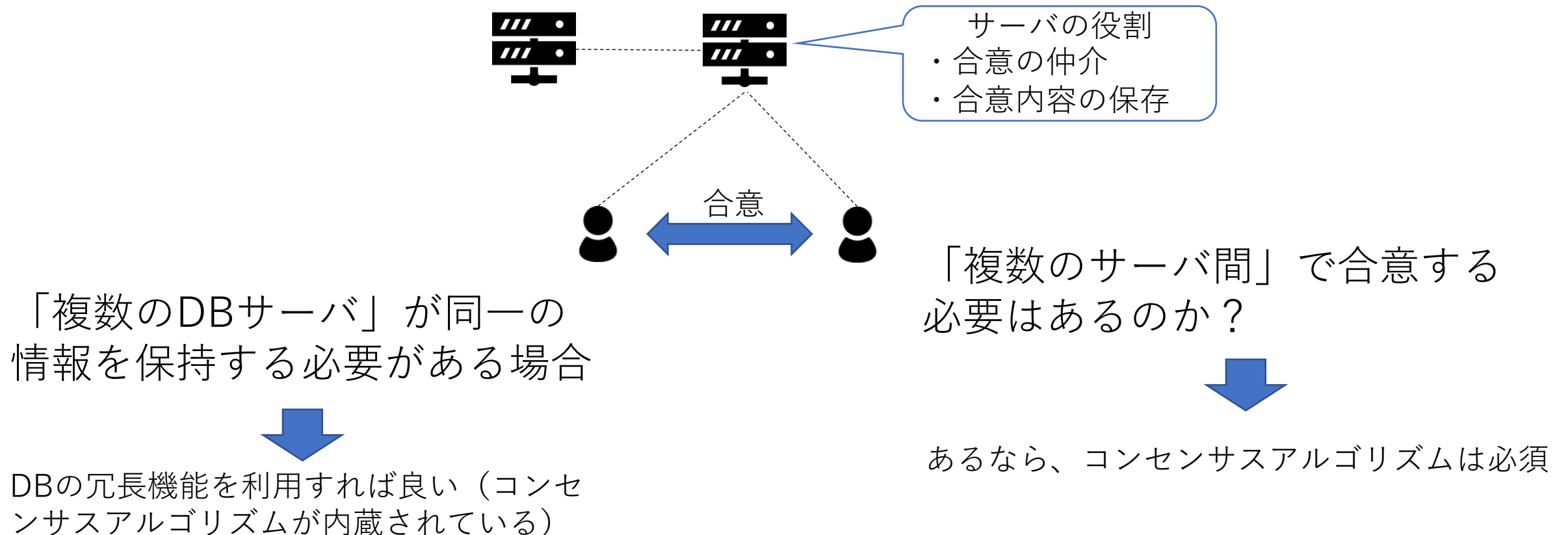
本資料5ページに記載した「合意すべき内容」
を精査する必要がある

なぜコンセンサスアルゴリズムが必要なのかをもう一度考える

- システムに参加する複数のサーバ間で同じ情報を保持するために必要
 - 本資料9ページを再掲
- 上の文章の「情報」という言葉は、どんな情報かについては一切言及していない
 - ビジネスで合意（本資料5ページの意味）された情報かどうかは実は関係ない
- ビジネスでの合意に「複数のサーバ」がどれだけ関与しなければならないのかをしっかりと考える必要がある
 - コンセンサスアルゴリズムは、分散システムを正しく動かすための仕組みだが、「ビジネスでの合意をどのように取り扱えばいいか」ということとは関係がない

ユーザの合意とサーバの関係

- 通常、合意はユーザ同士で行えば良いはず（サーバが合意するわけではない）



結論

- 複数のサーバ自身が「合意」に関わる必要がある場合
 - ビジネス上の合意を実現するためのプロセスの中にコンセンサスアルゴリズムが必要
- 複数のサーバは、合意された結果（＝情報）を冗長保管しておけば良い場合
 - DBの冗長機能を利用すれば良く、ビジネス上の合意を実現するためのプロセスにはコンセンサスアルゴリズムを含める必要はない
 - いらない機能を含めると、システムのパフォーマンスが落ち、不具合の温床になる

ビットコインにおける合意

ビットコインでは何を合意しているか

- ビットコインシステムでは2段階の合意が行われている
- 第1段階（トランザクション）
 - AさんからBさんへの支払い（トランザクション）について合意する
 - UTXO構造なのでAさんの署名がトランザクションに付与されるが、履歴を辿れるので、本質的にはAさんとBさん二人の署名が付与されていることと同等である
- 第2段階（ブロック）
 - 2重支払いや、残高不足などの不正が無いことを参加者全員で確認し、合意する
 - マイナー自身への報酬を与え、PoW（Proof of Work）を導入することで、不正のないブロックを作ることにインセンティブを与えている

ビットコインでは何を合意しているか

- ビットコインシステムでは2段階の合意が行われている

2者間の合意

- 第1段階（トランザクション）
 - AさんからBさんへの支払い（トランザクション）について合意する
 - UTXO構造なのでAさんの署名がトランザクションに付与されるが、履歴を辿れるので、本質的にはAさんとBさん二人の署名が付与されていることと同等である
- 第2段階（ブロック）
 - 2重支払いや、残高不足などの不正が無いことを参加者全員で確認し、合意する
 - マイナー自身への報酬を与え、PoW（Proof of Work）を導入することで、不正のないブロックを作ることにインセンティブを与えている

分散システム全体での合意

2種類の合意

- 合意とは（5ページの再掲）
 - 登録しようとする情報（トランザクション）に対して「間違いや偽りがないこと」を確認し承認すること
 - 情報＝取引契約だった場合、取引内容に偽りがあれば、当事者が損失を被るため、承認すべきではない
 - 情報＝存在を表すものだった場合、ある時点でその情報が確かにその形で存在していたことを承認しておくことで、存在証明が可能になる
- 2人または数人での合意
 - 当事者同士が、その取引が正しいことを確認し承認する
 - その当事者が誰も損しないようにする
- 参加者全員での合意
 - 当事者が参加者全員で、その内容が正しいことを全員で確認する
 - 資産総額が偽られることで実質的な価値が減少し、参加者が結果として損をすることがないようにする

ビットコインの資産総額と価値毀損

- 例えば全部で100BTCしか発行されていない状態を考える
 - 1BTC = 60万円とする
 - 資産総額は $100 \times 60\text{万} = 6000\text{万円}$
 - マイニングによる増加は考えない（10分間の間だけの話だと思えば良い）
 - Xさんが3BTCもっていたとする（ $3 \times 60 = 180\text{万円}$ ）
- もし、だれかの2重消費が認められたら
 - Aさん → Bさん 20BTC（2重消費＝Aが勝手に20BTC発行したのと同じこと）
 - 発行量が急に20BTC増加して、総発行量120BTCになってしまう
 - 実質的価値は急には変わらないので、資産総額は6000万円のまま
 - $6000\text{万} \div 120 = 50\text{万円}$
 - つまり、実質的価値が 1BTC = 50万円に減少してしまう
 - Xさんの資産価値は $3 \times 50 = 150\text{万円}$ なので、何もしていないのに30万円損した！

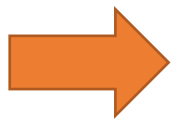
誰と合意すべきか

例：参加者全員で共有する資産（トークン）

- 価値をみんなで共有する資産（トークン）は、資産総額が重要になる
 - 各参加者は、その一部を保有する
- 一部の参加者の不正により、資産総額が不当に毀損されることは、その他大勢の参加者に損害を与える
- 資産総額が毀損されたときに、実際誰が損をするのか
 - パブリックブロックチェーンの場合
 - トークンの発行主体が存在しない（システム全体が発行主体）ので、参加者が損失を被る
 - プライベート/コンソーシアムブロックチェーンの場合
 - 通常はトークンの発行主体が存在し、発行主が法定通貨などを引当て、実質的価値を与える
 - したがって、資産総額が既存された場合に損失を被るのはトークンの発行主体になる

例：参加者全員で共有する資産（トークン）

- パブリックブロックチェーンの場合
 - トークンの発行主体が存在しない（システム全体が発行主体）ので、参加者が損失を被る



ビットコインのように2段階の合意を行う必要がある
（2段目は参加者全員の合意）

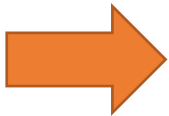
- プライベート/コンソーシアムブロックチェーンの場合
 - 通常はトークンの発行主体が存在し、発行主が法定通貨などを引当て、実質的価値を与える
 - したがって、資産総額が既存された場合に損失を被るのはトークンの発行主体になる



トークン取引の当事者（AさんとBさん）のやり取りを
発行主体も確認し、承認すればよい


例：参加者全員で共有する資産（トークン）

- パブリックブロックチェーンの場合
 - トークンの発行主体が存在しない（システム全体が発行主体）ので、参加者が損失を被る

 ビットコインのように2段階の合意を行う必要がある
(2段目は参加者全員の合意)

- プライベート/コンソーシアムブロックチェーンの場合
 - 通常はトークンの発行主体が存在し、発行主が法定通貨などを引当てを与える
 - したがって、資産総額が既存された場合に損失を被るのはトークンの所有者

AとBと発行主体の署名
をトランザクションに
付与するだけで良い

 トークン取引の当事者（AさんとBさん）のやり取りを
発行主体も確認し、承認すればよい

結論

- 誰が合意すべきか（取引を承認すべきか）を精査する必要がある
 - 何でもかんでも分散システムの合意を考えればいいというものではない
 - さらにいえば、コンセンサスアルゴリズムの必要性も検証したほうが良い
- 間違いや偽りがあった場合に「誰が損をするか」を明らかにし、その人達が合意（＝承認）すればいい
 - 承認の証が電子署名である

以上