特集　不動産テックの動向

スマートコントラクトによる土地売買を考える

慶應義塾大学 SFC 研究所 上席所員　斉藤　賢爾
さいとう　けんじ

1 はじめに

「スマートコントラクト(smart contract)」は、広い意味では「契約を機械で実装する仕組み、また、そのようにして実装された契約」と考えることができる。ただし、現時点で実際に可能なのは「デジタルに表現される資産を予め定められたルールに従って自動的に移転させる」ことに過ぎず、また、そのことすら実現上の課題が多い。

筆者は計算機科学、インターネットおよびそれらの社会応用を専門としており、土地や法曹の専門家ではないが、昨今話題となっているビットコインをはじめとする「デジタル通貨(digital currency)」や、「分散台帳(distributed ledger)」としての「ブロックチェーン(blockchain)」といった技術に長らく関わっており、その可能性および不可能性(現状の技術では実際にはできないこと)の啓蒙に携わってきた。

本稿では、土地に対する権利がデジタル資産として表現されることと、支払の手段としてデジタル通貨が用いられることを前提として、単純なモデルに沿って土地売買のエスクローサービスを自動化しうることを示すが、技術的・社会的な課題が多く、即、そのような世界が訪れることを喧伝するものではない。しかし、おそらく遅くとも 10 年、20 年といったスパンで諸々の課題は解決できると見込んでおり、こうした自動化が土地の取り扱いに及ぼす影響について今から想定しておくことには意味があると考えている。

2 ブロックチェーンを理解する

現状、スマートコントラクトはブロックチェーンの応用技術のひとつとして捉えられている。そこで、まずはブロックチェーンについて簡単に理解するところから始めたい。

あらゆる技術は、特定の問い(要求)に対する答えである。したがって、ある技術を理解するためには、まずその問いを理解する必要がある。ブロックチェーンが生まれるきっかけとなったビットコインの「問い」は、「自分が持っているお金をいつでも自分の好きに送金することを誰にも止めさせないためには？」というもの[1]であり、その他のブロックチェーンや分散台帳技術一般にも適用可能なように汎用化すると、「アセット(資産)の制御の権限を中央ではなくエンド(端点)が持つには？」となる。

図 1 は、そうした問いに応える技術としてのブロックチェーンや分散台帳技術を理解するために、その機能を階層構造として整理したものである。個々の機能は特定の技術により実現されるが、今の時点で個別の技術に着目してしまうと、現状では技術的な課題が多く、技術の変化が見込まれるだけに、本質を見失うことになりかねない。まず

[1] ビットコインの匿名の設計者であるサトシ・ナカモトの論文では明記されていないが、分散台帳技術のひとつである R3 Corda の開発者による整理。
http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

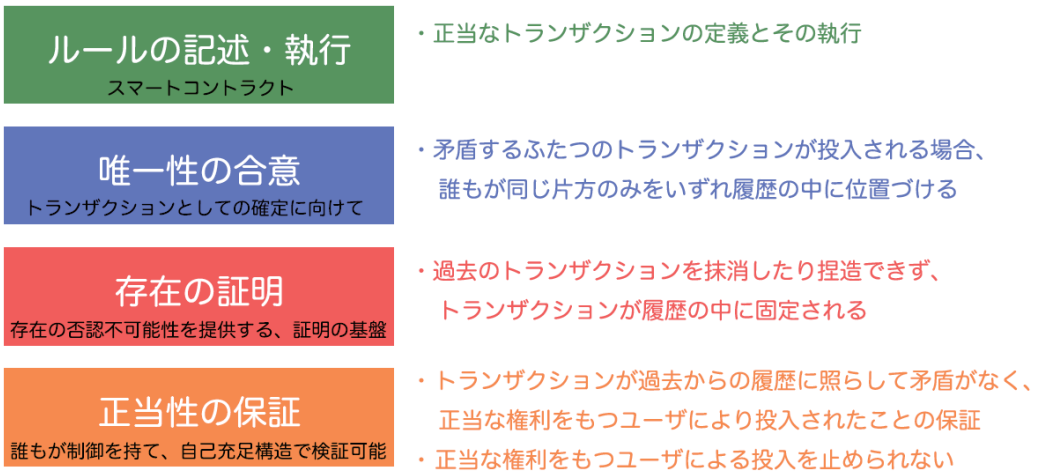

図 1: ブロックチェーン/分散台帳の機能の階層構造

は、図 1 のようなレベルで理解をしておくことが肝要だと筆者は考えている。

2.1 正当性の保証

正当性の保証は、システムに投入されたトランザクション(取引)またはレコード(記録)がルールに基づいて改ざん不可能なかたちで記述されており、過去の履歴と矛盾しないことを保証する機能である。また、そうしたトランザクションないしレコードが、正当な権限をもつユーザにより投入されたことを保証し、かつ、正当な権限をもつユーザによる投入が誰にも妨げられないことを保証する。

一般に、ブロックチェーンや分散台帳では、「デジタル署名(digital signature)」により、本人性(すなわち、正当な権限を持つ本人であるか)の確認と記述内容の否認不可能性が提供される。署名の検証を第三者が行う場合は、取引や記録のデータの中に公開鍵を埋め込んだり、あるいは何らかの PKI(公開鍵インフラストラクチャー)[2]を用いる必要がある。

2.2 存在の証明

存在の証明は、トランザクションやレコードの存在の否認不可能性を提供する機能である。過去に遡って、存在した取引や記録の証拠を抹消したり、あるいは存在しなかった取引や記録の証拠を捏造できない仕組みを提供する。

内容の否認不可能性は前述のようにデジタル署名によってもたらされるが、それでも「この時刻に存在した」あるいは「このイベントの前/後に存在した」ということは、原理的に否認できる。デジタル署名には時刻の概念がないからである。デジタル署名の対象を(相対)時間の中に位置づけるこの機能は、タイムスタンプサービスと関係が深い。

取引の当事者であれば、メッセージのやり取りの履歴の中にトランザクションやレコードの受信を位置づけることができるため、この機能を明示的に必要としない場合を考えることもできる(不要ではない)。

2.3 唯一性の合意

唯一性の合意は、トランザクションやレコードがユニーク(唯一)であること、すなわち、アセットに関わる履歴が分岐せず、単一のタイムラインを刻んでいることに参加者が合意するための機能である。

自律分散環境では、アセットの履歴の見え方が参加者によって異なる場合も発生し得るため、例えばアセットの二重消費が起きていないことを保証する等の目的でこうした機能が必要になる。

[2] 公開鍵の正当性を担保するための技術的・社会的な機構。

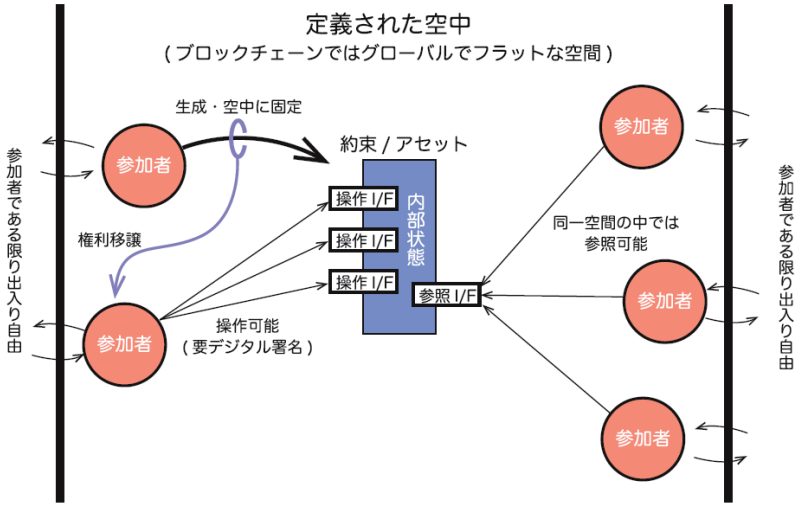

図 2：空中約束固定装置

ただし、例えばクリエイティブコモンズのライセンスにもとづくデータの頒布の記録など、この機能の必要がない場合を考えることもできる。

2.4 ルールの記述・執行

ルールの記述・執行は、正当性を確認するためのルールや自動処理の記述・エンフォースメントおよびその実行を提供する機能である。

ブロックチェーンや分散台帳の文脈では、この機能により記述されたルールがスマートコントラクトと呼ばれると整理できる。

ブロックチェーンや分散台帳が実世界とどうリンクできるかについて課題が山積している現状、スマートコントラクトでできることは、デジタルに表現されるアセットをあらかじめ定められたルールに従って移転したり、その状態を変化させたりすることくらいであるが、言わばアプリケーション層となるこの層は社会への影響と直接繋がる部分であり、今後特に重要になると考えられる。

2.5 空中約束固定装置

以上のような構造を持つことで、ブロックチェーンや分散台帳は、言わば「空中に約束を固定する装置」として機能する。ビットコインで言えば、約束とは「コインが宛てられた本人だと証明できる者だけが、そのコインを他の誰かに送金できる」というものである。約束（の証拠）がどの主体にも独占的に保有されず、空中で維持されていることにより、エンドが権限を持つことを保証でき、かつ、常時ネットワークに接続しているわけではなく間欠的にシステムに参加するような主体にも対応できる。

その様子を表したのが図 2 である（I/F はインタフェースを示す）。

以降、ブロックチェーンや分散台帳のこの性質に言及する際は、「空中約束固定装置」という用語を用いる。

日本銀行総裁は、2016 年 8 月の第 1 回 FinTech フォーラムの冒頭での挨拶[3]で、『「ブロックチェーン」や「分散型元帳」は、「帳簿は特定の主体が管理するもの」という従来の考え方を大きく変えるものです。金融の発展自体が帳簿というインフラに支えられてきたことを踏まえれば、帳簿の革新は、金融の形態にも大きな変化をもたらす可能性があります』と述べている。しかし、その監査可能性や、権限を持つ主体による運用の自律性を考えるなら、帳簿は本来的に空中に置かれるべきものである。

空中約束固定装置は、特に公共財に関して、その制御権を公正に運用することに適している。社

[3] https://www.boj.or.jp/announcements/press/koen_2016/ko160823a.htm/

会に影響力を持ちうるその最初の実装(ビットコインブロックチェーン)が、貨幣という公共財の分野に登場したことは象徴的だと言える。

3 ブロックチェーンへの期待と課題

ここで、ブロックチェーンや分散台帳の期待される応用について述べ、ブロックチェーンが抱える技術とガバナンスの諸問題を明らかにしておきたい。そうした諸問題は技術の成り立ちに大きく依存するので、ここではビットコインに代表される狭い意味でのブロックチェーンについて課題を述べていくが、そうした諸問題を解決していく取り組みは現在進行形で進んでおり、一般に分散台帳が同様な問題を抱えるわけではないことをここで明記しておく。

3.1 期待されている応用

ブロックチェーンや分散台帳は、金融アセットの直接取引や、企業の株式分割、減資・併合、株式移転・交換、合併、第三者割当増資など、また、サプライチェーン管理、マスターデータ管理、そしてシェアリングエコノミーや IoT(Internet of Things)への応用が特に取り沙汰されている。

前述のように、空中約束固定装置は、特に公共財に関して、その制御権を公正に運用することに適していることから、各参加者が私有する財を共有し、半ば公共財のようにして扱うことを可能にするシェアリングエコノミーが、ブロックチェーンの応用可能性のひとつとして挙げられること自体は頷ける。

3.2 実時間性・秘匿性の課題

しかし、ビットコインの流れを汲むブロックチェーンには、その動作が確率に基づいており、実時間で進行する現実と同期しにくいという問題がある。

また、任意の第三者に対してトランザクションやレコードの検証可能性が開かれているとすれば、それはすなわち一般公衆によるデータのアクセスを可能にしているということであり、秘匿性が要求される応用にはそのままのかたちでは適用できないという問題もある。

3.3 スケーラビリティの課題

実時間性や秘匿性の欠如に次ぐ技術的な課題の代表例としては、システムがスケールアウトしない、すなわち、参加するコンピュータを追加することでは性能上の問題を解決できないという課題がある[4]。

ブロックチェーンでは、その全機能を有する参加者の各々がブロックチェーンのデータ全体を処理するため、時間当たりのトランザクション数の増加に伴い、データ構造を維持するためのコストが直線的に上昇してしまう。このことにより、例えばスマートシティのような、大規模に成長しうるシステムの中核に据えるには懸念がある。

3.4 ワンネスの罠とガバナンスの課題

ブロックチェーンは、大規模災害や政変などによりネットワークが分断されると、チェーン(履歴)が安定的に分岐することになり、唯一の正しい履歴が保たれるという大前提が崩れ、正しく動作しない。「世界がひとつ」でなければ動作しないというこの性質を、以降は「ワンネス(oneness)」と呼称する。

ブロックチェーンは、分散システムあるいは非集中システムと言われることもあるが、実際には「ワンネス」は「分散」の考え方と真っ向から対立する。ブロックチェーンは、分散というよりはむしろ「複製」の技術なのである。

そのことがもたらす重要な帰結は、技術を進化させるガバナンスが利きにくいということである。ブロックチェーンでは、インターネットのその他のアプリケーションでは普通に行われている、「一部で違うことを試して、うまくいったら全体で採用する」ということができない。一部が異なる仕

[4] 対して、一般に大規模な分散システムは、要求が増え、システムの処理が追いつかなくなる怖れに対しては、コンピュータを追加して1台当たりの負荷を軽減することで対応できるように設計されている。

様で動くと履歴が分岐してしまうからである。すると、現実への適用性を実地で評価しながら技術を進化させていくことが困難になる。めまぐるしく変化する技術的・社会的状況の中で、実際に使われていく技術を維持していくためには、この困難性は致命的となる。

この困難性は、例えば、一度ブロックチェーン上に展開されたスマートコントラクトのコードを修正できないというかたちでも浮上しうる(もちろん､そのように設計しないことも可能であるが、スマートコントラクトの基盤として広く知られている「イーサリアム(Ethereum)」では、現状そうなっている)。ソフトウェアは､改善が可能な状態に置かれるべきであり、開発者の権限を不当に制限するそのような設計は決して望ましくはない。

3.5 インセンティブ不整合性

ブロックチェーンは、その各々のシステムの中核を成す「ネイティブ通貨」(例えばビットコインであればBTC)によって報酬を受け取る「マイナー(miner)」により維持される。従って、仮にマイナーが大規模に撤退すると､停止するおそれがある。

マイナーは、トランザクションやレコードを格納するブロックという構造を生成することにより報酬を得ている。ブロックの生成にはコストがかかるため、報酬として得られる通貨の価格が下落し、投入するコストに見合わなくなると、撤退という選択肢が現実的となる。

このことがもたらす帰結は、ビットコインの場合､「ビットコインの価格が下落する⇒ビットコインブロックチェーンが停止する」である。したがって、この設計は素のビットコインに関してはインセンティブ整合的と言える。

しかし、ブロックチェーンの上で、スマートコントラクトとして様々なアプリケーションが動作している場合はこの限りではなく､「ブロックチェーンのネイティブ通貨の価格が下落する⇒その上のアプリケーションすべてが停止する」となるため、このインセンティブ設計はブロックチェーンを汎用のアプリケーション基盤として見た場合に不整合的である。

4 スマートコントラクトによる土地の売買

以上のように、分散台帳、特にブロックチェーンには様々な課題があることを踏まえた上で、スマートコントラクトによって土地の売買を行うことの可能性について検証してみよう。

4.1 解くべき問題

現状、土地の売買では、典型的には銀行の一室に、売主、買主、不動産会社、司法書士、銀行員の５者が一同に集まることで初めて決済が実行されることになる。そのことの背景には、意思確認の効率化と、契約不履行による様々なリスクを避けるためといった理由があると考えられる。

契約不履行によるリスクとは、例えば売主が土地の代金を受け取ったのにその権利を移譲しなかったり、逆に買主が土地の権利を移譲してもらったのに代金を払わなかったりすることだと想像する。これは一般に商取引において考慮すべきリスクである。しかし、特に商品が高額となる土地売買においては、概念的にはアトミック(不分割)な手続きとして売りと買いを同時に実施する必要がある。

仮に、意思確認とリスク回避の手段としてスマートコントラクトを用い、売主と買主だけが参加するオンラインの空間で、双方が同時にアクセスする必要すらない中で売買を成立させることができるなら、取引コストや利便性の面で、ひとつの大きな改善になると考えられる。

そしてそれが可能であることは、単純化したモデルを用いて実証的に確認できる。

4.2 単純化したモデルによる解

単純化したモデルによる、スマートコントラクトを用いた土地売買の仕組みを図３に簡単に示した。このモデルでは、売主が土地の権利を、買主が土地の代金を、それぞれ自動化された売買契約のスマートコントラクトに預託し、双方が揃った状態でのみ売買を実行する。

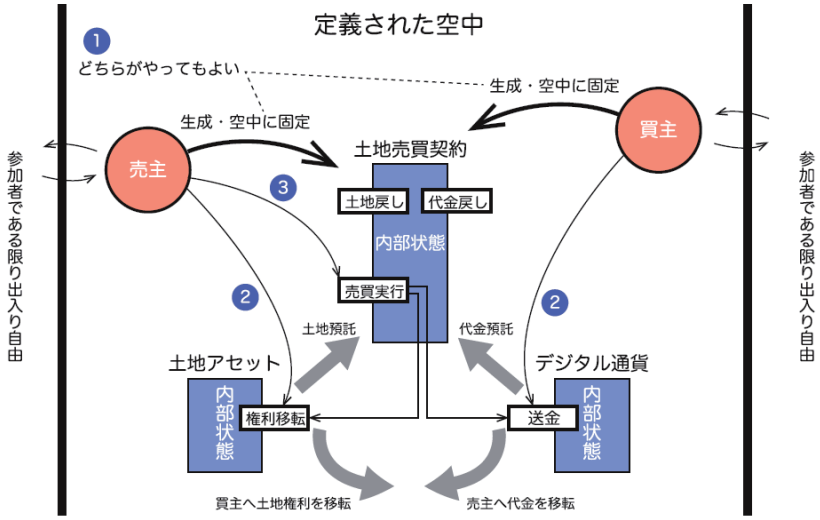

図 3：自動エスクローによる土地売買

このモデルでは以下の 3 つのコントラクトが売主と買主の指示にもとづいて動作する。

デジタル通貨：通貨システムを簡単に実現したものであり、システムの参加者それぞれが通貨残高をもち、参加者間で、送金元が所持する任意の量を送金先に送る「送金」のインタフェースを持つ。

土地アセット：土地の権利をデジタル資産として表現したものであり、内部状態として「権利者」をもつ。権利者が権利を他の参加者に移転するための「権利移転」のインタフェースを持つ。

土地売買契約：土地売買の仲介者をデジタルに表現したものであり、指定された土地アセットの権利と、その代金として支払われる通貨の量をそれぞれ預かることができる（その意味で、このコントラクトは参加者と同様にシステム内にアカウントを持つ）。取引が正常に進行しない場合（どちらかが預託すべきものを預託していない場合）に、売主が土地の権利を取り戻すための「土地戻し」、買主が代金を取り戻すための「代金戻し」の各インタフェースを持つ。また、両方が預託されている場合に限って土地の権利を買主に、代金を売主に渡す「売買実行」のインタフェースを持つ。

このコントラクトは、自らがシステムの参加者として、各機能の実現のために「デジタル通貨」および「土地アセット」のインタフェースを利用する。

この仕組みは、実際に筆者がプログラマ向けにイーサリアムにおけるプログラミングを体験してもらうために各所で実施している「スマートコントラクトプログラミング」の講義にて、最終課題として出題している例題でもあり、概ね 30 分程度で書ける簡単なコードで実際に記述し、動かすことができる。

4.3 解の特長と課題

この解の特長は、人間としてシステムに参加しているのが売主と買主という当事者だけであり、他の機能は自動化されているという点にある。

ただし、自動化とは言え、コンピュータのプログラムとして実行される以上、当該コンピュータを資源として提供する主体が必要であり、システム全体がまったく売主と買主の 2 者だけによって動いているというわけではない。イーサリアムでは、ブロックチェーン自体の動作がそうであるように、コントラクトを実行する特定の主体はいないが、大勢が同じコードを実行することによって、あたかもコントラクトが空中で自動的に実行され

ているかのようなイリュージョン(幻想)を生み出している。

課題としては、もちろん、これがあくまで極めて単純化されたモデルであるという点は無視してはならない。しかし、現実により即して適合するようにモデルを複雑化することは、基本的にはそのようにコントラクトのコードを記述すればよいことなので、本質的な問題とは言えないのではないかと筆者は考えている。

むしろ、単純化していることにより見えてくる、この仕組み自体が持っている課題を注視すべきだろう。そうした意味での課題のひとつは、コードを実行している大勢が必ずしも均質であることが保証されず、より強力な権限をもつ誰かの意図により実行を妨害されてしまう恐れがある、ということである。

実際に、イーサリアムでは、過去にネイティブ通貨の大量の盗難事件が起きた際に、開発コミュニティやマイナーたちといった、プラットフォームを提供する側の意思によって、事件そのものが無かったことにされたという経緯がある[5]。犯罪者の権利をどこまで認めるかという議論はありうるかも知れないが、そもそも誰が犯罪者であるかを決める権利がプラットフォームにあるかどうかということも含めて、こうした対応が可能であること自体が公正性の面で問題となりうる。

5 おわりに

本稿では、スマートコントラクトによる土地売買について、簡単なモデルによる仕組みを紹介することを通して考えた。

中盤で紹介したように、ブロックチェーン技術に関する課題は山積している。しかし、筆者はそうした課題は必ず解決されると信じている(その過程で「ブロックチェーン」という特定の技術は捨てることになるかも知れないが、新しい技術により、ブロックチェーンが目指したものが実際に実現できると考えている)。

本稿では、簡易な例であるものの、従来は売主、買主、不動産会社、司法書士、銀行員の5者が必要だった土地売買の取引について、そのほとんどの部分が自動化され、売主と買主という当事者たちだけによって取引が実行されうる可能性を示した。

そうした自動化が現実になる近い未来、土地登記、銀行、不動産仲介、といった役割の存在意義が改めて問われることになるだろう。筆者には、ブロックチェーン技術のようなデジタル技術の発展の行く末に、私たち一人ひとりが、本当は何をしたいのかが問われる時代が訪れるように思えてならない。

[5] 「THE DAO 事件」で検索されたい。