卒業論文 2016 年度 (平成 28 年)

3D プリントにおける Blockchain を用いた製造情報管理システム

慶應義塾大学 総合政策学部
阿部 涼介

卒業論文要旨 - 2016 年度 (平成 28 年度)

3D プリントにおける Blockchain を用いた製造情報管理システム

近年，デジタルファブリケーションと呼ばれるデジタル工作機器を用いたものづくりが急速に普及している．既存のメーカによる大量集中生産とは異なり，各個人が分散的に少量の製造を行う流れもできつつある．設計図となる 3D モデルは，個人で作成したものや，インターネット上で公開されたものを複製または改変したものが利用されている．

しかしながら，製造物の設計図や製造者などの情報を保存しなければ製造責任や知的財産権の所在を明らかにすることは難しい．製造責任や知的財産権の所在を明らかにするには，誰でもデータを参照できるという “公開性”，製造物に紐づけられた情報の “追跡可能性”，また製造以降不正に改ざんがされていない “完全性 ” が必要とされる．藤吉らにより，製造物の管理のために RFID を製造物に埋め込むことで，情報と製造物を紐付けることは達成されたが，未だ上記の問題は未解決である．

そこで本研究では，Blockchain 技術を用い，公開台帳上に製造情報を保存することで必要条件を満たし，製造責任や知的財産権の所在を明らかにすることができるのではないかと考えた．Blockchain 技術は，P2P ネットワーク上で分散的に公開台帳を形成し，入力データの検証を相互に行い保存することでデータの完全性を担保するシステムである．

本手法を検証するために，シングルボードコンピュータで 3D プリンタの制御を行い，Blockchain ノードとすることで，Blockchain 上に製造情報を保存する実装を行った．この実装を用いて，上記の “公開性”，“追跡可能性”，“完全性” の各項目において検証を行った．これにより，本実験システムでは製造物の製造情報の追跡と，製造者自身が設計図の製作者である場合の製造責任や知的財産権の所在を明らかにすることができる．

本研究の成果により，個人的な製造でも製造責任や権利の所在を明らかにすることができる．このシステムは，製造者にとっては責任が追及される事故が起こらないような質で製造を行わないためのディスインセンティブとなる．また，本手法を応用して Blockchain 上で設計図の流通も管理することで，3D プリンタで製造された製造物を知的財産として管理することができる．

キーワード:
1. デジタルファブリケーション, 2. 3D プリント, 3. 製造責任, 4. 知的財産権, 5. Blockchain

慶應義塾大学 総合政策学部
阿部 涼介

Abstract of Bachelor's Thesis - Academic Year 2016

Manufacturing information management system using Blockchain in 3D printing

In recent years, manufacturing using digital machine tools called digital fabrication has spread rapidly. Unlike concentrated mass production by existing manufacturers, a flaw in which each individual produces a small amount in a dispersed manner is also being developed. The 3D model to be the design drawing is used by those made by individuals or those made by duplicating or modifying things published on the Internet.

However, it is difficult to clarify the location of production or intellectual property unless information such as the design drawing of the product and the manufacturer is preserved. In order to clarify the location of manufacturing responsibility and intellectual property right, it is necessary to clarify "Openness" that anyone can refer to data, "Traceability" of information linked to products, "Integrity" which is not tampered is required. Fujiyoshi et al. Achieved the linking of information and products by embedding RFID in the product for product management, The above problem is still unresolved.

Therefore, in this research, I thought that by using Blockchain technology, by saving manufacturing information on the open ledger, it is possible to satisfy the necessary conditions and clarify the location of manufacturing responsibility and intellectual property right. The Blockchain technology is a system that secures the integrity of data by forming a distributed open ledger on the P2P network and mutually verifying input data and preserving it.

In order to verify this method, I implemented the system save manufacturing information on Blockchain by making a single board computer control a 3D printer a Blockchain node.Using this system, we verified the above items of "Openness", "Traceability", and "Integrity", so that the system tracks manufacturing information on products and, It is possible to clarify the manufacturing responsibility and the location of the intellectual property right when the manufacturer himself is the producer of the design drawing.

Based on the results of this research, it is possible to clarify the manufacturing responsibility and the location of the right also in personal manufacturing. This system is a disincentive not to manufacture at a quality that does not cause accidents that the manufacturer is responsible for. Moreover, by applying this method and managing the distribution of the design drawing on Blockchain, it is possible to manage the product manufactured by the 3D printer as intellectual property.

Keywords :
1. Digital Fabrication, 2. Product Libility, 3. Intellectual Property, 4. 3D print, 5. Blockchain

Keio University, Faculty of Policy Management Studies
Ryosuke Abe

目 次

図 目 次

表 目 次

第1章　序論

本章では本研究の背景，課題及び手法を提示し，本研究の概要を示す．

1.1　デジタルファブリケーションの発達

本節では，デジタルファブリケーションと呼ばれるものづくりの発達と，それに伴うパーソナルファブリケーションについて説明する．

1.2　デジタルファブリケーション

デジタルファブリケーションとは，3D プリンタやレーザカッタといったコンピュータに接続されたデジタル工作機器を用いて 3D モデルを実際に造形物として成形する技術のことである．近年，コンピュータの普及とともに，デジタル工作機器は安価かつ小型になりつつある．また 3D モデリングソフトウェアもオープンソースのものが現れるなど，個人であっても高精度で 3D モデルを出力できる機器を入手，製造が行える環境ができつつある．

1.2.1　3D プリントの普及と活用

2000 年代後半以降，技術の発達や低コスト化により，3D プリンタが急速に普及している。3D プリンタは樹脂素材などを加工し，設計図である 3D モデル同様の立体物を造形するデジタル工作機器である．1980 年代の開発当初 3D プリンタは工業製品の試作のために製造業の中で主に使われていた．2005 年にアメリカの 3D Systems 社が保持していた光造形法をはじめとする多くの造形手法が特許失効したことや，3D プリンタ自体の製造技術の発達などの理由で，安価なものが作られるようになった．

また，インターネット上で，3D プリンタに関連する情報や，実際にプリントを行うための設計図などが，数多く Web で共有されている [2]．そうした情報を入手することで，今まで専門的な機器であった 3D プリンタを個人でも扱える環境が整いつつある．

3D プリンタの安価化と情報共有の迅速化・簡易化の二つの要因により，専門家以外による 3D プリンタを用いたものづくりは急速に普及している．3D プリンタの市場規模は 2015 年の段階で 11 億ドルに対し，2019 年には 26 億ドル超になると予測されている [3]．そうした中で，現在 Fablab[4] と呼ばれるデジタル工作機器を扱うことができる施設が世

界各地で設置されており，デジタルファブリケーションの普及に努める拠点となっている．日本でも 2010 年以降神奈川県鎌倉市や茨城県つくば市を始めとして各地に設置されている．Fablab では個人がデジタル工作機器を持たずとも，デジタルファブリケーションを行うことができる．

3D プリントの普及に伴い，開発当初想定されていた試作以外にも様々な応用が考えられるようになった．応用例の一つとして義足が挙げられる [5]．義足は使用者によってそのサイズや形状が異なるため，一律に大量生産することはできない．そのため，既存の義足の製作は，熟練した専門家によってオーダーメイドで制作されており，製作自体や修正も簡単ではない．3D プリントであれば，3D モデルを個人の形に合わせて改変することが容易である．修正する場合も，3D モデルの修正と再出力は簡単に行うことができる．また，福田 [6] は自分の実物大の 3D モデルを用いた作品を製作し，慶應義塾大学湘南藤沢キャンパス内で展示を行った．出力の際に 3D モデルの解像度を調整することで，作品の閲覧者が制作物から 3D モデルの元となった人物を特定できることをなどを確認した．これは芸術分野においても 3D モデルの改変や再出力によって様々な可能性があることを示唆するものである．

1.2.2 パーソナルファブリケーションとオープンデザイン

3D プリンタの普及に伴い，個人で製造を行うパーソナルファブリケーションと呼ばれるものづくりも行なわれつつある [7]．インターネットを通じて入手した 3D モデルを自分の環境に合わせて改変しプリントを行うなど，3D モデルの 2 次利用，3 次利用も行なわれている．インターネット上で公開した 3D モデルが，他人によって改変され派生が生まれる中で，2 次利用者が加えた改変が元の 3D モデルに取り入れられることもある．これは，ソフトウェア開発におけるオープンソースと似た構造である．これらの動きから，オープンソースの考え方などをデザインに適用する “オープンデザイン” という概念も提唱されている [8]．

1.3 本研究の着目する課題と目的

現在のデジタルファブリケーションでは個人で製造において，製造責任の追及や知的財産権の保証のために，製造物の製造情報の管理が一つの課題となっている．ここで扱う製造情報としては，設計図情報である 3D モデルデータ，3D データの設計者，製造者，製造日時などが含まれる．例えば，製造物によって事故が起こった場合，その責任を誰に求めるかといった製造責任 (Product Liability，PL) の追求を行う．その際設計図などから設計上の欠陥を追及する必要性がある．また，自分の設計物を知的財産として証明する際にも製造情報が保存されていることが必要である．製造責任の追及や知的財産権の保障を行う為には，データが誰にでも参照できる公開性，製造物からデータが追跡できる追跡可能性，保存されたデータが後日改ざんされておらず完全性を保っていることが必要である．そこで，3D プリントの際に RFID を製造物に埋め込み，データサーバに保存された製造

情報と製造物を紐付ける試みが行われている [9]．この手法では，追跡可能性は担保されるものの，製造物に紐づけられた製造情報の完全性が担保されていない．

本研究では，パーソナルファブリケーションによる個人的な製造が行われる中で，製造責任の知的財産権の所在を明らかにするシステムを提案した．

1.4 本研究の仮説

Bitcoin の基幹技術として発明された Blockchain 技術は，P2P ネットワーク上でデータが検証されたことを合意し公開台帳を形成するシステムである．公開台帳上に記録されたデータは各参加ノードによって分散的に保持され，改ざんを相互に監視するため，正規の手続きを踏まなければデータの更新もできず，データが失われる可能性も極めて低い．

そこで本研究では，3D プリントにおける製造情報を Blockchain 上に保存することで，1.3 節で述べた条件を満たし，製造責任や知的財産権の所在を明らかにできるのではないかと考えた．

1.5 本研究の手法

本研究では，3D プリンタを制御するシングルボードコンピュータを Ethereum ノードとすることで Blockchain 上に製造情報を保存する実験システムを構築した．Ethereum とは Blockchain を状態遷移を記録する公開台帳として用いるためのアプリケーション開発プラットフォームである．Blockchain 上に製造情報を保存できていることを確認し，本システムのスケーラビリティ，情報の改ざん耐性を推定することで，要件を満たせることを確認した．

1.6 本論文の構成

本論文における以降の構成は次の通りである．

2 章では，3D プリント技術とそれに伴う法的課題と Blockchain 技術に関して議論し，本研究の背景を明確化する． 3 章では，本研究における問題の定義と，解決するための要件，仮説と手法について説明する． 4 章では，3D プリンタをネットワークに接続させ制御し，Blockchain ノードとすることで製造情報の保存をするシステムの実装を概説する．5 章では，2 章で求められた課題に対しての評価を行い，考察する． 6 章では，本研究のまとめと今後の課題についてまとめる．

第2章　本研究の要素技術と既存の法整備

本章では3Dプリント技術と，および関連する既存の法整備，また本研究で用いるBlockchain技術について概説することで，本研究における背景を明確化する．

2.1　3Dプリントと法整備

3Dプリンタは，合成樹脂などを用いて立体物を造形する技術である．本節では3Dプリント技術と，製造に関わる製造責任法と知的財産権法について概説する．

2.1.1　3Dプリント技術

3Dプリント技術は1984年に名古屋市工業研究所の小玉秀男が開発し，特許出願した“立体型作成装置”が始まりである[10]．この時の3Dプリンタは光造形法(Stereolithography Apparatus，SLA)呼ばれる，液体状の光硬化性樹脂を紫外線レーザーで一層ずつ硬化させて積層していく手法を用いて立体物を造形していた．現在一般的に普及しているFDM法の3Dプリンタより高精細かつ表面の滑らかな造形物を作成可能だが，造形物の強度は高くない．開発当初は“rapid prototyping”と呼ばれる，工業製品の試作をするためのものとして開発されていた．その後アメリカで1986年に世界初の3Dプリント会社である3D Systems社が設立され，それ以降SLA法以外の多くの3Dプリント手法が開発された．

3Dプリント手法の中でも熱溶解積層法（Fused Deposition Modeling，FDM）はストラテシス社が2009年に特許を失効してから多くの企業が開発に参加している．そのため，非常に安価で高精度な3Dプリンタも作られるようになり，急速に普及している．FDM法は，リール状に巻かれたフィラメントを高温で加熱し，造形テーブル上に押し付けるように積層することで，立体物を造形していく手法である．FDM法では使用できる素材であるフィラメントの種類が合成樹脂のほか金属製のものなどもあり，SLA法よりも種類が豊富である．そのためFDM法で造形した立体物は，造形物の強度を保つことも容易といった利点がある．そのため，現在主に個人向けとして販売されている3Dプリンタに広く取り入れられている．

2.1.2　製造責任と知的財産権に関する法制度

本項では既存の製造責任と知的財産権に関する法制度を概説し，それらのパーソナルファブリケーションの中での問題について整理する．

製造責任

製造責任とは，製造物責任法第一条によれば “製造物の欠陥により人の生命，身体又は財産に係る被害が生じた場合における製造業者等の損害賠償の責任”のことである．日本においては，1985 年の EC 閣僚理事会において製造物責任に関する法律の統一に関する指令が採択され，各国が製造物責任に対する立法が進んだ影響を受け，1994 年に製造物責任法が制定された．この法律では製造物の欠陥が過失であるかに関わらず，製造物が危険なものであればその責任が問える無過失責任であるとしている．制定当時，その理由としては，以下の三点が挙げられた [11].

危険責任 製造者は製造物の設計図などの情報を消費者より詳細に知り得るため

報償責任 製造者は製造物により利益を得るためそこから生じる責任を負うべきである

信頼責任 製造者は自己の製品の安全性について PR しており消費者はその品質が担保されているものであると期待する

この法制度により，製造物に対しては十分な品質管理がなされ，製造物の質や安全性が担保されるものであると期待されていた．

実際の判例としては，2008 年の当時 2 歳 10ヶ月の男児が所謂 “ガチャポン” と呼ばれるカプセル入り玩具のカプセルで遊んでいる際に誤飲し，重篤な障害が残ったとして，玩具メーカーに損害賠償を求めた裁判が挙げられる [12]．カプセルの形状は約 40mm でほぼ歪みのない形状をしており，幼児の口へは容易に入ることが想定され，玩具の入れ物という特性上，玩具とともに手にとって遊ぶことは通常予見されると判断された．そのため裁判では，設計上の欠陥があるとして，メーカーへの損害賠償を認めた．この判決を受けメーカーはサイズなどの基準の見直しを行い，再発防止に努めることとなった．

パーソナルファブリケーションにおいては，製造時に 3D モデルが危険なものかどうかの検証は行われずに製造物が流通することが多い．そのため，メーカーによる業界基準を満たさない製造物も容易に個人で製造することが可能である．よって，こうした事故は起こり得ると考えられる．

知的財産権

知的財産とは，知的財産権法第二条によれば “発明，考案，植物の新品種，意匠，著作物その他の人間の創造的活動により生み出されるもの (発見又は解明がされた自然の法則又は現象であって，産業上の利用可能性があるものを含む．)，商標，商号その他事業活動に用いられる商品又は役務を表示するもの及び営業秘密その他の事業活動に有用な技術上又は営業上の情報 ” のことである．著作権法，特許法，実用新案法，意匠法などにより設計物の知的財産権は保障され，権利者に無断な複製および製造を制限している．

2.2 Blockchain 技術

Blockchain は Bitcoin の中心技術として発明された P2P ネットワーク内でデータが検証されたをことを合意し公開台帳を形成するシステムである．近年，Fintech(金融テクノロジー，Finance Technology) の分野などで応用可能性が高いとして注目を集めている．本節では Blockchain 技術を概説し，その有用性と課題を示す．

2.2.1 Blockchain 技術と Bitcoin

Bitcoin[13]（以下 Bitcoin のシステム全体を Bitcoin，Bitcoin で扱われるデジタル通貨について BTC と示す）は，Satoshi Nakamoto により 2008 年に発明された，銀行などの中央管理者を持たない P2P ネットワーク上でのデジタル決済システムである．その基幹技術として発明された Blockchain 技術は，P2P ネットワーク上で，参加ノードによって相互に監視し合うことによってデータの完全性を担保しながら Blockchain（本研究では Blockchain で形成される公開台帳と技術自体の混同を避ける為に，技術自体を”Blockchain 技術”，形成される公開台帳を”Blockchain”と呼ぶ．）を形成する．Bitcoin では，トランザクション[1]を各ノードが検証，Bitcoin Blockchain 上に記録し保持することで，使用済み BTC の二重支払いといった不正な支払いを自動で検知し，排除することができる．

2.2.2 基礎暗号技術とデジタル署名

Bitcoin や Blockchain 技術では，暗号学的ハッシュ関数と公開鍵暗号によるデジタル署名が用いられている．本項ではそれらを概説する．

暗号学的ハッシュ関数

ハッシュ関数とは，ある入力データが与えられた際にその要約となる固定長のハッシュ値を得る関数のことである．中でも暗号学的ハッシュ関数は，次のような特性を持つ

- 入力データが類似していても，同一なハッシュ値を得られない．
- ハッシュ値から元のデータを求めることが事実上不可能である．
- 同じハッシュ値を持つ入力データを特定することが事実上不可能である．

[1]Bitcoin でいう “トランザクション”は Blockchain へ保存される “デジタル通貨の転移を示す取引”のことである．この “取引”は，“トランザクション”が各マイナーによってブロックに格納されるまで実行されない．Blockchain 技術では後に示す 50%攻撃の可能性を残したシステムのため実行が取り消される可能性もあり，“トランザクション”は完全に完了したことは保証できず，データベースにおける “トランザクション”とは異なる．

ここで “事実上不可能” と述べているものは，数学的に有限である入力とハッシュ値においては探索することは可能であるが，確率的にそれらを達成することができないことを示す．これらの特徴を図 2.1 に示す．Bitcoin では SHA-256 と呼ばれるハッシュ関数を主に利用している．ハッシュ関数を用いることで，固定長の要約を得ることができ，全く同一の入力データでなければ同一のハッシュ値を得ることはできない．そのため，容易にデータが同一であることが検証できる．

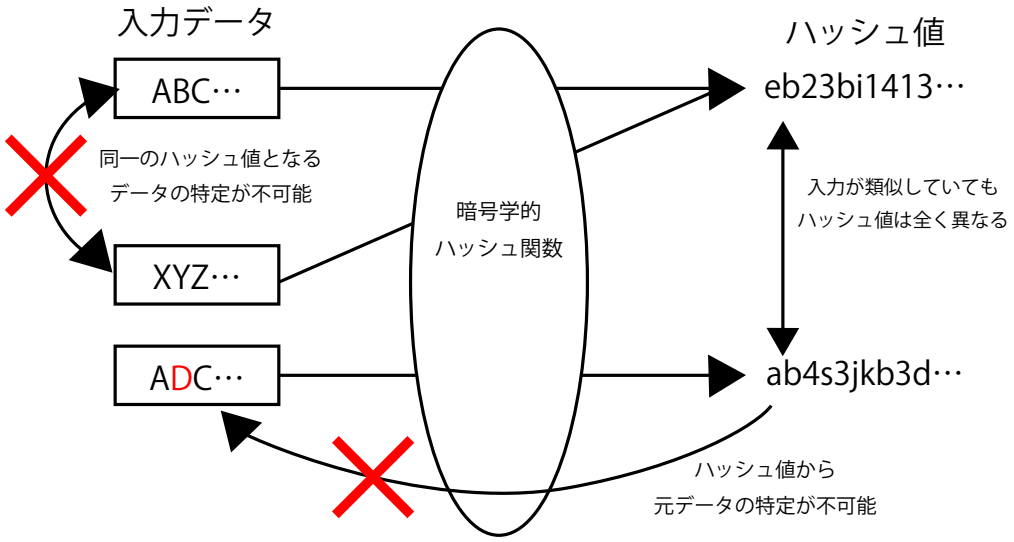

図 2.1: 暗号学的ハッシュ関数の特徴

デジタル署名

デジタル署名とは，公開鍵暗号を用いた署名を用いることで，データの送信者の真正性とデータが改ざんされていないことを担保する仕組みである．送信者が作成した鍵のペアである公開鍵と秘密鍵を用いる．公開鍵は秘密鍵から生成される．秘密鍵で暗号化したデータは，その秘密鍵から生成された公開鍵を用いてのみ復号することができる．データの送信を例に，デジタル署名の使用例を図 2.2 で示す．データの送信者は送信データをハッシュ関数を用いて暗号化し，更に秘密鍵を用いて暗号化したものをデジタル署名とする．データとともにデジタル署名を受信者に送信し，受信者は別の方法で共有された公開鍵を用いてデジタル署名を復号化すると共にデータをハッシュ化し，それぞれを比較することで，データが改ざんされずに送信者から送信されたことを確認する．Bitcoin では，ECDSA(楕円曲線署名アルゴリズム，Elliptic Curve Digital Signature Algorithm) が用いられている．

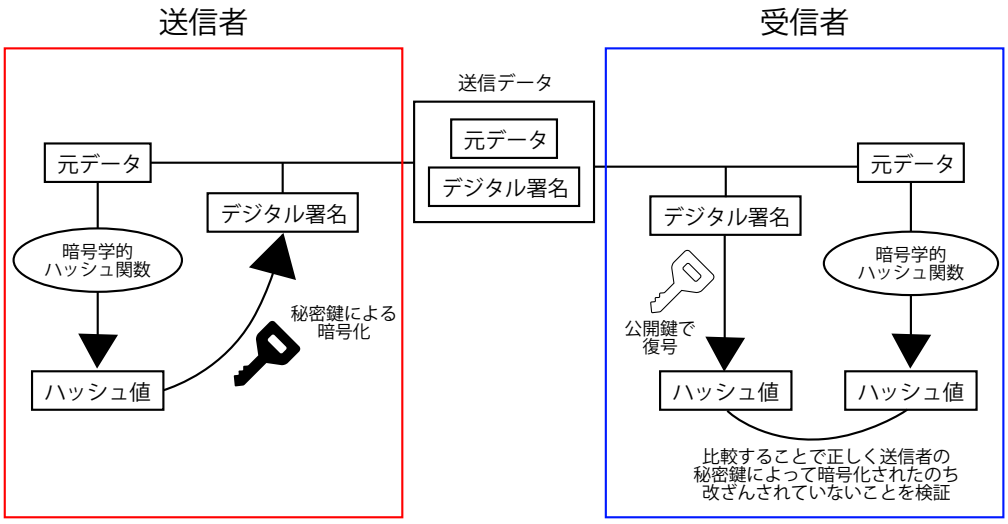

図 2.2: データ送信におけるデジタル署名の使用法

2.2.3 公開台帳 Blockchain の構造と生成

検証されたトランザクションは各ノードが持つ Blockchain に記録された段階で正当性が検証され，Blockchain ネットワーク上で承認されたトランザクションとみなされる．Blockchain は，検証済みトランザクションの集合を一つのブロックとし，ブロックの ID として一つ前に連なるブロックのハッシュ値を持つことで，ブロックを連鎖させた構造を持つ．Blockchain 上のある特定のブロックの前のブロックを “親ブロック”，続くブロックを “子ブロック” と呼ぶ．各ブロックの親ブロックを辿っていくと，最初のブロックである “Genesis ブロック” に辿り着く．“Genesis ブロック” からあるブロックまでのブロックの数を “ブロック高” と呼ぶ．

ブロックの生成はマイナーと呼ばれるノードが行い，作成されると Blockchain ネットワークへブロードキャストされる．新しいブロックを受け取った各ノードは Blockchain 末尾のブロックのハッシュ値をブロックの ID として持ち，含まれるトランザクションが全て正当性を持つことなどを確認したのち，自分の持つ Blockchain に追加する．もし受け取ったブロックが，自分の持つ Blockchain の末尾直後に続くブロック高よりも大きいブロック高を持つブロックの場合，Orphan ブロックとして一時的に保存する．これは，後述するように Blockchain ネットワーク上で Blockchain が分岐することや，自分が持つ Blockchain が常にネットワーク上で最新ではない可能性があるためである．ブロック作成中のマイナーは他のマイナーが生成したブロックを受け取ると，ブロックの検証，Blockchain への追加を行った後，新規ブロックに連なる新たなブロックの生成に取り掛かる．

2.2.4 Proof-of-Work

Blockchain のブロックハッシュ値の連鎖構造自体は，単独のコンピュータで容易に形成できる．Bitcoin においては，ブロックの追記を “Proof-of-Work(PoW，作業証明)” と呼ば

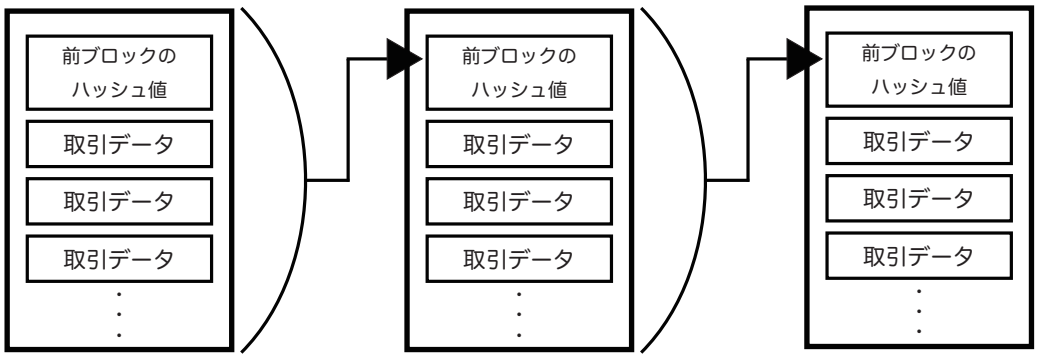

図 2.3: Blockchain の構造

れる仕組みで困難にしている．それに基づくブロック採用のコンセンサスによって，P2P ネットワーク上で改ざんが困難かつ一意な Blockchain が形成される．

Proof-of-Work とはマイナーがブロックを生成する際に，生成するブロックにある作業を行うよう条件を付け加えることで，ブロックの生成を即時には行えなくするものである．この条件とは，“ブロックの中に nonce と呼ばれる無意味なデータを追加することで，ブロックのハッシュ値が目標の値以下になるようなブロックを作成する”ことである．ハッシュ値は不可逆な暗号であり，データが 1bit でも異なれば全く異なるハッシュ値になる．そのため，条件を満たすためには nonce の値を変化させながらハッシュし，目標値以下になっているかを検証する方法しかない．この作業が完了するまでの時間は，コンピュータの計算パワーに依存する．また，目標値は過去のブロック生成にかかった時間を Blockchain 上から確認し，Bitcoin では平均 10 分に 1 回ブロックが生成できるように調整される．Bitcoin では，この Proof-of-Work を含むブロック生成作業を行わせるインセンティブとして，一定量の BTC を新たに発行し，自分の生成するブロックに含める．Proof-of-Work を行いコンピュータの計算パワーを投入することを金の採掘の比喩で “Mining(マイニング，採掘)”と呼ぶ．Proof-of-Work によって，ブロックのハッシュ値によるブロック同士の連鎖構造を構築することはコンピュータの計算パワーを投入しなければ構築することはできなくなる．

親ブロックが同一で，異なる検証済みトランザクションのセットを含んだブロックをほぼ同時に複数のマイナーが生成してしまうことがある．その場合，基本的には各ノードは先に伝播してきたブロックを Blockchain に繋げて保存していくことになる．その時，Blockchain ネットワーク上では複数の同じブロック高のブロックが異なる複数の Blockchain ができる分岐 (Fork，フォーク) が起こる．最終的に全参加ノード内で同一の Blockchain

を持つためには Blockchain ネットワーク上で採用するブロックを一意に合意する必要がある．そのため Bitcoin では，追加されているブロックの目標値の発見の困難度の累計が最も大きいものを採用し，コンセンサスを形成する．これにより，分岐が起こったとしても，採用される Blockchain は最も不可逆性が高く，信用に足りうる一つの Blockchain へと収束する．

2.2.5 改ざん耐性

Blockchain は連鎖構造を持ち，Proof-of-Work によるブロックのノンス目標値発見の困難度に基づくコンセンサスで分岐を収束させる仕組みを持つため，高い改ざん耐性を持つ．攻撃者がすでに Blockchain に格納されているブロックのトランザクションを改ざんし，分岐させたとする．その場合，改ざんしたトランザクションを含むブロックから最長の Blockchain 末尾のブロックのブロック高を超えるまで，Mining を行い，ブロックの生成を行わない限り改ざんされたブロックが他の善良なノードに受け入れられることはない．これは，全世界のマイナーが投入する計算パワーの 50%超を改ざんして分岐させた Blockchain を伸ばすために働かせなければ実現することはできない．そのため，現実的に改ざんは困難であるとされている．

Satoshi Nakamoto による Bitcoin の設計文書では，全世界のマイナーが投入する計算パワーの 10%を持つ攻撃者が改ざんに成功する確率が 0.1%以下になるのは，改ざん対象のブロック以降に 5 ブロック以上連なる時であると示した．それを元に慣例として，トランザクションを行ったのち，当該トランザクションを含むブロック以降 6 ブロックが Blockchain に格納されればそのトランザクションは完了されたとみなされている．また，Rosenfeld は，ハッシュレートを元に支払いを行った BTC を二重に消費することができる可能性を分析した [14]．ハッシュレートは Proof-of-Work における，ハッシュ計算を秒間に行える回数の指標である．そこでは攻撃者のハッシュレートがマイナー全体のハッシュレートの 50%超であれば必ず改ざんは成功し，ハッシュレートがどれだけ低くとも改ざんの成功可能性が無くなることはないと示した．その一方で，マイニングによる BTC の受け取り量を示し，改ざんを働く十分な経済的インセンティブは慣例の 6 ブロック以上の改ざんにおいては低いことを示唆した．

2.2.6 Bitcoin におけるトランザクションとスクリプト

Bitcoin におけるトランザクションは，送金元から送金先への BTC の支払いを記号化したデータの集合体である．送金元の持つ資金源をインプット，送金先を指定をアウトプットと呼ぶ．ユーザは自分が受け取ったアウトプットをインプットとして使用することで，トランザクションは連鎖構造を持つこととなる．まだインプットとして使用されていないアウトプットを未使用トランザクションアウトプット (Unspent Transaction Output, UTXO) と呼ぶ．全ての UTXO は Bitcoin Blockchain に記録されているため，各ノードはトランザクションに使われているアウトプットが UTXO であるかは容易に検証すること

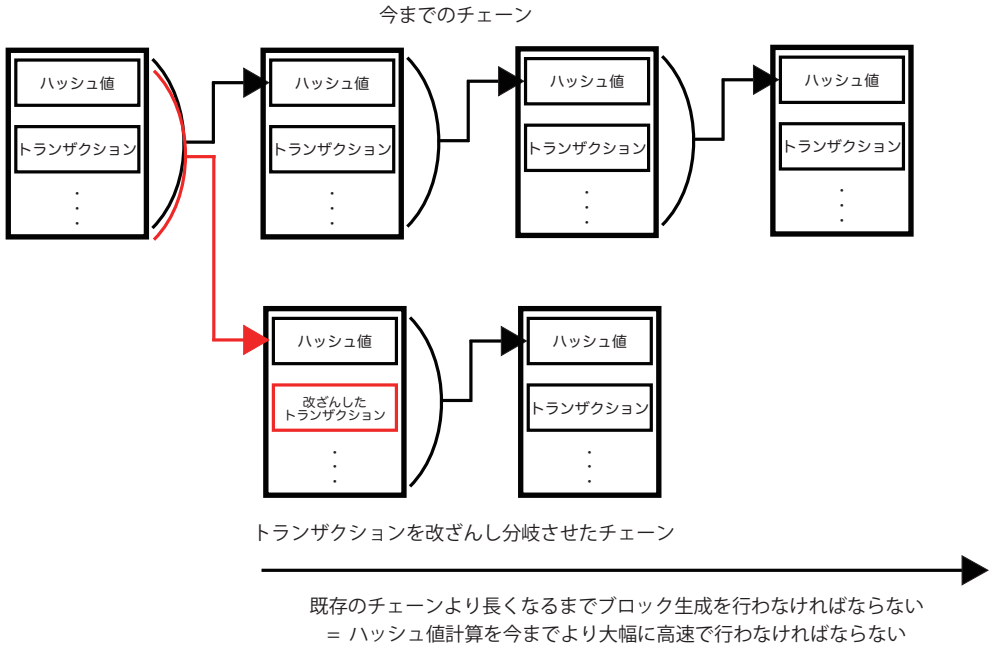

図 2.4: Blockchain 改ざんの不可能性

ができる．Bitcoin リファレンス実装のクライアントでは，UTXO を UTXO セットと呼ばれるデータベースに保存し，インプットとして使用されると削除することで効率的に当該 UTXO を処理する．

アウトプットには，そのアウトプットを使用する条件を記述した “scriptPubKey” と呼ばれるスクリプトを含んでいる．このスクリプトは Forth 言語に似た逆ポーランド記法のスタックベース言語で記述される．インプットには使用する UTXO のポインタと “scriptSig” と呼ばれる scriptPubKey の条件を満たすスクリプトを含む．トランザクションが発行され各ノードへブロードキャストされると，インプットに含まれるポインタで読み出した UTXO の scriptSig と scriptPubKey を実行することで，正当に当該 UTXO を使用していることを検証する．トランザクションと各スクリプトでの開錠の構造を図 2.5 に示す．

多くの二者間の BTC 支払いのトランザクションは，Pay-to-Public-Key-Hash(P2PKH) と呼ばれるスクリプトが用いられている．P2PKH を使うには，Bitcoin アドレスと呼ばれる送金先の公開鍵を SHA256 と RIPEMD160 によって二重にハッシュし，符号化したものを送金先が送金元に伝える．送金元は scriptPubKey に “scriptSig で Bitcoin アドレスに対応した公開鍵とその秘密鍵を用いた署名を提示する” ことを条件にマッチするデータとして書き込む．この scriptPubKey によって，秘密鍵と公開鍵を保持している人のみが支払われた BTC を使用することができる．

UTXO は，書き込まれている scriptPubKey に示された条件を満たしていることを，

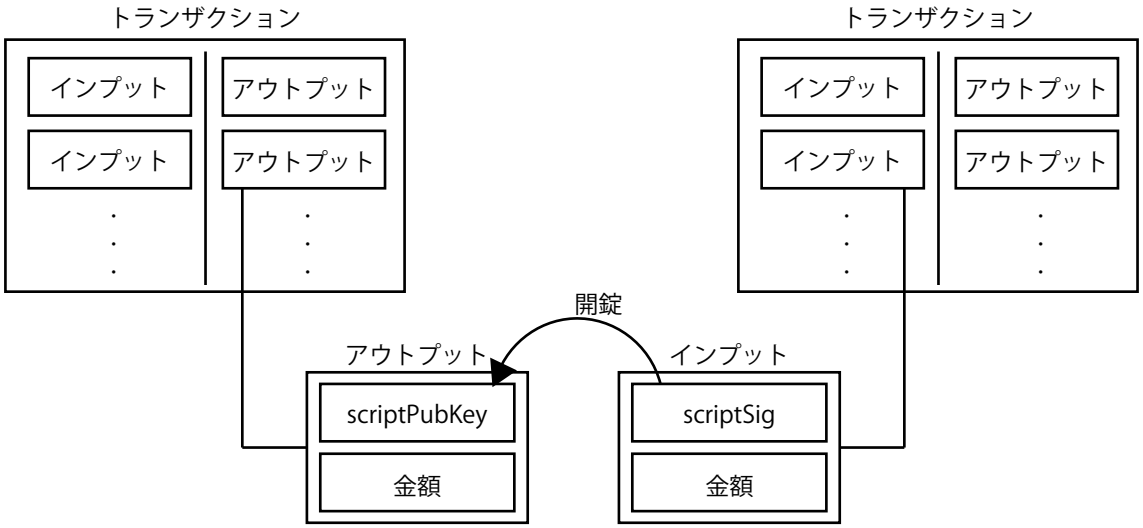

図 2.5: トランザクションの構造とスクリプトによる開錠

scriptSig で証明できれば使用することができる．scriptPubKey で示される条件は必ずしも先述のように公開鍵暗号を用いたものである必要はない．スクリプトで表現できる条件であればどのような条件でも設定することができる．だが，スクリプトで用いるプログラム言語は意図的にチューリング不完全になっている．これは，ループを設けないことにより簡潔にスクリプトを検証できることや，無限ループを作るなどして Bitcoin ネットワークを混乱させないためである．

2.2.7 Bitcoin Blockchain の応用

Bitcoin では通貨の保有量転移を扱うために，Blockchain 技術を発明した．しかし，P2P ネットワーク上で高改ざん耐性を持つデータを形成できることはデジタル通貨以外の多くの応用可能性がある．そこで，Bitcoin のトランザクションで用いるスクリプトを使うことで Bitcoin Blockchain を通貨以外の分野への応用が考えられている．

初期には，無効な Bitcoin アドレスに向けたトランザクションを発行し，その scriptPubKey に任意のデータを書き込むことで Bitcoin Blockchain 上にデータを書き込む応用が考えられた．しかし，この応用方法は Bitcoin Blockchain 上に Bitcoin とは関係ないデータを保存し，Blockchain を肥大化させるものであるとして批判を集めた．そのため，“OP_RETURN” というデータ書き込み専用の演算子を実装することで，Bitcoin Blockchain 上にデータを保存することを可能とした．“OP_RETURN” を scriptPubKey に用いている場合，このトランザクションのアウトプットは UTXO セットには保存されずインプットとして用いることはできない．Bitcoin クライアントのリファレンス実装では “OP_RETURN” を用いたトランザクションを受け取った際に処理しないで破棄するオプションが選択できる．

“OP_RETURN” を用いた Bitcoin Blockchain の応用として，Proof of Existence[15] が

ある．Proof of Existence は，文章ファイルのハッシュ値をトランザクションの中に書き込み Blockchain に格納させることによって，トランザクションが Blockchain に格納された時に当該文章ファイルが存在していたことを証明することのできる電子公証サービスである．Blockchain 格納後にある時点で文章が存在していたことを後日証明する際は，当該トランザクションが格納されているブロックを参照し，ハッシュ値を照合することによって検証することができる．

また，Namecoin[16] を始めとして，Bitcoin Blockchain を使わずに独自に Blockchain を構築し利用するアプリケーションも提案されている．しかし，独自で Blockchain を構築した際，十分な参加ノードの規模がない場合，Blockchain の高改ざん耐性を利用することは難しい． 2.2.5 節で述べたように，Blockchain で Proof-of-Work を用いた場合，参加マイナーの総計算量の 50%を改ざんを認めるように動かさなければ Blockchain を改ざんすることはできない．しかし，独自に Blockchain を構築した場合，参加ノードが少なければ，50%の計算量を超えることは難しくないだろう．

2.2.8 状態遷移システムとしての Bitcoin と問題点

Bitcoin は通貨の所有権の状態を Bitcoin Blockchain 上に記録された UTXO で表現するシステムとして考えることができる．通貨所有権の転移をトランザクションによって表現し，Bitcoin Blockchain 上の UTXO を使用済みにし，新たな状態を作成した UTXO で表現する．この状態の遷移のデータをデジタル署名と Proof-of-Work を用いることで，中央管理サーバなしに一意に確定することを実現している．

その一方で， 2.2.7 節で述べたような Bitcoin Blockchain を用いてアプリケーションを構築する際には幾つかの問題がある．以下その問題点を述べる．

チューリング不完全

2.2.6 節で述べたように，Bitcoin のトランザクションのスクリプトで用いるプログラム言語はチューリング不完全になっている．そのため，擬似的に繰り返し動作を記述するためには，基本的な実行内容を何度も記述しなければならない．このような記述を行うことで，Bitcoin Blockchain 上に非効率なコードが保存され Bitcoin Blockchain の肥大化の原因となる．Bitcoin Blockchain が肥大化することによって，トランザクションの検証の処理が非効率になり，Bitcoin 本来の処理に支障が出る可能性がある．また，アプリケーションのソースコードも難読化し，高度なアプリケーションは開発するのは困難である．

転移する取引量の制御

UTXO で表現されている通貨量転移の量をスクリプトから制御することはできない．例えば，トランザクションを発行してから 1ヶ月後に 100,000 円分の BTC を転移するという取引を行いたいとする．この時，一ヶ月後の BTC と円のレートによって転移すべき BTC 量は変動する．そのため Bitcoin ではこのようなトランザクションを単独で実行すること

はできない．様々な通貨量のアウトプットを複数持つ UTXO を持ちその中の 1 つだけを解錠できるようなトランザクションを発行することで，実現することは可能だが，使用しない UTXO を複数 Bitcoin Blockchain 上に記録することとなり，Bitcoin Blockchain 上の領域を非効率的に使用してしまう．

状態の表現の貧困さ

Bitcoin での状態を示すトランザクションのアウトプットは，トランザクションのインプットとして使用可能なものか，OP_RETURN などを利用した使用不可能なものの二つの状態しか表現できない．そのため，トランザクション内部に状態を一時的に持たせることは非常に困難である．また，その場合 Bitcoin Blockchain 上に任意のデータ構造を持つデータを保存し，転移させるような機能を実装することは非常に困難である．

Blockchain のスクリプトからの参照

Bitcoin トランザクションのスクリプトから Bitcoin Blockchain 自体を参照するようなことはできない．そのため，Bitcoin Blockchain 自体のブロックヘッダなどの情報を用いるようなアプリケーションを開発することが不可能である．これは作成できるアプリケーションに制約がかかっていると言える．

2.2.9 Ethereum

Ethereum（以下 Ethereum のシステム全体を Ethereum，Ethereum で扱われるデジタル通貨について Ether と示す）は，Blockchain 上でチューリング完全なプログラム言語を実行できるようにしたアプリケーションプラットフォームである [17]．Ethereum では Blockchain 上で汎用性の高いチューリング完全なプログラム言語を動作させることで，高度なアプリケーションを開発できるものである．そのため，小規模なアプリケーションでも，Ethereum の巨大なネットワーク上の多くマイナーによる検証を受けることができ，Blockchain 技術の高改ざん耐性を利用できる．

Ethereum では，その P2P ネットワーク全体をコードの実行をし，その結果の状態を保存する仮想マシンとして考えることができる．個々のマイナーでプログラムを実行する環境を Ethereum Virtual Machine(EVM) と呼ぶ．EVM それぞれはサンドボックス化されておりネットワークへのアクセスは制限がかかっているため，実行されるコードにバグが存在していても Blockchain 全体に悪影響を及ぼすことはない．コードの実行は Blockchain 上で行われるため，参加ノード全体で共有し，実行される．

Ethereum アカウント

Ethereum 上のアカウントは 20byte のアドレスと，以下のような状態を保存する領域を持つ．

- Nonce: 各トランザクション処理が一度きりであることを確約するためのカウンター
- Ether: Balance 内部通貨 Ether の保有量
- Contract Code: Ethereum 上で実行可能なプログラムのソースコード
- Storage: データを保存するストレージ領域

Ether は Ethereum 上で使用される内部通貨であり，後述するトランザクションの手数料を支払うために使用される．一般的に，アカウントは，外部所有アカウント（Externally Owned Account，EOA）とコントラクトアカウント (Contract Account，CA) の 2 種類である．EOA は秘密鍵と結びついており，コードを持たずアカウントの Ether 残高を管理する．その一方，CA はアルゴリズムを記述するためのコードとその保存領域を持つ．各アカウントよりトランザクションやメッセージを送信することで，CA は保有するコードを実行可能にし，ストレージを書き込み可能状態にしたのち，コードの実行に合わせて新たにメッセージを送信，またはコントラクトを作成する．

Ethereum 上では主に Solidity と呼ばれる JavaScript によく似たプログラミング言語が使われている[2]．Solidity によって記述されたコードはコンパイルされ，EVM 上で実行できるバイトコードとして保存される．

トランザクションとメッセージ

Ethereum におけるトランザクションは EOA から送信され，以下のような情報を含む．

- トランザクションの送信先
- 送信者のデジタル署名
- 送金される Ether 量
- データフィールド
- コード実行にかかる計算ステップの最大値 (STARTGAS)
- 送信者が払う 1 計算ステップあたりの手数料 (GASPRICE)

最初の 3 つは一般的にデジタル通貨システムでは必要となる項目である．データフィールドは，CA に対してコードの実行を行う際に CA に与える関数の引数となるデータを書き込む．STARTGAS と GASPRICE はチューリング完全な言語を実行可能にしたことによる，無限ループなどを起こさせないための仕組みである．“gas” と呼ばれる単位でコードの実行ステップを表現する．STARTGAS によって実行するステップ最大値を指定することにより，無限ループが発生すると，実行途中で支払う手数料が無くなり，“gas 切れ”

[2]他にも Python によく似た Serpent，Lisp によく似た LLL などがある．

を起こす．“gas 切れ”を起こすと，その時点までコードの実行で行われた状態遷移はトランザクション発行の手数料以外は失われ，トランザクションが発行される前の状態のままとなる．そのため，Ethereum 上で実行するチューリング完全性を持たせても，無限ループを起こすことは事実上困難である．

トランザクションによって CA のコードが実行されている中で，別の CA を読み出すことができる．その際は CA からトランザクションとは異なる “メッセージ” を CA に向けて送信することで実行を行う．メッセージには以下の情報を含む．

- メッセージの送信者
- メッセージの受信者
- 送金される Ether 量
- データフィールド
- STARTGAS

EOA からトランザクションを発行する際，実行するコードを持つ CA がメッセージを発行し，別の CA のコードを実行した際，EOA から必要な “gas” は 2 つの CA のコードの実行の総量となる．実行途中で読み出された 2 つ目 CA の実行途中で “gas 切れ” を起こした場合も状態遷移は起こらない．

Ethereum Blockchain とマイニング

Ethereum における Blockchain も Bitcoin と同様に，Proof-of-Work を用いて，マイナーにブロックヘッダに含まれる適切な nonce を見つけさせることでマイニングを困難にしている．Ethereum Blockchain に於ける Proof-of-work では Ethash と呼ばれるハッシュアルゴリズムを用いている．Ethash は採掘専用ハードウェアの開発が困難なアルゴリズムであり，マイニングが特定のマイニングプールだけに集中させないことを目指している[3]．

Bitcoin においては状態は UTXO として各トランザクションのアウトプットとして表現されているだけであるが，Ethereum においてはトランザクションのリストと、ブロック生成時点での状態をデータとして保存している．Ethereum Blockchain 上に全ての CA のコードは記録されている為，実行することで，トランザクションの結果直前のブロックに記録された状態から正常な状態遷移が行われているかを検証することが可能である．Ethereum Blockchain においては，トランザクションの保存に “パトリシア木” というデータ構造が使われている．これにより Bitcoin Blockchain よりも効率的に状態を保存することが可能である．そのため，状態を検証する為に Genesis ブロックからの全てのブロックを持つ必要はない．

[3] しかし，現実として Ethereum ネットワーク上では特定のマイニングプールが 20%程度のハッシュレートを維持している．

また，Ethereum における状態遷移，つまりコードの実行は当該トランザクションが Blockchain に格納された時に完了する．つまり，マイナーが正当にトランザクションをブロックに格納していれば，そのコードの実行はブロックが生成された時点で行われる．各ノード上では，新規ブロックを受け取り，正当なブロックとして検証されれば，自分の持つ Blockchain に追加した際にそのブロックに含まれる状態遷移が実行される．

2.2.10 Blockchain 技術の課題

Blockchain 技術にはいくつかの課題がある．本節ではそれらを指摘する．

イクリプス攻撃への耐性

P2P ネットワークへの攻撃として，イクリプス攻撃と呼ばれるものがある．これは P2P ネットワークにおいて，攻撃者のノードが本来受け取り隣接ノードへ送信するべきデータを送信しなかったり，特定のノードのみへと送信することでネットワークを分断する攻撃である．イクリプス攻撃が行われると，実際には P2P ネットワーク上に存在するデータが特定のノードからは見えないといった状況が発生する．図 2.6 のネットワークにおいて攻撃者 E が右側のから送られてきたデータを左側のネットワークに送信しないといった攻撃を行う．すると，これが Blockchain ネットワークであった場合，ノード A はノード B の作ったブロックやトランザクションを受け取ることはできなくなる．そのため，Blockchain ネットワークでイクリプス攻撃が行われると，作成される Blockchain が分岐することとなる．渋田 [18] はこのイクリプス攻撃を Bitcoin などの Blockchain 技術で行われる際の手順を体系化し，それに対する現状での Bitcoin リファレンス実装における対策が不十分であることを示唆した．

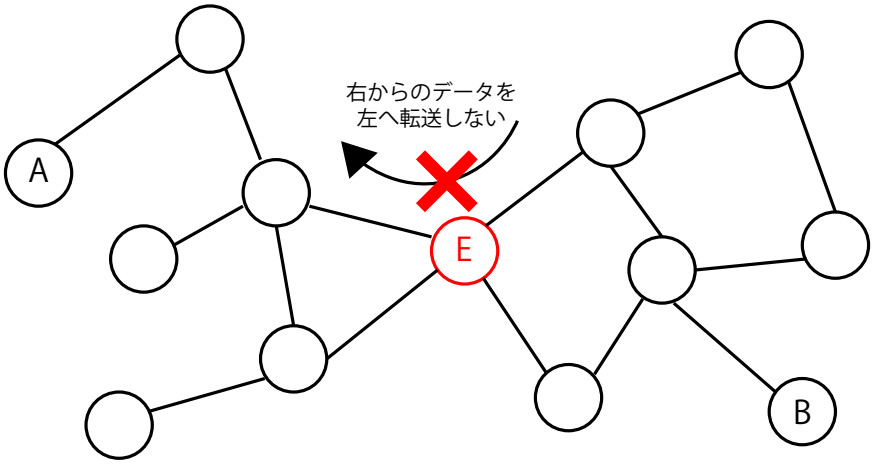

図 2.6: イクリプス攻撃の例

ガバナンス定義の不可能性

斉藤 [19] は，Blockchain を状態遷移システムとして捉え，その状態遷移が確定することはないことを指摘した．2.2.5 節で述べたように Blockchain 技術においては改ざんを行おうとするマイナーが全体のマイナーが持つ計算量の 50%を超えなければ改ざんは困難であるとされている．しかし，自由にネットワークに参加，離脱ができる P2P ネットワークにおいて，“全体”を定義することは不可能である．そのため，Blockchain 技術においては状態遷移は “確定”することはなく，いつでも巻き戻しが起こる可能性を否定できない．よって，状態遷移に確率的な許容ができるシステムに Blockchain 技術を応用できる可能性を示した．

強権発動

Blockchain 技術は，P2P ネットワーク上で中央管理ノードを作らず権威者などの第三者による取引および状態遷移に対する介入を認めないことが，一つの利点となっている．その根拠は参加マイナーの 50%超の計算パワーを動かさなければ Blockchain 上のデータを改ざんし，変更することができないことが根拠となっている．しかし，現実的に改ざんが行える状況が存在する．

Bitcoin Blockchain 上では計算パワーの 50%超を上位 5 つのマイニングプールで確保している．図 2.7 に 2017 年 1 月のハッシュレート分布を示す．また，過去には単独のマイニングプールが 50%超のハッシュレートを確保したことも確認されている．これは専用ハードウェアの開発が活発化したなどの理由から，個人がマイニングを行うことが効率的でなくなったため，専門的に取り組む企業などが多くのハッシュレートを確保してしまったためである．現状であれば，それら大多数のハッシュレートを保持するマイナーたちが “利己的なマイニング”を行い，Bitcoin Blockchain を混乱させることが可能である．

また Etherum においては，2016 年 6 月に Ethereum 上で構築された自律分散投資ファンド The DAO で，CA のコードにバグがあり，開発者が意図しない形での Ether の大量な送金が行われた事件が発生した．これによって The DAO は多額の損失を出した．それらを回収するために，Ethereum 開発者コミュニティは所謂 “ハードフォーク”と呼ばれる対策を実行した．これは，The DAO より Ether を引き出したトランザクションを無効にするような Etherum クライアントを開発者コミュニティが配布し，Ethereum Blockchain を改ざんする対応である．これに対しては大きな批判が集まり，Ethereum Classic[20] と呼ばれる，ハードフォーク実行前の Ethereum Blockchain を採用したものと Ethereum Blockchain が分岐する事態となった．

Bitcoin，Ethereum 両者において，Blockchain を特定の意思の元変更するように大部分のマイナーを働かせる “強権発動”が可能となっている．この強権発動は，計算パワーを保持しない Blockchain 技術開発者コミュニティが，特定の意思の元動くクライアントなどを配布することで可能である．これは事実上開発者コミュニティが中央となり改ざんを提案することと同義であり，権威者を作らず，第三者の介入を認めない P2P ネットワークを採用している Blockchain 技術の思想と異なるものである．Blockchain 技術は全世界で一

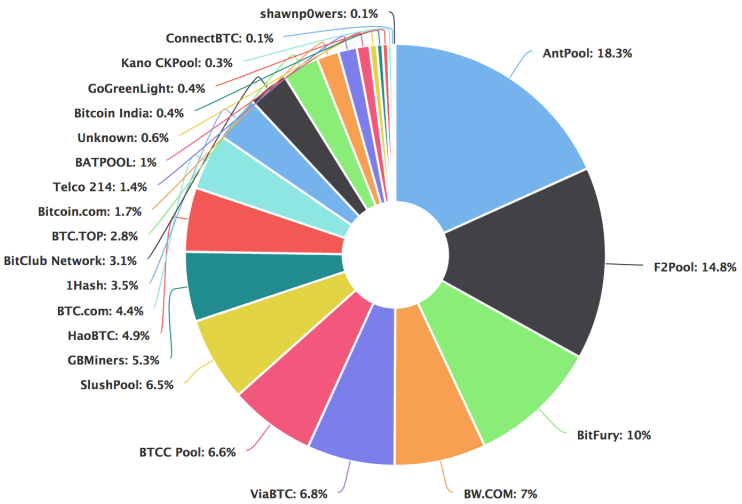

図 2.7: 2017 年 1 月のハッシュレート分布 出典：Blockchain.info[1]

意な Blockchain を形成するが，逆に全世界で一意でなければ動作しないという欠点がある．Blockchain ネットワーク一部で実験的にテストを行う，といったことも困難である．

第3章　本研究における問題定義と仮説

本章では，１章で述べた背景より，本研究における問題とその要件に関して議論し，先行研究および提案システムを概説することで本研究で用いるアプローチについて述べる．

3.1　本研究における問題定義

現在のパーソナルファブリケーションのような，個人におけるものづくりに対して現行の製造物責任法や知的財産権法はそぐわない面があると指摘されている [21]．例えば危険責任に関して，3D プリンタで出力を行う者は Thingiverse などインターネット上から 3D モデルをダウンロードし，出力を行った場合必ずしもその製品の特性に関して熟知してるとは言い難いだろう．また，現行の法制度では，責任を負う製造者は “当該製造物を業として製造，加工又は輸入した者” とされており，販売，頒布を広く行わなければ個人で製造を行っても製造責任を問われることはない．その一方でパーソナルファブリケーション環境下でも製造物責任を問わなければ，個人が製造した粗悪な製品による事故が発生する危険性も存在するだろう．そこで本研究では，パーソナルファブリケーションといった個人による製造において，製造責任と，知的財産権の所在を明らかにするシステムを提案した．

本研究では，保存する情報が製造責任の追及や，知的財産権の保障を行うための証拠とされることは扱わない．3D プリントにおける製造元を明らかにすることで，その製造者に対して設計図情報を開示できるため，それらは実運用上の対処で解決できる問題であると考える．

3.2　問題解決における要件

3.1 節で述べたパーソナルファブリケーション環境における製造責任および知的財産権の所在を明らかにするために必要な要件を述べる．

3.2.1　公開性

製造責任を追及する際，製造物の製造者が秘匿され，消費者からアクセスできなければその欠陥を指摘することや，製造者を訴えることができない．また，製造者が製造物を自分の知的財産であることを公に示すためには，その設計者であることと製造日が明らかに

なっている必要がある．そのため，製造情報が誰にでも閲覧可能な形で公開されていることが求められる．

3.2.2 追跡可能性

製造，流通の過程などにおいて製造責任と，知的財産権の所在を明らかにするために，追跡可能性が担保されることが必要である．ここでは，製造物と紐付いた製造情報を読み出すシステムが，多くの場所などから問い合わせに応答できるためにスケーラビリティを持つことが重要であると考えられる．

3.2.3 完全性

製造情報が保存されたのち，改ざんされていれば，製造責任や，知的財産権の所在のための根拠として用いることはできない．そのため，情報の完全性が担保されている必要がある．

3.3 先行研究

デジタルファブリケーションにおける製造物と製造情報を紐付ける手法として，3D プリントを行う際に製造物に RFID を埋め込む技術の研究が行われている [9]．プリント中に RFID を埋め込み，ID を製造物自体に付与することで，その製造情報を管理するサーバへ問い合わせる形で閲覧し，追跡可能性を担保する仕組みである．RFID 以外にも製造物自体に ID を埋め込む InfraStructs という技術も開発されている [22]．これらの技術を用いることで製造物に識別番号を埋め込むことが可能である．その一方，識別番号と紐付けられるデータをどのように管理するかが課題となっている．

Blockchain を用いてものの追跡可能性を確保する試みは Everledger などが挙げられる [23]．Everledger はダイアモンドの情報を Blockchain 上で管理することで，その追跡可能性を担保する試みである．掘り出された鉱山，過去の所有者，カラット数などの情報のマークル木のマークルルートのハッシュ値を Blockchain 上に保存し，データそのものは Everledger が管理することでデータの完全性を保証する．主に紛争地域などで行われる取引において，Blockchain を用いて取引の公開性を担保している．

3.4 本研究における仮説

本研究では 3.2 節で述べた公開性，追跡可能性，完全性を担保しながらデジタルファブリケーションにおける製造物の製造情報管理システムを構築したい．そこで，Blockchain 技術を用いることで，それらの要件を満たしたシステムが構築できるのではないだろうかと考えた．それぞれの要件に対して Blockchain 技術による実現が可能であると考えられる点を本節では述べる．

3.4.1 公開性

Blockchain 自体が公開台帳であり，Blockchain 上に保存されたデータは各ノードから読み出すことが可能である．そのため，Blockchain 上に製造情報を保存することで，検証が必要な際に誰でも参照でき，公開性が担保されると考えられる．

3.4.2 追跡可能性

Blockchain 上にデータを保存する際にトランザクションを発行する．その時トランザクションには Blockchain ネットワーク上で一意な ID が発行される．この ID をもとに Blockchain 上のトランザクションが格納されているブロックを特定し，トランザクションを参照することが可能である．そのため，製造情報を Blockchain 上に保存し，Blockchain に格納されれば，トランザクションの ID を製造物の ID として用いることができる．先行研究で挙げた 3D プリントにおける製造物への RFID の埋め込みなどによって製造物と ID の紐付けを行い，Blockchain を参照するシステムを構築することで，製造物の製造情報の追跡可能性が担保できると考えられる．また，Blockchain は参加ノードによって分散的に保持されている．そのため，単独のノードが情報を失ったり，ネットワークから分断されたとしても，他のノードから情報を参照できるので，追跡可能性が失われることはない．

3.4.3 完全性

Blockchain は 2.2.5 節で述べたように，そのチェーン構造と合意形成アルゴリズムによってデータを改ざんすることは困難である．単独の製造者がデータを改ざんする状況は，製造責任が問われた場合の責任逃れや，知的財産権の侵害を隠蔽することが考えられる．これらの状況下で，Blockchain を改ざんできる環境を単独で構築することは困難であり，攻撃者によって完全性を失わせられる可能性は低いと考えられる．

3.5 提案システム概要

提案システムの概要を述べる．3D プリンタと 3D プリンタ制御のため接続された Raspberry Pi を一つの Blockchain ノードとすることで，3D プリントを行う際に製造物の情報を Blockchain 上に保存するという手法を用いる．製造物に埋め込まれた ID から Blockchain 上のデータを読み出すことで，製造物の製造情報を参照することができる．

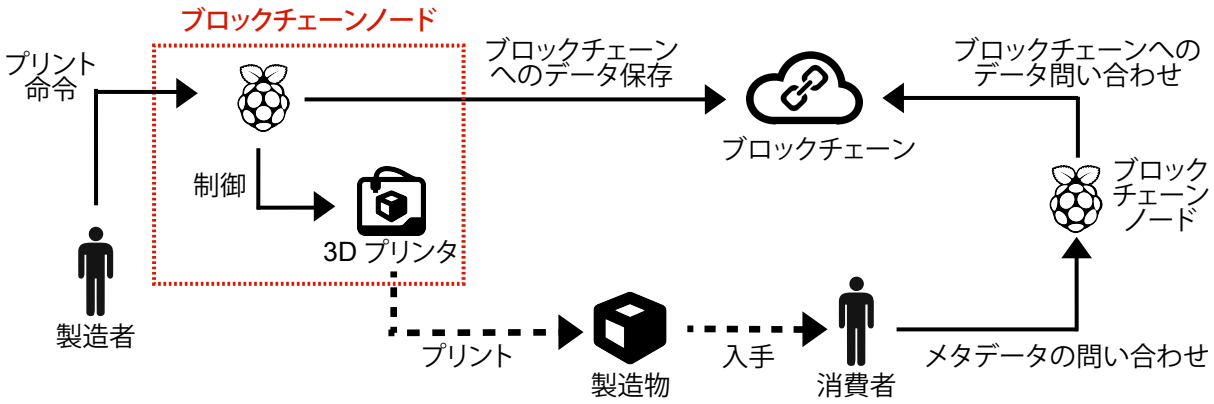
ブロックチェーンノード
プリント
命令
ブロックチェーン
へのデータ保存
ブロックチェーンへの
データ問い合わせ
ブロックチェーン
制御
ブロック
チェーン
ノード
3D プリンタ
製造者
プリント
製造物
入手
消費者
メタデータの問い合わせ

図 3.1: システム概要図

第4章　実装

本章では，3.5 節で述べた提案システムの実験として行った実装に関して説明する．

4.1　実装環境

本研究で実装するシステムを構成するためのハードウェアおよびソフトウェアについて説明する．表 4.1 に詳細なバージョンを示す．

表 4.1: 使用ソフトウェアおよびハードウェアのバージョン

ハードウェア/ソフトウェア	実装環境	バージョン
シングルボードコンピュータ	Raspberry Pi3	ModelB
3D プリンタ	simple metal	1403
3D プリンタ制御	Octoprint	1.3.0
Blockchain クライアント	Geth	1.5.8
アプリケーションフレームワーク	laravel	5.2

4.1.1　ハードウェア

3D プリンタを制御および Blockchain への製造情報の保存を行うためのシングルボードコンピュータとして Raspberry Pi3 を用いる [24]．Raspberry Pi3 は安価に購入でき，Linux ベースの OS によって動作する．そのため，Blockchain ノードとして正常に動作せることが可能である．また，USB ポートで 3D プリンタを接続し，制御するソフトウェアもいくつか存在する．

今回の実装では，3D プリンタとして printrbot 社の simple metal を用いる [25]．simple metal は SLA 法の個人向け 3D プリンタであり，比較的安価なモデルである．USB ポートによってコンピュータを接続することで制御を行うことができる．

4.1.2　3D プリンタの制御

本システムでは，3D プリンタを制御するシステムとして，Octoprint[26] を用いる．Octoprint はオープンソースの 3D プリンタ制御ソフトウェアであり，Raspberry Pi に導入

し，Web インターフェースよりプリントを行うことができる．3D モデルの形式は一般的な STL 形式ではなく，3D プリントを実際に行う際の制御コマンド体系である G-CODE 形式で入力を行う．多くの機能が RESTful な API で実装されており，3D プリンタを制御しながら他のアプリケーションへ容易に連携させることが可能である．

4.1.3 Blockchain へのデータ保存

本システムでは，Blockchain に製造情報を保存する方法として，Ethereum Blockchain の CA として保存する．Ethereum は Blockchain を用いたアプリケーション開発プラットフォームとしては最も一般的に使われている．そのため本システムで独自に Blockchain を構築し十分にスケールさせなくとも，Blockchain の高改ざん耐性を利用することができる．また，Ethereum 上で動作するプログラムはチューリング完全性を持つため，データ構造などを比較的自由に記述することができる．Ethereum のクライアントとしては，Go 言語で実装された Geth[27] を用いる．Geth は JSON-RPC による API が実装されており，プログラムから制御できる．

4.1.4 システム全体

本システムは，本節で述べた複数のソフトウェアを連携させて動作する．今回は，全体をコントロールするインターフェイスとして Web ブラウザからアクセスすることを想定した．そこで，PHP による Web アプリケーションフレームワークである Laravel[28] を用いて実装した．Laravel は 2012 年にリリースされてから急速に普及している PHP フレームワークであり，オープンソース化されている．

4.2 データ登録システム

ユーザが 3D プリントを行う際のシーケンス図を以下に示す．ユーザが 3D プリントを命令した際に JSON RPC より Ethereum 上にコントラクトをデプロイし，その CA のアドレスをプリントされる製造物の ID とする．この ID を製造物の内部に RFID を埋め込むなどで製造物と紐付け，製造物からコントラクトを呼び出すことができ，追跡可能性を担保する．デプロイされたコントラクトはマイナーによって実際にブロックへ格納され，後日改ざんすることは困難になる．

4.2.1 保存するデータ構造

製造物の製造責任の追及，および知的財産権の保証には，製造物の設計図となる 3D モデル，3D モデルの設計者，製造者，製造日時の記録が必要である．3D モデルの設計者の担保を行うためには 3D モデルにデジタル署名が埋め込まれている必要があるが，現状では埋め込まれていない．また，製造日時については，P2P ネットワークにおいて特定の

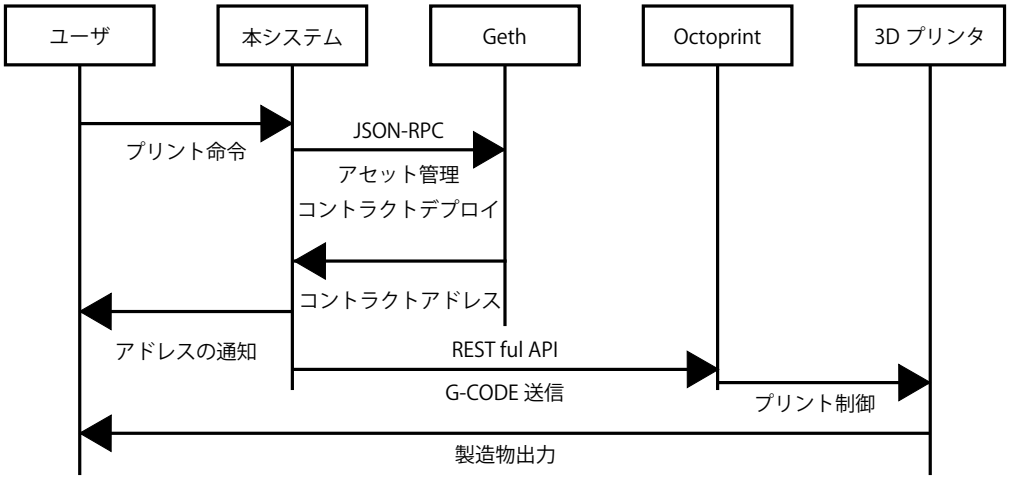

図 4.1: システムシーケンス図

ノードが述べる日時が正しいことを保証することはできないため，製造時に保存したとしても信頼出来るデータとは限らない．そこで本実装では 3D モデル，製造物の名前，製造者のみを保存する．Ethereum では 3D モデルを直接 Blockchain に保存することは Ethereum 上に保存できるデータ容量の制限により不可能なため，3D モデルのハッシュ値を保存する．ハッシュ値を参照することで，製造物をプリントした 3D モデルと同様のデータであることを検証可能とする．また，製造者のデータとしては Ethereum のアドレスを使う．

表 4.2: 保存するデータ構造

Label	データサイズ	概要
name	最大 32byte	製造物の名前
3d data hash	32byte	SHA256 を用いた 3D モデルのハッシュ値
maker	32byte	製造者の Ethereum アドレス

第5章　評価および考察

本章では，4章で実装した本研究での提案システムの評価とその考察を述べる．

5.1　評価項目

本実験システムの評価として， 3.2節で述べた要件に対して評価を行う．それぞれの評価項目について述べる．

5.1.1　公開性

本提案システムにおいては，各ノードから自由にBlockchain上に保存された情報を読みだせることが必要である．そこで本提案システムからBlockchainに製造物の情報を保存した上で，Ethereum Blockchainにアクセスすることで，本提案システムにおいて情報が十分に公開され，読み出せていることを確認した．

5.1.2　追跡可能性

本提案システムで追跡可能性を担保するためには，3Dプリントを行う製造者たちの多くが本システムを導入することが必要である．ここでいう製造者とは，パーソナルファブリケーションにおける製造者であるため，今まで製造を行っていなかった各家庭などでの製造が考えられる．また本提案システムで用いたBlockchainは，そのデータの正当性の検証のために形成されたBlockchainをGenesisブロックから全て保持する必要がある．そこで，本提案システムより発行されるトランザクションのデータサイズから本システムを用いた場合のBlockchainのデータサイズを推定し，ストレージの面で本システムの導入コストの推定を行った．

5.1.3　完全性

Blockchainの改ざん耐性に関する研究は多く行われている．中でもGervaisら[29]はProof-of-Workを採用しているBlockchainへの攻撃をマルコフ決定過程を用いてモデル化し，分析を行った．その中で，Bitcoinで攻撃者がネットワーク全体の計算パワーに対して30%を持ち，当該トランザクションを含むブロック以降6ブロック連なった場合と同等

の改ざん耐性を持つには，Ethereum においては 37 ブロック連なることが必要であると示した．Blockchain においては改ざん耐性が 0%になることはないが，ブロックが連なるにつれて 0%へ限りなく近づいていく．Satoshi Nakamoto は Blockchain に対する改ざん成功可能性 P(z) を以下の式によって示した．

- p = 善良なノードが次のブロックを見つける可能性
- q = 攻撃ノードが次のブロックを見つける可能性
- z = 最新ブロックのブロック高 - 攻撃者が改ざんを試みるトランザクションを含むブロックのブロック高
- $\lambda = z\frac{q}{p}$

$$P(z) = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (q/p)^{(z-k)}) \tag{5.1}$$

本提案システムにおいては，3D プリント開始時に CA をデプロイすることで製造物の情報を Blockchain 上に保存した．そこで，3D プリントを開始からの経過時間と共に改ざんの成功可能性の変化を上記の式を元に計算し，分析を行った．

5.2 評価と考察

5.2.1 公開性

4 章で述べた実装を行い，Ethereum プライベートネットワークを構築することで動作検証を行った．プライベートネットワークの図を 5.1，それぞれに用いた OS および Geth のバージョンを表 5.1 に示す．本システムが構築されている Raspberry Pi3 ノードをノード A，Mac OS　X のノードをノード B，Ubuntu のノードをノード C と呼ぶ．それぞれ異なるバージョンの OS，Geth を使用することで，ネットワーク上に様々な環境のノードが存在しても動作することを確認した．

表 5.1: 各ノードの OS と Geth のバージョンおよびマイニングの実行有無

Node	OS	Geth	マイニング
A	Rasbian stretch	1.5.8	×
B	Mac OS X El Capitan 10.11.6	1.4.16	○
C	Ubuntu 16.04.1 LTS	1.4.10	○

Blockchain への格納を行うマイニングは Raspberry Pi3 上では Geth の実装上行えないため，B，C ノードで行った．発行されたトランザクションが B，C ノードに渡り，マイニング後ブロックに格納され，ノード A 上の Blockchain に格納されることを確認した．実

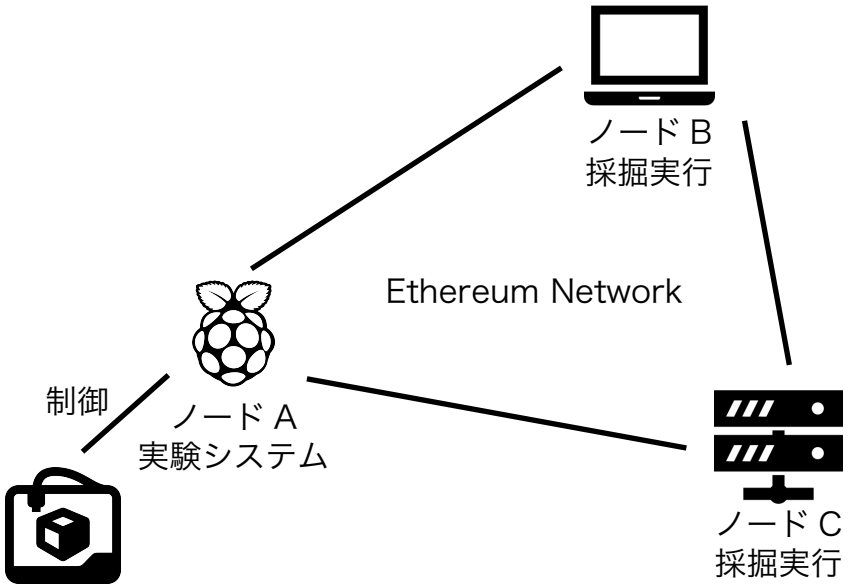

図 5.1: 動作検証プライベートネットワーク

```
ryosuke[~]$curl -X POST -H "Content-Type: application/json" --data '{"txadd":"0x
947758439d8c56cdf8656cc50773c0de750189bff49dca5c767b43c7bb1fafdf"}' http://local
host:8000/api/info
{"txadd":"0x947758439d8c56cdf8656cc50773c0de750189bff49dca5c767b43c7bb1fafdf","c
ntadd":"0xaa1f159512e61ecfb8b0e41141801a5255718bea","name":"test01\u0000\u0000\u
0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000","maker":"0x6d168
da00ac96410ebccf5104cd9a95704d3abee","hash":"e7e3438918ace490cbca217e7b8500f68ca
bd28baa291c388f618aa3b99bc7b9"}%
```

図 5.2: Blockchain に保存されたデータの読み出し

際に本システムに実装した API を用いてトランザクションのアドレスを元に Blockchain よりデータを読み出すことができた実行結果を図 5.2 に示す.

本研究の提案システムを用いた 3D プリンタでは，常にプリントを行った際は Blockchain に製造情報を保存し，Blockchain 自体は各ノードで保持されている．そのため，どの Ethereum 参加ノードでも製造物の製造情報を読み出すことが可能である．また，仮に Ethereum ライブネットで本システム動作させても製造情報の記録されている Blockchain を入手することは容易に可能であり，製造情報の公開性は担保されていると言える.

5.2.2 追跡可能性

本提案システムを使用した際の Blockchain サイズ増大を推定し，必要となるストレージ容量を推定することで，本システムのスケーラビリティを推定する.

ストレージサイズとコスト

McCallum[30] による調査を元に，$100 で購入できるストレージサイズの変化を図 5.3 に示す．2017 年現在の 100$で購入できるストレージサイズは約 3500GB である．

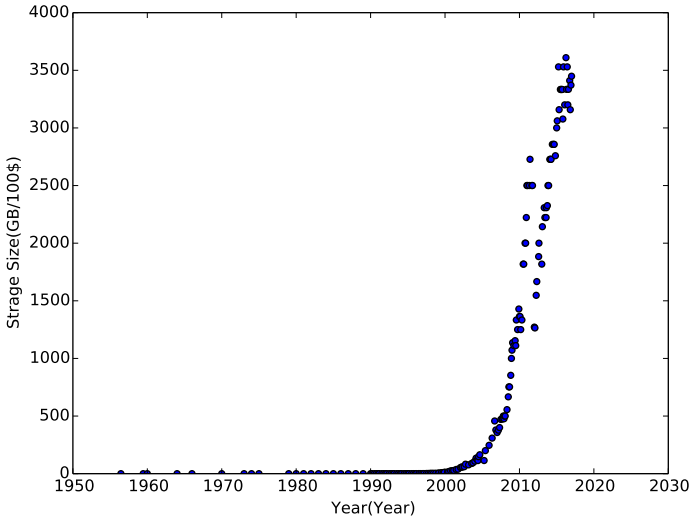

図 5.3: $100 で購入できるストレージサイズ

Blockchain サイズと 3D プリンタ台数

以下にようにそれぞれの係数を定義する．

- P = 世界の 3D プリンタの台数 (台)
- O = 年間に 1 台の 3D プリンタによって製造される製造物数 (個)
- T = 本提案システムにおけるトランザクションのデータサイズ (byte)

それぞれによって，1 年間に世界 3D プリンタで製造される製造物の数 A を以下のように定義出来る．

$$A = P * O \tag{5.2}$$

そこで，以下の式によって本提案システムを用いた場合の年間 Blockchain サイズ増加量 SIZE(byte) を定義することができる．

$$SIZE = A * T = P * O * T \tag{5.3}$$

本提案システムで発行したトランザクションを 1 件含むブロックはトランザクションを含まないブロックよりサイズが約 1500byte 大きくなった．そこで，$T = 1500$ と仮定する．

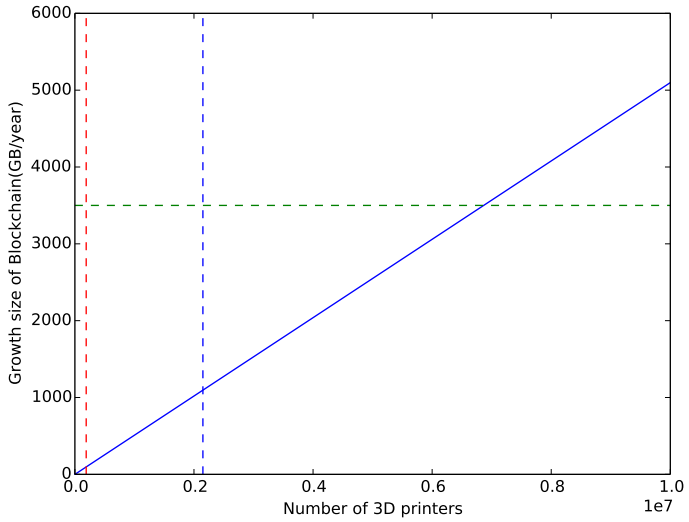

図 5.4: 3D プリンタの台数に対する年間 Blockchain サイズの増加数

仮に製造者は毎日 1 回 3D プリントを行うと仮定する．3D プリンタの台数を変化させることで，描いたグラフは図 5.4 になった．

矢野経済研究所の調査と予測による 2015 年と 2020 年における 3D プリンタの世界での出荷台数をそれぞれ赤破線と青破線で示した [31]．2015 年の世界の 3D プリンタ出荷台数は 19 万台であり，その際の Blockchain サイズの年間増加量は約 96GB である．また 2020 年に予測される 3D プリンタ出荷台数は 215 万台で Blockchain サイズの年間増加量は 1096GB である．先述の 2017 年現在$100 で購入できる 3500GB は緑破線であり，約 686 万台の時である．ストレージのサイズは今後も増加していくと考えられるため，本提案システムの導入コストはある程度に収まると考えられる．その一方で，Blockchain は増大し続けるため，永続的に本提案システムを使うためには継続してストレージ容量を追加しなければならず，各個人で Blockchain を維持する際はコストが増大し続けることになる．

5.2.3 完全性

5.1.3 節で示した式を元に，Ethereum におけるブロック生成間隔を 15 秒として，時間を変数へ拡張する．3D プリント開始からの経過秒数を s とすると，改ざん成功可能性 P(s) は以下の式となる．

$$P(s) = 1 - \sum_{k=0}^{\lfloor s/15 \rfloor} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (q/p)^{((\lfloor s/15 \rfloor)-k)}) \tag{5.4}$$

この関数より以下の仮定でそれぞれグラフを描くと，図 5.5 のようになる．

- 攻撃者 A p = 0.1

- 攻撃者 B p = 0.3

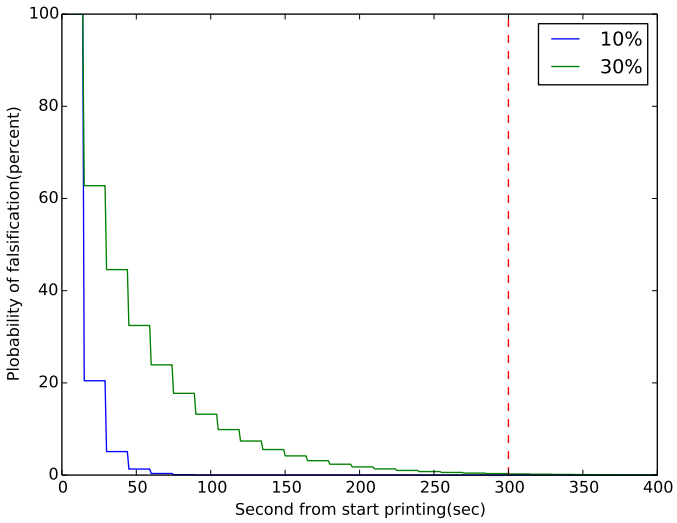

図 5.5: 時間経過と改ざん成功可能性

3D プリントの完了までかかる時間は製造物の大きさや 3D モデルの複雑さ，3D プリンタの性能に影響を受ける．本提案システムで用いた 3D プリンタである Printrbot 社の Simple Metal で 1cm 四方の立方体を出力する時間は，約 9 分であった．そのため，実用的な製造物をプリントする際は，少なくとも 5 分の時間がかかると仮定する．本提案システムではプリント開始と同時にコントラクトを Ethereum Blockchain にデプロイする．プリント開始から 5 分後の改ざん成功可能性は攻撃者 A は約 0.0000000056%，攻撃者 B は約 0.2480397604%である．その後時間経過と共に改ざん成功可能性は 0%へ近づいていく．

攻撃者が Blockchain を改ざんする状況を想定すると，自分の製造物によって事故が起こった際の責任逃れが考えられる．そうした状況で改ざんを行うのは 5 分後時点より後であると考えられ，尚且つ製造から流通し，消費者の手に渡った後であることを考えると改ざんが成功するのは極めて低い可能性であると言える．

5 分後の改ざん成功可能性を，攻撃者のブロック発見可能性 p を変数としてグラフを描くと，図 5.6 のようになった．2017 年 1 月現在，Ethereum ライブネット上のマイナーで最大のハッシュレートを持つマイナーは全体の約 23%のハッシュレートを維持している [32]．20%の確率で攻撃者がブロックを発見する時の 5 分後の改ざん成功可能性は約 0.0001742798%である．そのため実運用上でも，3D プリントが完了してから改ざんを試みたとしても，改ざんが成功する確率は非常に低いと言える．

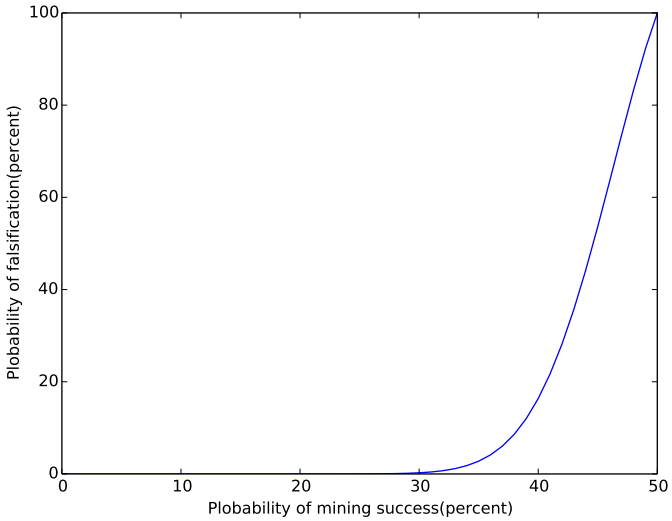

図 5.6: 攻撃者ブロック発見確率と 5 分経過後の改ざん成功可能性

第6章　結論

本章では，本研究のまとめと今後の課題を示す．

6.1　本研究のまとめ

本研究では，個人的にものづくりを行うパーソナルファブリケーションにおいて，製造責任と知的財産権の所在を明らかにするために，Blockchain 技術を用いた 3D プリントにおける製造情報保存システムを提案した．パーソナルファブリケーションにおける製造責任と知的財産権の所在を明らかにするには，データの公開性，追跡可能性，完全性が求められる．そこで，実験システムとして，Raspberry Pi3 より 3D プリンタを制御し，Ethereum Blockchain 上に 3D プリント実行時に製造物の名前，製造者，3D モデルのハッシュ値を保存するシステムを実装した．3 点の要求に対して，実験システムでそれぞれが満たせるかを検証した．プライベートネットワークを構築し，Blockchain からデータの読み出しが行えることから，データの公開性が担保されていることを確認した．また，追跡可能性は本システムのスケーラビリティに影響を受ける．そこで，3D プリンタの数と本システムを使用した時に Blockchain を維持するために各ノードが持たなければならないストレージ容量から本システムの導入コストを推定した．その結果，継続して本システムを使い続けると Blockchain のサイズが増大し続け，個人で維持するためには課題が残ることが明らかになった．時間経過と Blockchain の改ざん耐性を推定することで，本システムにおける改ざんを行う状況を考えると，改ざんが成功する確率が非常に低いことを確認した．

本システムを用いることで，パーソナルファブリケーションといった小規模な製造でも製造情報を公開し，製造物の責任や権利の所在を明らかにすることができる．また，3D モデルのハッシュ値を保存しているため，特定の 3D モデルで作られたものであることも証明できる．3D モデルが盗用された場合，その製造情報を参照することで，同一の 3D モデルから作成していれば，検出することが可能である．

6.2　本研究の課題と展望

本節では，本研究で提案したシステムの課題と展望について述べる．これらの課題は，Blockchain 技術に依存する問題もある．今後，Blockchain 技術を用いるべきかを含めて，パーソナルファブリケーションにおける 3D モデルの二次利用などを考慮した，システム的側面，社会制度的側面，両側面からの検討が必要である．

6.2.1 製造者のインセンティブ設計

本システムでは製造物の製造情報を保存することで，製造責任や知的財産権の所在を明らかにするシステムを提案した．しかし，本システムは製造者が 3D プリンタを使う際に本システムを使うことで，製造責任を問われる可能性や，知的財産権の侵害が公開されてしまうという製造者にとってのデメリットとして捉えることもできる．また，Ethereum のコントラクトをデプロイするため，そのための手数料として gas が必要とされている．そこで，製造者にとって本システムを利用することに対するインセンティブの設計が必要である．この問題は，3D モデルの 2 次利用が盛んに行なわれていることも踏まえた知的財産権の制度面での設計を行うことも一つの解決手段として考えられる．

6.2.2 3D モデルの改変の追跡

本システムでは 3D モデルのハッシュ値を保存している．そのため，3D モデルを改変して製造を行った場合，元の 3D モデルと改変後の 3D モデルの関係性を証明することはできない．その一方で，パーソナルファブリケーションにおいては，3D モデルなどの 2 次利用が盛んに行なわれている．その中で，製造物の 3D モデルはどこのモデルのフォークなのか，類似の 3D モデルから製造されたものは何か，ということも重要な情報である．そのため，それらの追跡ができることもパーソナルファブリケーションにおける製造物のデータ管理として必要であると考えられる．また，知的財産権の保障の面でもこれは重要なことである．2 次利用を追跡できることで，知的財産権を正当に譲渡された 2 次利用であるかを検証することも可能となるだろう．

Ethereum 上でソフトウェアのソースコードを Git 管理するコントラクトを構築するプロジェクトがある [33]．パーソナルファブリケーションにおいてはソフトウェア開発におけるオープンソースと同じように，他人の作成した 3D モデルを複製し改変することや，3D モデル製作者以外によるの 3D モデルの改変を元の 3D モデルに取り入れられることがある．そのため，Git 管理のようなオープンソースの考え方を 3D モデルの管理に取り入れることは多くの可能性を持っていると考えられる．

社会制度面でも，現在は 3D モデルの製作者だけにその知的財産権は帰属する．しかし，それに改変を加えた 2 次利用者にも，改変部分の権利を与えるなどの取り組みの検討が行なわれている．元々の製作者本人だけでなく，パーソナルファブリケーションにおける適切な権利管理を制度面から検討することも必要である．

6.2.3 3D モデル自体の Blockchain 上への保存

3D プリントを行う際に使われた 3D モデルに関して，本システムでは 3D モデルのハッシュ値のみを保存している．そのため，後日検証する際に製造者が 3D モデルを保持しておらず，再入手，作成も困難な場合，3D モデルを確認することはできない．よって，本システムだけでは製造責任を追及するための根拠とすることはできない．そのため実際に 3D モデルを直接 Blockchain 上に保存することが考えられる．しかし，Ethereum では保存

できるデータ容量は文字列であれば，最大 32byte である．これは，コントラクトとして大きなデータを保存することで，各ノードが持つ Ethereum Blockchain が急速に肥大化してしまうため，保存できるデータサイズに制限をかけているためである．これは Blockchain 技術自体の特性として，トランザクションの検証の為に全てのノードが Genesis ブロックから最新まで全てのブロックを持たなければならないことが原因である．仮に上限がなければ，本システムを採用した場合，本システムを利用した 3D プリンタで製造されたものの 3D モデルを参加者全員が保持することになり，ストレージの上限から現実的ではない．

これは将来的にはパブリックなストレージが存在すれば，解決できる問題であると考えられる．Blockchain 技術を応用した storj[34] は，断片化したファイルを暗号化し，参加ノードのコンピュータに分散的に保存するシステムである．ストレージを提供したノードにはデジタル通貨が支払われる．このようなパブリックストレージ技術を応用することで，本システムにおいても 3D モデルの追跡可能性を担保することが可能になるだろう．

6.2.4 物流への応用

Blockchain 上で物流における物の所有権を管理する試みがある [35]．パーソナルファブリケーションのような個人で製造した製造物の物流管理を P2P ネットワークである Blockchain 技術で行うことは，有用性があると考えられる．また本システムで保存した製造物の情報を物流へ応用することは可能であると考えられる．

しかし，3D プリントは必ず正確にプリントが完了するとは限らない．プリント中に 3D プリンタへ振動が加わる，部屋の温度をはじめとした 3D プリンタの周辺環境など様々な要因でプリントが失敗する可能性がある．そうした際に，本システムではプリント命令をした時にすでに Ethereum 上にコントラクトをデプロイしているため，製造物の製造情報が製造が完了しなくとも Blockchain 上に保存されることになる．また，Ethereum 上にデプロイするコントラクトのソースコードを参照することで，直接 Ethereum へ製造していない製造物の情報を保存することも可能である．本システムを物流システムと連携させた場合，作られていない製造物の権利を転移させることが可能である．例えば 3D プリンタで製造した Blockchain 上のデータを参照し，通信販売を行うことを考えると，実際に商品は存在しないにも関わらず，商品があるかのように見せかけることができてしまう．そのため，製造物の廃棄や，未完成品の製造情報における定義が必要である．

謝辞

本論文の執筆にあたり，ご指導頂いた慶應義塾大学環境情報学部村井純博士，同学部教授徳田英幸博士，同学部教授中村修博士，同学部教授楠本博之博士，同学部准教授高汐一紀博士，同学部教授三次仁博士，同学部准教授植原啓介博士，同学部准教授中澤仁博士，同学部準教授 Rodney D．Van Meter III 博士，同学部教授武田圭史博士，同大学政策・メディア研究科特任准教授鈴木茂哉博士，同大学政策・メディア研究科特任助教中島博敬氏，同大学政策・メディア研究科特任准教授佐藤 雅明博士，同大学政策・メディア研究科特別招聘教授下村健一氏，同大学 SFC 研究所上席所員斉藤賢爾博士に感謝致します．

特に斉藤氏には重ねて感謝致します．研究活動の中で，デジタル通貨や Blockchain に関する氏からの多くの助言がなければ，本論文のテーマで書ききることはできませんでした．また，下村氏にも重ねて感謝致します．氏の授業内で Bitcoin に関する講義をさせていただき，“人に伝える”ということの難しさ，楽しさを経験させていただいたことは研究活動の中で確実な力となりました．

徳田・村井・楠本・中村・高汐・バンミーター・植原・三次・中澤・武田合同研究プロジェクトに所属している学部生，大学院生，卒業生の皆様に感謝致します．中でも慶應義塾大学政策・メディア研究科峯木厳修士，同大学政策・メディア研究科後期博士課程永山翔太氏には研究室での振る舞いや論文執筆にあたり，多くのことを指導して頂きました．

また NECO グループとして意見交換をした，小山忠氏，波玉純氏，後上峻一氏，藤ヶ谷康平氏，諸澤正樹氏，塚越広彬氏，加藤奈美女史，相川美菜子女史，田中公人氏，渡部貴博氏，瀬川雅弘氏，板垣孝明氏，鎧坂文菜女史，押見太雄氏，菅藤佑太氏，佐々木優子女史，森島隆成氏，倉田志門氏，金子浩幸氏，島津翔太氏，大友和幸氏，宮本眺氏に感謝致します．至らない KGL である自分を支えてくれた氏らがいなければ，本論文の執筆に集中することはできませんでした．

研究室生活の中で多くを共にした，黒米祐馬氏，鈴木恒平氏，木下舜氏，東海林晃氏，尾崎周也氏，桑原誠尚氏，河口綾磨氏，栗原祐二氏に感謝致します．氏らと楽しく研究室生活を送れたことで，本論文を書ききる活力となりました．

藤沢剣友会の同期，芦澤智氏，大網修平氏，長谷川優太氏を始めとした会員全員に感謝致します．氏らと稽古することは研究生活の中での大きなストレス発散となりました．

第二十五回七夕祭実行委員会に感謝致します．実行委員の中で，Web 制作を担当させていただいた経験は自分のエンジニアとしての力量不足を痛感し，プログラミングの学習に励むきっかけとなりました．

Layout my Torturechamber のメンバーに感謝致します．彼らの理解がなければ，研究活動とバンド活動を両立することはできませんでした．

山崎綾香女史に感謝致します．自身の生活が忙しい中，自分と様々な議論を交わしなが

ら，研究生活を精神面から支えて頂きました．
細川毅騎氏に感謝致します．氏の誘いがなければ自分がこの研究室に所属することはありませんでした．また，4 年間を通じて生活から研究のことまで多くのことを語り明かしたことは自分の大学生活の欠かせない時間でした．
ここには書ききれない，自分の 23 年間の人生の中で出会った全ての人に感謝致します．全ての関わりがあったからこそ，現在の自分に至り，この成果を生むことが出来ました．
最後に，4 年間を通じて，多くの残留などで家に帰らない好き勝手な生活をしていた私を，陰ながら応援し支えてくれた祖父 小久保博義，祖母 小久保基子，父 裕一，母 洋子，兄 洵介，姉 蕗子に深く感謝いたします．

参考文献

[1] Blockchain.info. Hashrate distribution. https://blockchain.info/ja/pools.

[2] Thingiverse. http://www.thingiverse.com/.

[3] Worldwide spending on 3d printing forecast to grow at a compound annual rate of 27http://www.idc.com/getdoc.jsp?containerId=prUS40960716, 2016.

[4] Fablab japan. http://fablabjapan.org/.

[5] 全日本空輸株式会社. 3d プリント義足を共同開発. http://www.ana.co.jp/group/pr/201608/20160829-2.html.

[6] 福田香子 and 田中浩也. 個人の身体に関する 3d スキャンデータと, その実物大 3d プリント品に対する鑑賞者の行動と考察:「i am」 の制作を通して. **日本バーチャルリアリティ学会論文誌**, 21(3):437–445, 2016.

[7] Catarina Mota. The rise of personal fabrication. *Proceedings of the 8th ACM conference on Creativity and cognition*, pages 279–288, 2011.

[8] 田中浩也. パーソナルファブリケーション時代におけるものづくりのオープンソース化の動向と fab commons の提案. **情報処理**, 54(2):127–134, 2013.

[9] Ken Fujiyoshi, Chihiro Fukai, Hiroya Tanaka, Jin Mitsugi, and Jun Murai. Rfid 3d printing objects that connote information. *NIP & Digital Fabrication Conference 2014 1*, pages 316–319, 2014.

[10] 小玉秀男. 立体図形作成装置. **特開昭** *56-144478*, 1980.

[11] 消費者庁. 第 13 次 国民生活審議会 消費者政策部会報告 製造物責任制度の在り方. http://www.caa.go.jp/seikatsu/shingikai2/kako/spc13/houkoku_g/spc13-houkoku_g-4-1.html, 1992.

[12] 鹿児島地裁平成 20 年 5 月 20 日判決. **判例時報**, 2015 号, 2008.

[13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf, 2008.

[14] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

[15] Proof of existence. https://proofofexistence.com/.

[16] Namecoin. https://namecoin.org/.

[17] Vitalik Buterin. "a next-generation smart contract and decentralized application platform." white paper. https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, 2014.

[18] 渋田拓也. 単一グローバル台帳暗号通貨のエクリプス攻撃脆弱性分析. **慶応義塾大学政策・メディア研究科修士論文**, 2015.

[19] Kenji Saito and Hiroyuki Yamada. What's so different about blockchain?—blockchain is a probabilistic state machine. In *Distributed Computing Systems Workshops (ICDCSW), 2016 IEEE 36th International Conference on*, pages 168–175. IEEE, 2016.

[20] Ethereum classic. https://ethereumclassic.github.io/.

[21] 総務省. 「ファブ社会」の展望に関する検討会 報告書. http://www.soumu.go.jp/main_content/000299339.pdf, 2014.

[22] Karl DD Willis and Andrew D Wilson. Infrastructs: fabricating information inside physical objects for imaging in the terahertz region. *ACM Transactions on Graphics (TOG)*, 32(4):138, 2013.

[23] Everledger. http://www.everledger.io/.

[24] Raspberrypi. https://www.raspberrypi.org/.

[25] printrbot simple metal. https://printrbot.com/product-category/3d-printers/simple-metal/.

[26] Octoprint. http://octoprint.org/.

[27] geth. https://github.com/ethereum/go-ethereum/wiki/geth.

[28] laravel. https://laravel.com/.

[29] Arthur Gervais, Ghassan O Karame, Karl Wust, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains.

[30] John C. McCallum. Disk drive prices (1955-2017). http://www.jcmit.com/diskprice.htm.

[31] 矢野経済研究所. 3 Dプリンタ世界市場に関する調査を実施（2016 年）－産業用ハイエンド 3d プリンタ好調 最終製品の造形が進む－.

[32] Etherscan. Top miners by blocks pie chart. https://etherscan.io/stat/miner.

[33] Ethergit. http://ethergit.io/.

[34] Storj. https://storj.io/.

[35] 豊田健太郎, 笹瀬巌, 大槻知明, et al. 偽物商品流通防止に向けたブロックチェーンを利用した商品所有権管理システム. **コンピュータセキュリティシンポジウム** *2016* **論文集**, 2016(2):696–703, 2016.