「マルチメディア，分散，協調とモバイル
(DICOMO2017) シンポジウム」 平成29年6月

パーソナルファブリケーション時代における Blockchain を用いた製造情報保存システム

阿部 涼介[1]　斉藤 賢爾[2]　村井 純[3]

概要：デジタルファブリケーションの普及を背景に，インターネット上で公開された設計図データを入手し，個人の環境に合わせて改変，製造を行うといった，パーソナルファブリケーションと呼ばれる個人的な製造が積極的に行われている．そうした中で，個人で製造物の製造者，設計者のデータを管理しておくことは困難である．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においては公開性，完全性，追跡可能性の 3 点が求められる．そこで，本研究では 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 Blockchain を用いて製造物の情報の保存を行うことで 3 点の要件を担保できると考えた．実験システムとして，Raspberry Pi3 で 3D プリンタの制御を行いプリント実行時に Ethereum Blockchain 上に製造物の情報を保存するシステムを実装した．上記 3 点の要件に対して評価を行い，要件が満たされていることを確認した．

Product Information Storage System Using Blockchain in Personal Fabrication Era

RYOSUKE ABE[1]　KENJI SAITO[2]　JUN MURAI[3]

1. 序論

1.1 デジタルファブリケーションと 3D プリントの普及

デジタルファブリケーションとは，コンピュータで制御される 3D プリンタやレーザカッタを始めとし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．

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．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 [1]．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．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．また，福田 [2] は自身の実物大の 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．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 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 [3]．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 [4]．

[1] 慶應義塾大学大学院 政策・メディア研究科
[2] 慶應義塾大学 SFC 研究所
[3] 慶應義塾大学 環境情報学部

1.3 本研究の問題

現在のパーソナルファブリケーションでは個人での製造において，製造責任の追及や知的財産権の保護のために，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．またそれらの情報の更新をする必要性もある．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護を行う為には，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 [5]．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，製造責任や知的財産権の所在を明らかにし，その管理ができるシステムを提案した．

1.4 本研究の仮説

デジタル通貨 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，前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し，管理することが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，アプリケーションを記述できるよう拡張された Blockchain である Ethereum の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し，その権利保持者を転移できることを確認し，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する．

2. 既存の法整備と基礎技術

2.1 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 [6]．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 法は，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．

2.2 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．

2.2.1 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，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．この法制度により，製造物に対しては製造者による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 [7]．この裁判では，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．その一方で，必ずしも設計者が製造者ではないパーソナルファブリケーションにおいて，製造者または設計者個人に

製造責任を追及することは，議論の余地がある．しかし，製造物の設計者および製造者の情報の履歴が管理されていることは，責任の所在を明らかにする過程で必要な要件である．

2.2.2 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護され，権利者に無断な複製および製造を制限している．

パーソナルファブリケーションにおいては，データを改変し二次利用することが広く見られる．そのため，製造者は必ずしも設計者であるとは限らない．また，そうした二次利用をした際の “改変を行った” という二次利用者が付与した付加価値をどのように扱うべきは，法制度面での課題でもある．その検討のためにも，設計者の情報及び来歴が保存されるシステムが構築されることは，その議論の具体化に貢献できるものである．

2.3 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，Financial 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．

2.4 Blockchain 技術と Bitcoin

Bitcoin [8] は，Satoshi Nakamoto[*1]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 を形成する（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．）．Bitcoin では，トランザクション[*2]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．

ブロックチェーンは図 1 に示すように，一定取引をまとめたブロックの暗号学的ハッシュ値を次のブロックに含めることによってブロックを連鎖させた構造を持つ．ブロックは，“マイナー”と呼ばれるノードによって生成される．Proof-of-Work と呼ばれる計算パワーを必要とする作業をしなければブロックを生成できなくすることで，ブロックの生成は困難になっている．そのため，過去のブロックの中のデータを改ざんすれば，後続のブロックに格納されているデータを持つブロックを正しく連鎖させるよう計算パワーを投入し生成しなければならない．過去のブロックを再生成している間にも改ざんされていない Blockchain に連なるように善良なノードによってブロックは生成されている．ネットワーク全体は典型的には最も長い（最も累積で計算パワーが投入された）Blockchain を採用する．それにより，過去のブロックを改ざんした上で新たに最長の Blockchain を作成することは，攻撃者が参加マイナー全体の 50%超の計算パワーを保持しなければ困難であるため，Blockchain は高い改ざん耐性を持つ．

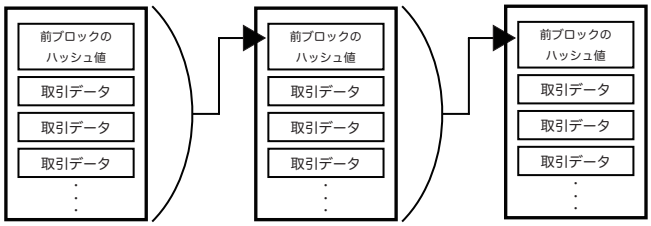

図 1 Blockchain の構造

2.5 UTXO とスクリプトによる状態遷移の記述

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ができる．

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．アウトプットには，そのアウトプットを使用

[*1] Satoshi Nakamoto を名乗る匿名の個人または集団．

[*2] 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．

する条件を記述したスクリプトを含んでいる．そのスクリプトを解錠する条件を記述することでBTCの支払いを可能にする．つまり，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で表現してるのである．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に示す．

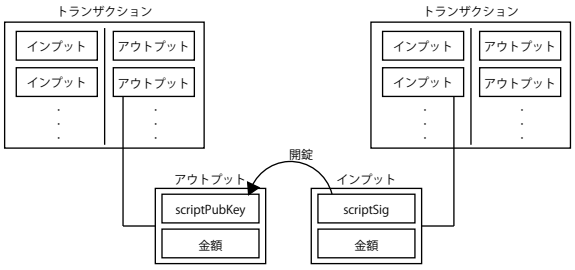

図 2 トランザクションの構造とスクリプトによる開錠

2.6 Ethereum

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，そのデータの取り扱いをスクリプトによって自由に記述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．その一方で，Bitcoinのトランザクションのスクリプトで用いるプログラミング言語はチューリング不完全になっている[*3]．そのため，高度なアプリケーションの開発は，アプリケーションのソースコードも難読化しやすく，困難である．そこで，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アプリケーションプラットフォームであるEthereumがある[9]．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ってブロックへトランザクションを格納してもらうことができ，Blockchain技術の高改ざん耐性を利用できる．

プログラムはトランザクションを発行することでコントラクトアカウント(Contract Account，CA)としてBlockchain上にデプロイされる．各ユーザは外部所有アカウント（Externally Owned Account，EOA）と呼ばれるアカウントを持ち，内部通貨であるEtherを保持する．CAとEOAにはそれぞれEthereum Blockchain上で一意なアドレスを持つ．CAのプログラムは，CAのアドレスを指定し，EOAやCAからトランザクションを発行することで実行することができる．コードの実行結果である状態遷移はBlockchain上で行われるため，参加ノード全体で共有される．

[*3] これは，チューリング不完全にすることによってスクリプトの無限ループでDoS攻撃を起こすことなどを不可能にするためである

Ethereumでは“gas”と呼ばれる単位でコードの実行ステップを表現する．実行するステップ最大値を指定し，実行ステップ数に応じた手数料を支払う仕組みにより，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”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不可能である．

3. 問題定義と仮説

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[10]．例えば危険責任に関して，3Dプリンタで出力を行う者は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，必ずしもその製品に関して設計上の欠陥を把握しているとは限らない．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，Blockchainを用いることで，製造責任と，知的財産権の所在を明らかにできるようにし，それらの情報を正当に更新するシステムを提案する．

本研究では，保存する情報が実際に製造責任の追及や，知的財産権の保護を行うための証拠とされることまでは扱わない．3Dプリントにおける製造元及び設計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の開示を請求できるため，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．

3.1 問題解決における要件

パーソナルファブリケーション時代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．

3.1.1 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，利用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設計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．

3.1.2 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．

3.1.3 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．また，その情報の更新は正当にその権利保持者でなければ行えないシステムでなければならない．

3.2 先行事例

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 [5]．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 [11]．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．

Blockchain の改ざん耐性と，それによる過去の存在証明を利用した応用に Proof of Existence [12] 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 Bitcoin Blockchain に格納させることによって，トランザクションが Bitcoin 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．Bitcoin 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．

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 [13]．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．主に紛争地域などで生産され，紛争の資金源とされる所謂 “ブラックダイヤモンド”を排除するために，Blockchain を用いて取引の公開性を担保している．

3.3 本研究における仮説

本研究では 3.1 節で述べた公開性，追跡可能性，完全性を担保しながらパーソナ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．

3.3.1 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．

3.3.2 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，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．

3.3.3 完全性

Blockchain は，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．また，スマートコントラクトによって，保存された情報の更新はその権利者しか行えないシステムを構築できる．

3.4 提案システム概要

提案システムの概要を図 3 に示す．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．

4. 実装

本章では，前章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．

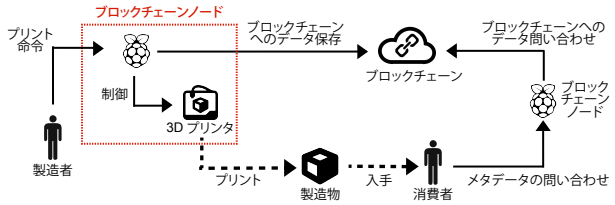

図 3 システム概要図

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 1 に詳細なバージョンを示す．

表 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 を用いた [14]．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させ，ノード群を作成し運用することも可能である．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 を用いた [15]．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 [16] を用いた．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 上に CA として保存した．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，情報更新のアクセス権の記述も容易である．Ethereum のクライアントとしては，Go 言語で実装された Geth [17] 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 [18] を用いて実装した．

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．

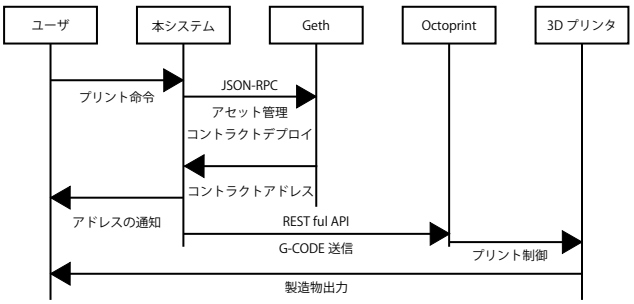

図 4 システムシーケンス図

4.3 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，製造日時，3D モデルの設計者，製造者，の記録が必要である．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 モデルの暗号学的ハッシュ値を保存する．暗号学的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，製造者および設計者のデータとしては Ethereum の EOA アドレ

スを使う．本実験システムで保存する情報のデータ構造を図 2 に示す．

表 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
date	8byte	製造日時のタイムスタンプ
3d data hash	32byte	SHA256 による 3D モデルの暗号学的ハッシュ値
designer	20byte	設計者の Ethereum アドレス
maker	20byte	製造者の Ethereum アドレス

5. 評価

前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， 3.1 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 では，そのデータの正当性の検証のために形成された Blockchain を各ノードが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 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
- $\lambda = z\frac{q}{p}$

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

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 プリントの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

前節で述べた項目について評価を行った結果を述べる．

5.2.1 公開性

本論文で述べた実験システムの実装を行い，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を図 5，それぞれに用いた OS および Geth のバージョンを表 3 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．

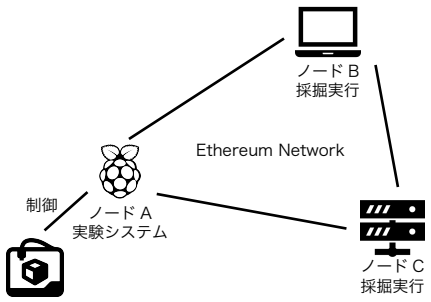

図 5 動作検証プライベートネットワーク

表 3 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 では Geth の実装上行えないため，ノード B，ノード C で行った．発行されたトランザクションがノード B，ノード C に渡り，どちらかでマイニング後ブロックに格納され，ノード A へそのブロックが渡った後，ノード A の Blockchain に格納されることを確認した．実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ノード B 上の Blockchain よりデータを読み出すことができた．

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．

5.3 追跡可能性

本提案システムを使用した際の Blockchain サイズの増大を推定し，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．

5.3.1 ストレージサイズとコスト

McCallum [19] による調査を元に，$100 で購入できるストレージサイズの変化を図 6 に示す．2017 年現在の 100$で購入できるストレージサイズは約 3500GB である．

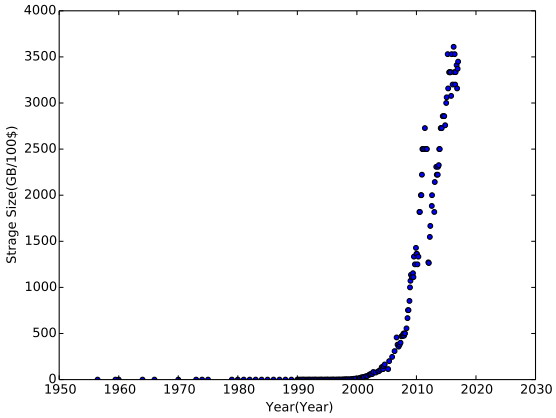

図 6 $100 で購入できるストレージサイズ

5.3.2 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．

$$A = P * O \tag{2}$$

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．

$$SIZE = A * T = P * O * T \tag{3}$$

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．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 7 になった．

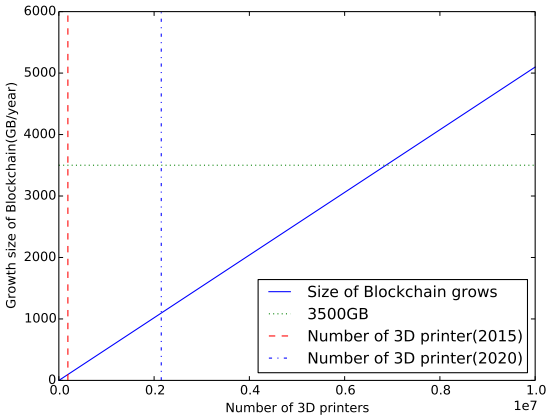

図 7 3D プリンタの台数に対する年間 Blockchain サイズの増加数

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示した [20]．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 で購入できるストレージサイズは 3500GB 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．

5.4 完全性

5.1.3 項で示した式を元に，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．

$$P(s) = 1 - \sum_{k=0}^{\lfloor s/15 \rfloor} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (q/p)^{((\lfloor s/15 \rfloor)-k)}) \tag{4}$$

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．

本システムにおいて攻撃者が 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，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．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 8 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 [21]．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．

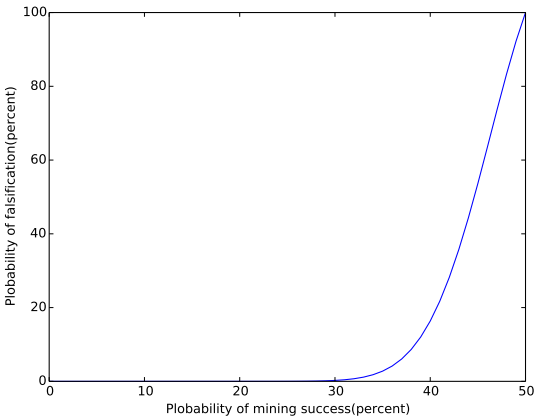

図 8 攻撃者ブロック発見確率と 5 分経過後の改ざん成功可能性

6. 結論

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できるようにするには，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，製造日時，3D モデルのハッシュ値，3D モデルの設計者，製造者を保存し，設計者と製造者の更新のでき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．

6.1 本研究の課題

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．

6.1.1 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なることもある．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．

6.1.2 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派生なのか，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，知的財産権の保護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，設計者により正当に許可された 2 次利用であるかを検証することも可能となるだろう．

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．

6.1.3 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，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 [22] 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．

6.1.4 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 [23]．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．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．

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．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．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．

参考文献

[1] 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.

[2] 福田香子, 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, Vol. 21, No. 3, pp. 437–445, 2016.

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

[4] 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, Vol. 54, No. 2, pp. 127–134, 2013.

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

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

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

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

[9] 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.

[10] 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.

[11] Karl DD Willis and Andrew D Wilson. Infrastructs: fabricating information inside physical objects for imaging in the terahertz region. *ACM Transactions on Graphics (TOG)*, Vol. 32, No. 4, p. 138, 2013.

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

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

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

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

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

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

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

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

[20] 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－.

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

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

[23] 豊田健太郎, 笹瀬巌, 大槻知明ほか. 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, Vol. 2016, No. 2, pp. 696–703, 2016.