ブロックチェーン技術を用いた車両データ・製品トレーサビリティデータの改ざん防止

Development of Blockchain Technology to Protect Mobility Data and Traceability Data

岡部 達哉 Tatsuya OKABE
三谷 陽 Akira MITANI
徐 昕 Xin XU
坂本 快矢統 Hayato SAKAMOTO
水摩 智 Satoshi MIZUMA
並木 陽彦 Haruhiko NAMIKI
黄 浩倫 Haolun HUANG
田村 由佳 Yuka TAMURA

Blockchain technology was born in 2008 to realize the cryptocurrency of bitcoin. Since the blockchain was originally developed for cryptocurrency, the blockchain was often treated as the same meaning of the cryptocurrency. However, due to its capability of difficulty for tampering of data and its transparency, the blockchain has been often used to manage the data. In this paper, we have tried to apply this blockchain technology to utilize its capability into the mobility service using CAN data and the traceability of products.

Key words :
Blockchain, Data management, Mobility service, Traceability

1. まえがき

仮想通貨を支えるブロックチェーン技術[1]は，データ改ざんが困難かつ透明性の高いデータ管理手法として注目を浴びている．一方，2008年に生まれた非常に新しい技術である為に定義が明確ではない等の混乱があるのも事実である．

本論文では，次章で紹介するような①分散台帳，②合意形成アルゴリズム，③ハッシュチェーンの3つの技術を持ったものを融合的にブロックチェーンと呼ぶ．なお，一部の技術のみを使うケースも後述するが，それは別途明記をする．

元々は仮想通貨を支える技術として生まれたブロックチェーンではあるが，近年では本来の仮想通貨での使用以外に，スマートコントラクトに代表されるような各種契約にも使われるようになっており，ブロックチェーン2.0とも言われている．さらにはブロックチェーン上で動作するプログラムをブロックチェーンに入れることで，プログラムの信頼性を確保しようとするブロックチェーン3.0という動きも出ており，ブロックチェーン活用が急速に広がりつつある[2) 3)]．

このブロックチェーンを車のデータ管理やサプライチェーンの管理に使おうという動きも出ている[4) 5)]．例えば，Volkswagenは車両データ管理のためにIOTAと連携してDigital Car Passを[6)]，Renaultは車両の管理を一元化し信頼性を保証するためのDigital Car Maintenance[7)]を，Daimlerはエコ運転の報酬としてmobiCOIN[8)]を開発中であり，車領域でもブロックチェーン活用の動きは活発である．

また，食料品のトレーサビリティや公文書の改ざん

防止に使うという動きも活発である．例えば，日本ジビエ振興協会では，ジビエの安全性確保の為に流通経路や安全性検査をブロックチェーンでデータ改ざんが出来ない状況で管理する取り組みを開始している[9]．また，エストニアでは公文書をブロックチェーンで管理し，不正な改ざんが出来ない取り組みを行っている[10][11]．

これらの技術的な背景と世の中の動向を踏まえ，本論文ではブロックチェーンを MaaS（Mobility as a Service）で重要となる車両データの管理，車両製造過程のトレーサビリティ管理に適用したので，その結果を報告する．

2. ブロックチェーン技術の概要

2.1 分散台帳技術（Distributed Ledger）

ブロックチェーンは，Fig. 1 に示すように，マスタースレーブ型のような中央集権的なネットワーク構造を持たず，全ての参加者（ノード）が同等として扱われる．データは全てのノードで等しく保管されており（分散台帳），その為にデータの改ざんがあっても，すぐに検出が可能である．例えて言うならば，全てのデータや取引きを即時に新聞として公開してしまうという考え方である．データを全てのノードで等しく保管をしている為に，例えば 2009 年にスタートしたビットコインにおいても，致命的なサービス停止が一度もないという安定したサービスが可能となっている．これは，一部のノードに故障などの障害があっても，他のノードが補完することで，全体システムが動作するためである．

2.2 合意形成アルゴリズム（Consensus Algorithm）

ブロックチェーンでは，ネットワーク上にどのような参加者がいるか分からない状態で，データのやり取りをすることが前提になっている．全ての参加者が正しいデータのやり取りをしているとは限らない為，データの正当性を全員で合意しながらデータを分散台帳上に追記する必要がある．このようなビザンチン将軍問題に対して，Proof of Work（POW）という仕事量による証明という考え方を用いている．すなわち，参加者（マイナーと呼ぶ）にある一定の仕事（マイニングと呼ぶ，後述）をさせ，最も仕事をした参加者に報酬を与えるというものである．データ改ざんをする為に必要な仕事量よりも，報酬を得る為の仕事量の方が少なくなるような設計となっており，データ改ざんが起こらないような仕組みとなっている．ただ近年では，このマイニングに膨大な計算リソースと膨大なエネルギーが必要なことが問題となっており，参加者を限定する許可型ブロックチェーン（Permissioned Blockchain）や新しい合意形成アルゴリズム Proof of Stakes (PoS), Proof of Importance (PoI), Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT) というような新しい合意形成アルゴリズムが提案されている．詳細は，多くの文献で紹介されているので，ここでは説明を省略する[12][13]．

2.3 ハッシュチェーン（Hash Chain）

Fig. 2 のようにデータを複数まとめたものをトランザクションと言うが，それらにタイムスタンプ等のヘッダー情報を足してブロックを構成する（Nonce に関しては後述）．ブロックの情報を逆変換不可能なハ

Fig. 1　Centralized network and distributed network

ッシュ関数を用いてブロック全体のサマリーを作成する．そのハッシュ値を次のブロックに入れるということを繰り返すことで，改ざんの検出を容易にする．ハッシュ値とは，文字列や文章を暗号学的に 64 文字等にまとめたもののことを言う．このような仕組みでデータを結合することで，一部のデータが変わるとそのブロックのハッシュ値が変わり，そしてそのハッシュ値を使っている次のブロックも値が変わるというようにドミノ倒しが起こるようにデータが設計されている．ブロックがそれぞれ鎖のようにつながれているために，ブロックチェーンと呼ばれる．なお，データを一ヶ所でも改ざんすると，それ以降のデータがすべて破綻をするようにデータが構成されているため，データ改ざんの検出が容易である．

ハッシュ関数として，SHA256 暗号などが用いられる．この SHA256 暗号は，①順計算は容易に行える，②逆計算は行えない（逆関数が存在しない），③入力データの量に関わらず 64 文字が出力される，④同じ文字列・データを入力すると同じハッシュ値が出力される，⑤入力データのわずかな違いが，出力されるハッシュ値に大きな影響を及ぼすという特徴を持つ．一例として，次の 2 つの文章のハッシュ値を示す．

The technology of blockchain was developed in 2008.
→ ad28748c5a6c726819fee93f8f15dc71176402f1667e22cdf6ed0863a77a7673

The technology of block chain was developed in 2008.
→ 6c5c0f332458b4ef17631bbd2d28dfc93aa3c95cb122dff046db438e7506a1ae

2 つの文章の違いは，単に「blockchain」としたか「block chain」としたかである．結果から出力されるハッシュ値が大きく異なることが分かる．なお，元々ブロックチェーンの表記は block と chain の間にスペースがあったが，現在ではスペースをなくして一つの言葉とすることが多いので，本論文では前者（blockchain）で記載を進める．

2.4 マイニング（Mining）

ブロックチェーン技術を分かりにくくしている一つが，このマイニングである．そこで，Fig. 3 に示すような例を使ってマイニングを説明する．なお説明を単純化する為に，前ブロックのハッシュ値は省略すると共に，時間の例として 1970/10/19，トランザクションの例として Data1，Data2 という単純なデータを用いる．

前節で説明を省略したが，ブロックにはナンス（Nonce）という自由に数値を入れても良い領域がある．マイニングでは，ナンスに適当な値を入れて計算されたハッシュ値が，ある閾値よりも下回った場合にデータを追加できる権利を先着 1 名が得るというルール（プロトコル）になっている．例えば，ハッシュ値の頭の数字に 0 が 4 つ続いた場合にデータ追記できる権利を得られるとしよう．Fig. 3 に示すように，ナンスを 1000 から順番に変化をさせると 1011 にするとハッシュ値の頭に 0 が 4 つ続く．それを最も早く見つけたマイナーがデータ追記の権利を得て，さらに報酬を貰えるというものがマイニングである．

実際は，0 が 4 つ続くというような単純なものではなく，20 弱程度続くような非常に困難な問題となっている為に膨大な計算リソースと膨大な電力使用が必要となっているのが現実である．この 0 をいくつにするかというものが，難易度（difficulty）と呼ばれるもので，計算時間が 10 分程度になるように調整が行われる．前述の PoS, PoI 等では，参加者の仮想通貨保有量，保有期間などに応じて難易度が変わるような仕組みにすることで，計算量を抑えるような工夫もされている．

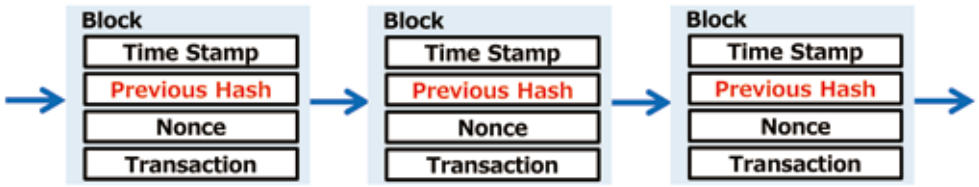
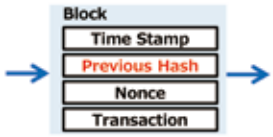


Fig. 2　Blockchain connected by Hash value



(例) Proof of Work (PoW)

```
1970/10/19 1000 Data1 Data2
      841a8f8acaf786dd5e1dedbc1038dbe0bcb50ffea7b0a25c502a4bfc5a20fa3f
1970/10/19 1001 Data1 Data2
      617c4e697b3efae803a8b1b0558bb272e6092e0dc160a16122559094f06cbd61
1970/10/19 1002 Data1 Data2
      93355aed5362d68f7bc1a78bf2ec125e36e38944f566ec05084e60ca4ade18dd
...
1970/10/19 1011 Data1 Data2
      0000036046d63480d1ef3b42f40fed5147db1b57542a237bb77a71c859d164869
```

Fig.3　Mininig mechanism using simple example

2.5 ブロックチェーンの動向

ブロックチェーンは，仮想通貨を実現するために構築された技術ではあるが，近年では Fig. 4 [14] に示すように，仮想通貨のような価値情報の移転記録から取引きや手続きの登録など，応用分野を急激に広げている．最近では，仮想通貨で用いるブロックチェーンをブロックチェーン 1.0，それ以外の用途をブロックチェーン 2.0 ／ 3.0 と区別しており，2.0 ／ 3.0 の動きも非常に活発化してきている．

車載領域に目を向けると，アメリカを中心にブロックチェーンの車載化プラットフォームの構築と標準化を目指すコンソーシアム MOBI (Mobility Open Blockchain Initiative) が 2018 年に立ち上がった [5]．MOBI では，近年普及をしているブロックチェーンを車のデータ管理に使おうという志を持って活動が行われている．Table 1 に MOBI で計画されているワーキンググループの一覧を掲載した．車両製造時情報の活用であったり，運転時の情報活用であったりするだけでなく，将来のカーシェア時代におけるサービスや税金支払いなども念頭において活動していることもあり，MOBI の活動は，車載ブロックチェーンの活用や標準化という観点からも目が離せない．なお，我々は Table 1 中の 6 番に示す Connected Mobility Data Marketplaces（CMDM）で車両データの動的管理にブロックチェーンを適用することに取り組んでいる．

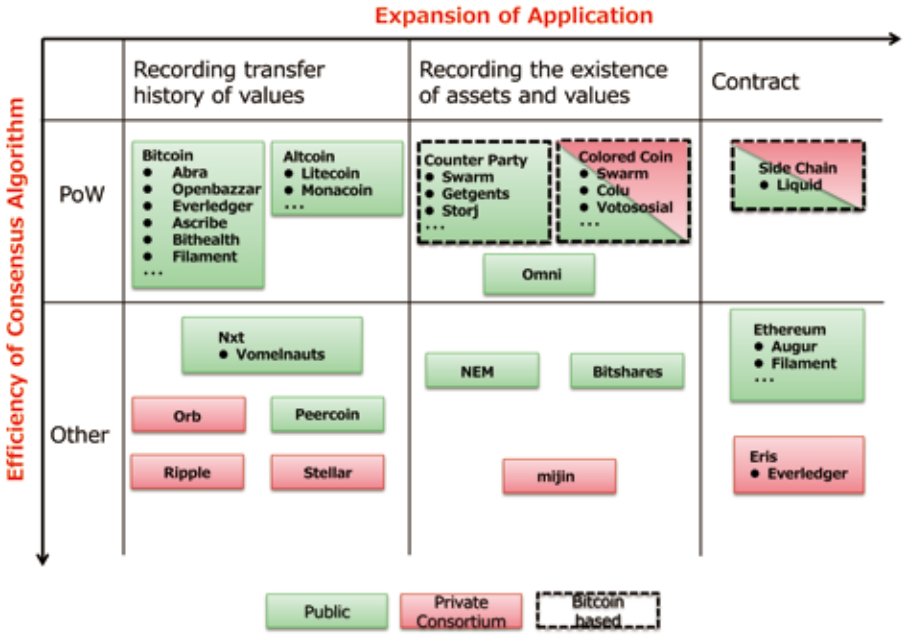


Fig. 4　Expantion of blockchain from cryptocurrency to smart contract

Table 1 Working groups in MOBI

1	Vehicle Identity and History
2	Data Tracking
3	Component Supply Chain Tracking
4	Autonomous Machine Payment
5	Mobility Commerce Platform
6	Connected Mobility Data Marketplaces
7	Car and Ride Sharing
8	Usage Based Insurance
9	Usage Based Taxes
10	Others

3. ブロックチェーンの MaaS への適用

本章では，車載に向いたブロックチェーンの提案，構築とユースケースの提案を行う．ここでは，2 つのブロックチェーン技術の紹介を行うが，まず全体の構成を Fig. 5 を用いて説明する．

車両データを用いて MaaS のようなサービスを考える際，データを守るべきタイミングが 2 つある．まず 1 点目が，車両にデータが存在するタイミングである．MaaS は，クルマがネットワークに接続されていることが前提ではあるが，クルマの走行環境を考えた場合，ネットワークが不安定となりデータ通信が安定して行えない，ドライバーが通信ユニットを意図して切るなどのケースも考えられる．また，スマートキーに代表されるような重要なデータを車内に置くことも必要な場合がある．そこで，1 点目の車両にデータが存在するタイミングでのデータ保護が重要である．3.1 節では，車両がネットワークから切り離された状態でデータをブロックチェーンにより守る技術を紹介する（以降，ローカルチェーンと呼ぶ）．もちろん，通常行われるような CAN（Car Area Network）のセキュリティ保護が併用されることが望ましいことは言うまでもない．

車載ネットワークのセキュリティとローカルチェーンの大きな違いは、前者がネットワークを後者がデータを主として守っていることである。

2 点目が，サービスを行うために車両データを車両外に出すタイミングおよび車両内に他のデータを取り込むタイミングである．MaaS のようなサービスを考える場合，一部の車両データを保険会社，シェアリング会社などの他のビジネスユニットに出すことは必須である．また，他のビジネスユニットからの情報やサービス提供指示を車両内に取り込むことも必須である．そこで，3.2 節では，他のビジネスユニットとのデータのやり取り時のデータを守る技術を紹介する（以降，企業間ブロックチェーンと呼ぶ）．なお，3.2 節の企業間ブロックチェーンでは，他ビジネスユニットとのサービス提供を考えて，通常のブロックチェーンプラットフォームを活用している．

3.1 ローカルチェーン

車両がネットワークに接続されている場合，通常のブロックチェーン技術でデータを守ることは可能であるが，前述のようにクルマがネットワークから切り離されている場合のデータ改ざん防止について考える．

本論文でテーマとしているブロックチェーンを考えると，ネットワークからクルマが切り離された段階で，分散台帳，合意形成アルゴリズムという 2 つのコンセ

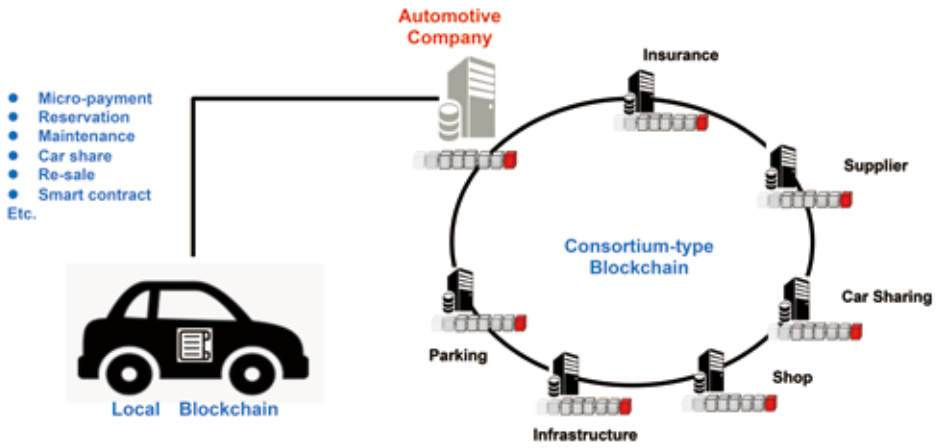


Fig. 5 Mobility blockchain and consortium-type blockchain

プトが使えないことは自明である．すなわち唯一使えるのが，ハッシュチェーンだけである．しかし，分散台帳，合意形成アルゴリズムを使わない段階でデータの耐改ざん性は大幅に落ちる．不正なデータを結合したり，一部または全部のデータを消してデータをつなぎ直したりしたとしても，外部から判断する手段がないためである．そこで，後述するような仕組みを車載モジュールに追加し，低下した耐改ざん性の向上を目指す．

近年の CPU などのアーキテクチャーの中に，セキュリティ拡張機能が付与されるようになってきた [15]．CPU の動作モードをノーマルワールド，セキュアワールドに分割して，重要なデータをセキュアワールドに退避しデータを守る仕組みである．ノーマルワールドは通常の書き込みが可能な領域，セキュアワールドは通常の書き込みが困難な領域とイメージすると分かりやすい．携帯電話の指紋認証などのデータを保護するためにも同様の仕組みが使われている．

車両データを守る仕組みとして，今回新しく追加した仕組みを Fig. 6 を使いながら説明する．なお，セキュリティの観点から概要の説明に留めるが，読者の方々に全体のイメージを掴んで頂ければ幸いである．基本的にはノーマルワールドにブロックチェーンを置き，データをハッシュ値でつなぎながらデータを守る．しかし，分散台帳，合意形成アルゴリズムが使えないことから，データを完全に書き直すことが可能である．そこで，ブロックチェーンの最終ハッシュ値をセキュアワールドに退避し守ることで，万が一，ノーマルワールドのデータが改ざんされれば即時にハッシュ値の矛盾が生じ，データ改ざんが発覚するような仕組みとしている．また，ノーマルワールドのプログラムのハッシュ値もセキュアワールドに退避することで，プログラム改ざん時にはハッシュ値の矛盾によりプログラム改ざんも即時に検出できるようにしている．

Fig. 6 の中に記載はしていないが，これ以外にも Logger と呼ばれる機能（CAN のデータをブロックチェーンに書き込む役割）や，Auditor と呼ばれる機能（ブロックチェーン内のデータを取り出す役割）も実装しており，この Auditor をベースに外部とデータのやり取りをすることとしている．

Fig. 7　Total view of local chain

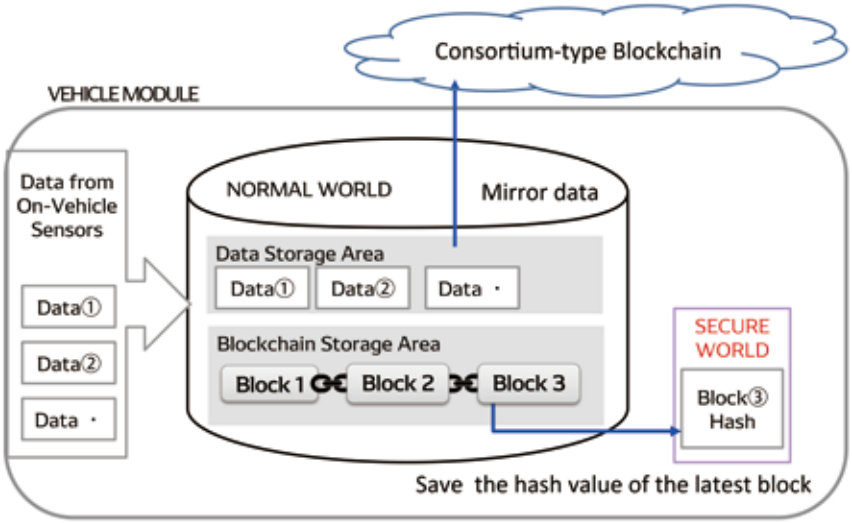


Fig. 6　Local chain using secure area

Fig. 8 Time to record and read the data in secure world (Take care of the range of the vertical axis)

Fig. 7 に実際に構築したローカルチェーンのシステムを示す．図は車載エッジコンピュータである Mobility IoT Core[16] にローカルチェーンを実装したものであるが，ルネサス社の R-Car-H3 や ASUSTek Computer 社の Tinker Board などにも実装を行っている．手前のケースがローカルチェーンを実装した Mobility IoT Core 評価キット，奥のディスプレーがローカルチェーンに保存されているデータを可視化したものである．

次に，これらのシステム（R-Car-H3 版）を使って実際にセキュアワールドでの処理時間を実測した結果を Fig. 8 に示す．ハッシュ値保存に平均 68.4 msec，ハッシュ値の取得に 6.9 msec 程度が必要であり，実際にローカルチェーンを使用する上で，処理時間による遅延はそれほど問題ないと考えられる．

3.2 企業間ブロックチェーン

車両がネットワークに接続された状態で MaaS などのサービスを安全に受けるために，車両データを他のビジネスユニットに送信する際の改ざん防止や，他のビジネスユニットからのクルマへの指示にあたるコマンドなどを受信する際の改ざん防止を実現するためにブロックチェーンを考える．

前節のローカルチェーンとは異なり，他のビジネス

Fig. 9 Total View of Consortium Blockchain

ユニットと連携する為には，特殊なブロックチェーンを使うことは出来ない．それは，ビジネスユニット毎に異なるブロックチェーンの仕組みを使うと，システムの接続やデータのやり取りの際に阻害要因となるためである．そこで，通常のブロックチェーンでスマートコントラクト等が使える Ethereum[17] を使って，サービスの実装を試みた．なお，Ethereum では Proof of Work 以外に Proof of Authority 等も使える為に，ここでは参加企業が限定されていることからも Proof of Authority を用いることにした．これは，参加企業に権限を分散した上で承認をしあうものであり，Proof of Work に比べて，ブロック追加が早い．

Fig. 9 が全体システムであり，ここでは一例とし

てカーシェアのサービス例を実装した．中央手前の箱が前節のローカルチェーンを実装した Mobility IoT Core，左の 3 台の PC が Ethereum に参加し，分散台帳を保持しているノード，右手の iPad/iPhone がカーシェア予約でエンドユーザーが使うアプリであり，奥のディスプレーに予約状況やブロックチェーンの中身を示した．

iPad/iPhone でカーシェアの予約をすると，その予約情報がブロックチェーン（Ethereum）に格納され，参加ノード間で共有される．そして，カーシェアを提供している会社から予約情報を Mobility IoT Core に送付し，予約時間になれば iPad/iPhone でクルマの鍵を開けられるようにした．実際は，Mobility IoT Core の機能を使って，CAN にドア開錠の指示を送る．その開錠情報もブロックチェーンに格納する．また使用後には，iPad/iPhone で施錠指示をすると，ブロックチェーンにデータが蓄えられ，カーシェア会社と Mobility IoT Core を経由してクルマのドアを施錠する．

これらの仕組みにより，予約情報，開錠情報，施錠情報などが改ざんできない状態でブロックチェーンに保存できる為，エンドユーザーはもちろんのこと，サービサーも安心して MaaS のようなサービスが提案できるようになった．

4. ブロックチェーンのトレーサビリティへの適用

食料品の産地偽造，賞味期限の改ざんなどの問題が世間を賑わすことが多いが，自動車領域を考えても紛争鉱物（レアメタル）の未使用証明のニーズも増えてきており，商品のトレーサビリティ基盤の重要性は増してきている．そこで，ブロックチェーンの耐データ改ざん性をトレーサビリティ基盤構築に用いることを考える．

商品・製品のトレーサビリティを考える上で，次の 4 点を解決する必要がある．①トレーサビリティ情報と商品・製品の一致（情物一致問題），②商品・製品のトレーサビリティ情報の容量制限，③トレーサビリティ情報の改ざん防止，④エンドユーザーによるトレーサビリティ確認手段の確保の課題である．

4.1 情物一致問題

①の情物一致問題に対しては DENSO が 1994 年に開発し，25 周年を迎えた QR コード（Quick Response Code）[16] の内，コピーガードが付いた SQRC（Secure Quick Response Code）を用いることとした．選定の理由は，4.4 の節で説明をする．SQRC では情報の公開・非公開情報を制御でき，サプライチェーン関係企業が各種データを入れる上で使い勝手が良く，さらにはコピーが出来ない QR コードを使うことで，正規品の QR コードをコピーして不正な製品に添付して正規品として流通できないようにした．

4.2 容量制限問題

②の容量制限の問題に関してだが，トレーサビリティに一般的に使われる QR コードや RFID タグでは，情報容量が半角文字で 6000 文字，全角文字で 3000 文字程度の為に，クルマや航空機のような部品点数が多く，サプライチェーン関係者が多い場合には全てのデータを保存することが出来ない．そこで，ブロックチェーンの最終ハッシュ値（SHA256 の場合 64 文字）とブロックチェーンサーバーのアドレス（12 文字）だけを入れることとして，容量制限の問題を解決した．

4.3 トレーサビリティ改ざん防止問題

③のトレーサビリティ情報の改ざん防止に関しては，本論文のテーマであるブロックチェーンを使ってデータを守ることとした．また，ブロックチェーンの基本的な機能である UTXO（Unspent Transaction Output）を用いることで，不正品の混入や正規品の横流しを避けるようにした．

4.4 エンドユーザーによるトレーサビリティ確認問題

④のエンドユーザーが如何にトレーサビリティを確認するかは非常に重要な問題である．専用ディバイスの購入等で追加コストが必要な場合，また確認に手間がかかる場合，「トレーサビリティは確認したいが，確認する手段が非常に複雑で手間だから確認しない」という状況が容易に想定される．そこで，エンドユーザーが追加コストなくトレーサビリティを確認でき，非常に単純な確認フローとするべく，iPad/iPhone な

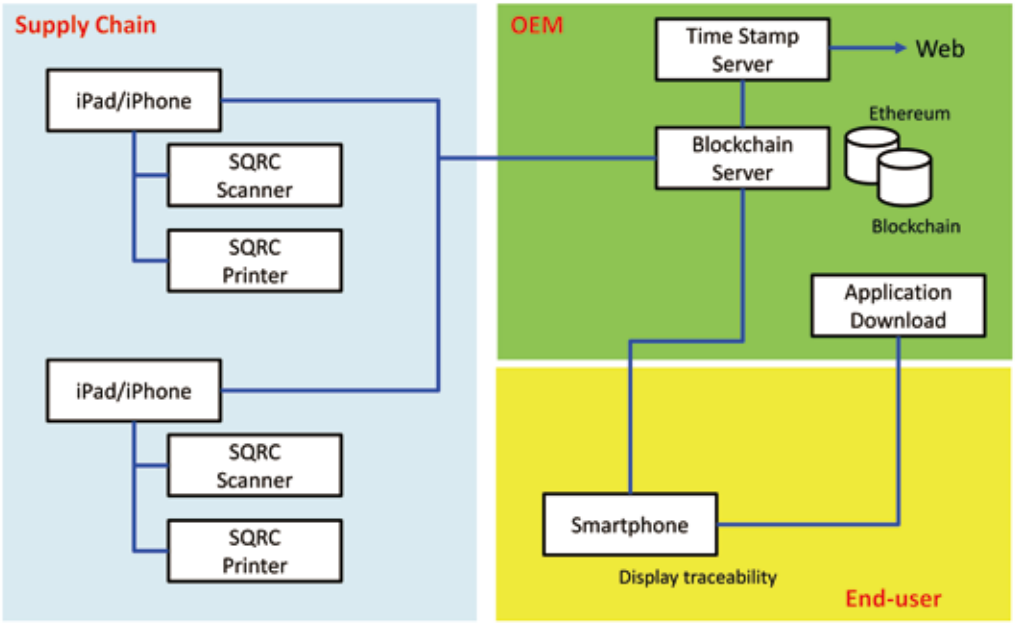


Fig. 10 System structure for traceability using blockchain and secure QR code

どによるトレーサビリティ基盤を QR コードによって実現することとした.

4.5 構築したシステム

Fig. 10 に構築したシステムのシステム構成図を示す. トレーサビリティデータを保存するブロックチェーンサーバーの中に, Web のトップニュースなどと共に時間に関するハッシュ値を作るタイムスタンプサーバーを準備する. これは, ある 1 つの企業がオンプレミスまたはクラウドでブロックチェーンサーバーを構築することも可能であり, また複数の企業でそれらを構築することも可能である. また, サプライチェーン参加者は, iPad/iPhone 等の端末に QR コードを読み込むスキャナーと QR コードを印刷するプリンターを関係者分, 準備をする. また, エンドユーザーはサーバーから専用のスマホアプリをダウンロードすることで, トレーサビリティ確認用の端末にすることが出来る.

Fig. 11 に全体システムを示す. 中央のタブレット端末, スキャナー, 左側のプリンターがサプライチェーン関係者に必要な端末群であり, 右側の iPad がエンドユーザーの iPad/iPhone アプリを示している. サプライチェーン関係者は原材料に張られた QR コードをすべてスキャナーで読み取り, 企業認証用 QR コードを読みこむことで, 関連データがブロックチェーン上に保存される. ブロックチェーンに登録されると最終ブロックのハッシュ値が計算され, それらにブロックチェーンサーバーのアドレスを加えて, コピーガード付 SQRC を 1 枚だけ発行する. これらの作業によって, 情報とコピーガード付 SQRC との完全な一致, ひいてはコピーガード付 SQRC を貼られて製品・商品とのマッチングが可能である.

上記の作業を繰り返すことで, 製品のトレーサビリティをブロックチェーン内に蓄えていく. 結果として, エンドユーザーに届く製品の QR コード内にあるブロックハッシュ値から情報を検索し, ユーザーのスマホアプリに示すことで, エンドユーザーは容易に製

Fig. 11 Total system of traceability using blockchain and secure QR code

品・商品のトレーサビリティを確認することが可能となる．

これらの仕組みにより，情報量を気にすることなく，信頼性の高い情報とモノの保証が可能となる．データに基づいた反応時間の検討など，これからの課題も多くあるが，現状のところ高い信頼性を確保できるトレーサビリティ基盤が確立したものと考えている．

5. むすび

仮想通貨の分野で発明されたブロックチェーンは，近年データが改ざん出来ないデータ管理手法として注目を浴びている．そこで本論文ではブロックチェーンの基礎的な原理の紹介をした上で，車載領域への適用事例（ローカルチェーン，企業間ブロックチェーン）とトレーサビリティへの適用事例を示した．

今後は，車載領域のブロックチェーン，トレーサビリティ領域でのブロックチェーンの Proof of Concept を行い，早急な製品化を目指すと共に，車載領域とトレーサビリティ領域のブロックチェーン技術を融合することで，製品・商品の全ライフサイクルにおけるデータ管理技術を構築し，安心かつ安全に各種サービスを行って頂ける技術基盤に深化を図る．

参考文献

1） Satoshi Nakamoto:「Bitcoin: A Peer-to-Peer Electronic Cash System」, https://bitcoin.org/bitcoin.pdf, pp.1-9（2008）
2） 岸上順一他：「ブロックチェーン技術入門」, 森北出版（2017）
3） 杉井靖典：「いちばんやさしいブロックチェーンの教本」, インプレス,（2017）
4） Martin Goesele, Philipp Sandner:「Analysis of Blockchain Technology in the Mobility Sector」, FSBC Working Paper（2018）
5） Kevin Simon:「MOBI-the Mobility Open Blockchain Initiative」（2018）
6） https://bittimes.net/news/25293.html （2018）
7） https://mspoweruser.com/renault-partners-microsoft-blockchain-based-digital-car-maintenance-book/（2018）
8） https://bittimes.net/news/6766.html（2018）
9） 石毛俊治：「ジビエの食肉利活用におけるトレーサビリティの必要性について」, テクノロジーインパクト 2030, 日経ビジネススクール（2019）
10） 伊本貴士：「ビジネスを変えるブロックチェーンの可能性」, テクノロジーインパクト 2030, 日経ビジネススクール（2019）
11） https://e-estonia.com/tag/blockchain/（2019）
12） Zibin Zheng etc.:「An Overview of Blockchain Technology: Architecture, Consensus, and Future trends」, IEEE 6th International Congress, pp. 557-564（2017）
13） Zibin Zheng etc.:「Blockchain Challenges and opportunities: A Survey」, Int. J. Web and Grid Services, Vol.14, No.4（2018）
14） 経済産業省：「平成 27 年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）(2016)
15） http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0388fj/Beigibha.html （2019）
16） https://car.watch.impress.co.jp/docs/event_repo/ces2019/1165412.html （2019）
17） https://www.ethereum.org/ （2019）
18） https://www.denso-si.jp/dictionary/dic_qr/GeneralDescriptionoftheQRCode.pdf#search=%27%E4%BA%8C%E6%AC%A1%E5%85%83%E3%82%B3%E3%83%BC%E3%83%89+ISO%27 （2019）

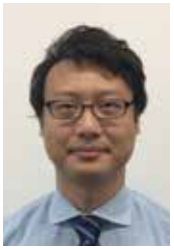
著者

岡部 達哉
おかべ たつや

MaaS 開発部ブロックチェーン開発室
Doktor Ingenieur
ブロックチェーンの研究開発業務，AI の研究開発業務に従事

三谷 陽
みたに あきら

AI 研究部モデリング研究室
AI の研究開発業務に従事



徐 昕
Xin XU

モビエレ事業グループコネクティッド開発室
車載用のコンピュータ (Mobility IoT Core) の開発業務に従事

坂本 快矢統
さかもと はやと

MaaS 開発部ブロックチェーン開発室
車載化ブロックチェーンの開発業務に従事

水摩 智
みずま さとし

MaaS 開発部ブロックチェーン開発室
車載化ブロックチェーン，トレーサビリティのシステム開発に従事

並木 陽彦
なみき はるひこ

MaaS 開発部ブロックチェーン開発室
トレーサビリティのシステム開発に従事

黄 浩倫
Haolun HUANG

MaaS 開発部ブロックチェーン開発室
ブロックチェーンの基礎研究・基盤研究に従事

田村 由佳
たむら ゆか

モビシス企画部事業開発室　博士 (工学)
ブロックチェーン事業の設計に従事