Vol.2018-SPT-31 No.17
Vol.2018-EIP-82 No.17
2018/11/2

ブロックチェーン応用の拡大と標準化における要求項目の検討

金子 格†

ブロックチェーンは Bit Coin の普及により注目を集めたが現在では暗号通貨だけでなく，非常に広範囲の様々な分野で実際の応用を目指した検討が進んでいる．今後応用分野が急速に拡大する可能性があると考えられる．ブロックチェーンの普及において標準モジュールやインタフェースの早期の標準化が普及や応用開発に資すると考えられるのでその標準化は喫緊の課題である．すでに様々な分野で標準化の動きがある．本稿では MPEG における検討状況にふれながらブロックチェーンを利用したシステムにおける標準的な符号化表現が満たすべき要求仕様を検討する．.

On the evolution of the application of block-chain and consideration of the requirements for the standardization

Application area of block chain is rapidly expanding. With such rapid expansion, appropriate standardization may contribute the standardization of the component and easier expansion of the use of such technologies. We will discuss on the requirements for the standardization of common representation which can be used in the system which uses block-chain..

ITARU KANEKO†

1. ブロックチェーンの標準化検討の目的

ビットコインの普及によりブロックチェーン技術が広く知られるようになった．現在ではビットコイン以外の暗号通貨が多種流通している．しかしブロックチェーンの応用は暗号通貨だけではないと考える専門家は多く，現在非常に広範囲の様々な分野で実際の応用を目指した検討が進んでいる[1] ．

応用分野が拡大した場合，ブロックチェーンの要素技術をそれぞれ別個に開発するのではなく，ある程度ライブラリ化して供給元を絞る方が高品質のモジュールが作れるだろう．また複数ソリューションについて常に互換性のある代替品が多数用意されていることは，セキュリティ上も重要であろう．

ブロックチェーンの普及は，まさに始まったところであるが，標準化は可能であれば早期に行った方が効果的である．モジュールやインタフェースの早期の標準化は普及や応用開発に資する．標準化が遅れれば効果は限定される．標準化作業には多くの時間がかかり，最低でも 5 年程度を要する．本年(2018 年)本放送が始まる次世代デジタル放送に使用された MMT の標準化が開始されたのは 2010 年であり標準化作業の開始から実用化には 8 年を要している[2] ．今後ブロックチェーンの応用が各分野で急速に進むとすれば標準化は喫緊の課題である．

ブロックチェーン関連ですでに様々な分野で標準化の動きがある．本稿では MPEG における検討状況を中心にブロックチェーンを利用したシステムに有用な標準化とその動向について検討する. MPEG 以外に多くの標準化や事業化の動向があることは言うまでもない. 本稿は MPEG における標準化を題材とするが, MPEG における検討過程は他の分野におけるブロックチェーン関連の標準化にも活用可能であると期待している．

2. MPEG 標準化と国際標準の効用

2.1. MPEG 標準化

まず MPEG における標準化について簡単にまとめる．MPEG は ISO/IEC 傘下の WG(作業グループ)である． これまでに MPEG-1 (ISO/IEC 11172-x)シリーズ, MPEG-2(ISO/IEC 13818-x)シリーズ, MPEG-4(ISO/IEC 14496-x)シリーズ, H.263/AVC, ISO/IEC 13818-7/AAC, ISOBMFF, MPEG/DASH, MPEG/MMT, H.264/HEVC など

† 東京工芸大学
Tokyo Polytechnic University

Vol.2018-SPT-31 No.17
Vol.2018-EIP-82 No.17
2018/11/2

の国際標準を策定した．会合参加者は 300 人前後で増減しており 1988/5/10-12 の第一回会合から今日まで平均年 4 回の会合で各国の委員が集まり標準化作業を進めてきた．現在は HEVC の次のビデオ符号化，3D オーディオの符号化を始め point cloud，ネットワーク分散符号化，ニューラルネットワークの圧縮，遺伝子データの符号化など新たな分野の標準化も積極的に取り組んでいる．

2.2. 標準化のメリット

一般的に，標準化といえば「一つの仕様に統一すること」と理解されることが多い．国際標準化も，直接的に一つの仕様に統合することをイメージされことが多い．実際には国際標準化が直接一つの仕様を規定してその仕様の採用が強制されることはほとんどない．むろん仕様の統一は最終的には国際標準化がもたらす重要な恩恵である．しかしそれは仕様統一の周辺環境が国際標準化によって整えられることにより間接的に実現される．直接的に仕様の統一がなされるのではないので，それではいかにして間接的に仕様統一が促進されるのか，という点の理解は重要だ．

まず標準規格の採否は利用者の自由であり，いかなる製品や法制度においても特定の国際標準や仕様を強制する効果はない．いかなる仕様も国際標準の採用も不採用も任意である．

国際標準はそこで記述された技術的内容における用語やパラメータ，そして互換性の定義を統一するだけである．

たとえば MPEG-2 規格の採用はいかなる意味でも強制はされていない．実際初期においては MPEG-2 規格に基づかない放送システムやマルチメディア製品は多数存在した．また解像度においても SD(標準解像度)や HD(高解像度)を含む様々な解像度，フレームレートが規格に含まれる．また HD 解像度のデータをデコードした結果を物理的にどの解像度で表示するかも MPEG 規格の中では規定していない．したがって HD(1440x720)やフル HD(1920x1080)，そして 4K の表示は自由に選択できる．

一方，国際標準が作られることで仕様の統一が促進されることは疑いない．それには以下の 3 つの要因が寄与していると考えられる．

第一に，特許の共有あるいは無償化が促進されることである．国際標準の仮定で必須特許の FRAND(fair, reasonable and no discriminative) の宣言が要求される．したがって国際標準に含まれる技術は，だれもが非差別的に利用できるようになると期待される．ただしロイヤルティが不要になるとはかぎらないことに注意が必要である．さらに，国際標準化期間は必須特許の FRAND 宣言が得られない場合は国際標準化のプロセスを中断するルールであるとはいえ，これはその特許が知りえるところとなった場合のことであり，いわゆるサブマリン特許が後から見つかる可能性を完全に排除することはできない．国際標準を使った場合の特許紛争の可能性は完全にゼロにすることはできないが，その分野の主要な企業のほとんどが参加している標準であれば，他の私的なコンソーシアムにくらべれば特許紛争の可能性は低いと期待できる[3]．

ライセンス料を不要にすべきだ，という意見は多いが現実的には困難が伴う．ライセンス料不要の規格を作ろうとすると(国際標準であるかそうでないかにかかわらず), パテントトロールやサブマリン特許で特許実施者から莫大な実施権料をとろうとする動機を持たれやすい．これについては様々な工夫により努力が続けられているところである[4]．

第 2 が立法や調達により仕様を統一することが可能になることである．国際標準であれば通信放送関連法規や国の入札により特定規格を指定することが可能となる．一方，国際標準でない規格を指定することはできない． WTO TBT Agreement （貿易の技術的障害に関する協定)に違反するからである[5] [6]．日本ではデジタル放送の音声に AAC を指定したが，こうした場合に国際標準であることが採用の条件となる．

第三は代表的な仕様を絞り込んで共有することにより共通の仕様で合意しやすくなるという効果である．DVD において MPEG-2 メインプロファイルが採用されたのがその一例である[7]．

2.3. MPEG 標準における標準化プロセス

多くの標準化組織が同様のプロセスを持っているが MPEG(およびその上位組織である ISO/IEC JTC1)の標準化プロセスはおおむね以下のようになっている[8]．

(1) 調査段階 どのような標準化を進めるべきかを調査する
(2) New Project 提案段階 標準化プロジェクトを提案する
(3) Committee Draft 委員会原案
(4) Draft International Standard 国際標準原案
(5) Final DIS 最終国際標準原案

各段階で担当するグループ内での投票があり最終的には全加盟国の投票を得て 2/3 以上の賛成があれば国際標準として成立する．

Vol.2018-SPT-31 No.17
Vol.2018-EIP-82 No.17
2018/11/2

3. MPEG における Block chain の検討

3.1. Long term workplan の検討

2018 年現在 MPEG では long term work plan の検討を行っている．次の標準化テーマを検討するため，何回かにわたって次に取り組むべき標準化テーマの抽出を行っている．特にオーディオ・ビジュアル以外のメディア符号化についての検討に焦点をあてて様々な分野の中で符号化の需要がないかを検討している．その中で block chain も検討項目としてとりあげられている．

3.2. 第 124 回 MPEG meeting

第 124 回 MPEG 会合は 10 月 6 日(土)～12 日(金)までマカオで開催された．現在 Video, Audio, PCC, 3DoF(VR 的に視聴できるコンテンツの符号化)，遺伝子符号化，ビジュアル検索，ネットワークベース符号化，ニューラルネットワークの圧縮などの標準化作業が進んだ．

その中で先にのべた long term work plan の検討も今回の議題としてとりあげられ検討が行われた．

MPEG では会合間に実際の標準化作業を指定されたメンバーが分担して実施する．長期プランは前回会合で 10 名程度の専門家に各分野が割り当てられそれぞれのサーベイを行うことになっていた．

4. M44017 における block chain

4.1. 作業の経緯

前回(2018 年 7 月)の MPEG 会合において前述の長期プランは筆者を含む 10 名程度の各分野のエキスパートによって策定されることになった．その結果は入力文書 m44017 にまとめられた．

m44017 Analysis of promising non-media data compression areas Ad hoc group on MPEG long term work plan

筆者はこのうち blockchain に関する検討項目を担当した．

入力文書は各参加者が成果を報告するための文書であり出力文書は会合の結果をまとめ合意事項や外部に告知する内容を確認するために発行する．

今回の結果は執筆時点では番号，タイトルとも未定であるが本研究報告の発表時点では発行しているはずである．出力文書の一部は委員会内限定であるが，long term work plan はおそらく公開文書になると予想される．

入力文書は非公開であるが，文書の中で筆者が投入した部分公開しても問題がないと考えられるので以下に概要を示す．

4.2. Block chain の定義

ブロックチェーンは電子署名と暗号を用いた文書の真正性証明システムのひとつである．従来手法では単一の信頼源を元として電子署名などで証明を引き継ぐ場合が多かった．ブロックチェーンでは署名を行ったデータを引継ぐと同時に競争的な検証を導入することで，記録の真正性を単一の信頼源を必要とせずに行う．したがってブロックチェーンは「分散型台帳」と呼ばれている．

4.3. 利用目的

一般的にはブロックチェーンは真正性を署名などで確認できる台帳の共有に利用する．またその真正性の証明につかうシステムを分散的で適用的で進化可能とするために利用される．

4.4. 現在の応用分野

参考資料[1] によれば現在以下の応用が検討されている．

(1) 国際銀行間取引
(2) 食品流通の安全情報の証明
(3) デジタルトークンやデジタルキーの配布(宅配ボックスなど)
(4) 不動産情報の交換
(5) 電力市場
(6) ソーシャルゲーム
(7) ソーシャルメディア
(8) クラウドストレージ
(9) シェアリングエコノミー

4.5. 技術課題

同じく参考資料[2] によれば現在以下の技術課題が検討されている．

(1) PoW 改良，代替手段の開発
現状で多大なリソースを消費しトランザクションに時間がかかる原因となっている．

(2) チェーンの構造
以下の 3 通りがある．(a)パブリック型 (b) 併用型 (c) コンソーシアム型

(3) データ容量
現状のシステムはチェーンを追加するのみで削除しないので，容量の問題が生じることがある．

加えて筆者は以下の課題があると考える．

(4) AI, IoT との融合
AI, IoT においては多数のセンサーや処理システムを「人間の関与なく」運用する技術への需要が高まると予想される．

4.6. 提言

MPEG は高能率のデータ保存伝送についての専門技術を有している．この専門性を blockchain の様々な分野で活用するためには blockchain 技

術の動向を把握することが有益である．ビデオ配信への block chain の応用は特に MPEG の標準化分野と関連性が高い．MPEG は blockchain 技術自体の標準化は行わないとしても，blockchain 技術の動向を把握することはメディア符号化の有用な標準を作るためには必須である．

5. 検討経緯と動向

今回このレポートにまとめられた結果が会合中に審議され，出力文書としてまとめられる予定である．今回議論の具体的な経緯と結果は執筆時点で未発表であるが，MPEG 標準化の中で blockchain を「利用する」ための標準の検討は積極的に続くと筆者は考えている．

上記の提言に加え，メディア符号化における block chain の応用についてのいくつかの提案が示され，今後の検討項目に加えられた．

今後は blockchain 技術の詳しい調査, 他標準の動向の把握とともに, MPEG 標準の中でどうこの技術が利用できるかという点の検討が進む見込みである．

むろん会議中の議論は現時点ではあくまで議論の経緯であり今後先にのべた NP として提案されてはじめて具体的な技術的分野についての正式な標準化のプロジェクトが開始することになる．本稿は現時点でいかなる動向や分野が確定したことを示唆するものではない．

6. AI 分野での応用

ここでは筆者が AI 分野においてブロックチェーンの活用が可能ではないかと考える応用分野の一つとして AI の創作物の知的財産権の管理における利用について説明する．これらは既発表であり，ここでは block chain の応用の一つとして述べるが，現時点で標準化の提案を行っているわけではなく応用分野の一例として示す．

AI 技術を利用したコンテンツ制作加工が実用化されようとしている. AI 技術を利用したコンテンツは多数の「学習データ」をベースにそれらと同一ではないがほぼ同様の目的に適した大量のコンテンツを生成することに利用することができる. 詳細の議論は著者による参考文献[10] に詳しいが，いわば著作権法の「表現」に相当する部分が一部自動化されることにより自動的に大量の「新しい」著作物を生成することができるのである．これが学習に利用したオリジナルと競合することが懸念される．

例として AI によるマンガの少女キャラの生成をあげる[9] ．この分野の進歩は激しく，もはや類似著作物の生成は非常に簡単に安価に大量に行える時代が到来しようとしている．

このような時代に著作権法の枠組みの今後についておおまかに二つのアプローチが考えられる．

一つは既存の著作権法の考え方に基づき「表現」が異なる著作物には元の作品の著作権は及ばないとする立場を継承することである．この場合オリジナルのコンテンツは AI によって生成された大量の類似コンテンツと競合するだろう．そしてコンテンツ自体からの対価の回収は困難になるだろう．

これに対抗するためには多くの作者は作品を公開をせず, AI に対する教師データを秘密保持契約によって提供する，というアプローチを取ることになるかもしれない．これはいわば知的財産権が確立したコンテンツ流通経済の崩壊を容認することを意味する．

一方筆者は「機械学習」の成果への学習データの寄与を積極的に評価することで，オリジナルの作品への対価の還流を図る仕組みを提案している[10] ．このような還流を可能にするには知的財産権関連法規の改訂が必要になるだろう．これは時間もかかり非常に困難であるが，うまく機能すれば印刷と同様に知的創造の利用に新たな価値拡大の機能が加わり，クリエイター，利用者，AI 技術の開発者の win win の関係が構築できると考えられる．

このような枠組みにおいては創作された価値の「伝搬」の追跡やその価値の「評価」が重要な技術的要素となる．その際に上記考察は筆者は，創作の価値は数量的な情報量では評価できず何等かの「市場の評価」を含めた人間による価値評価と調停が必要となるかもしれない，という点を論じた．

したがってコンテンツの流通に際してなんらかの評価を付与していく仕組みを何等かの方法で構築することが有益であると考えられる．そこにはこの block chain が利用できると考えられる．同様にコンテンツの価値の「連鎖」において block chain を活用できるのではないか，と考える関係者も多い．

ところで，おりしも漫画村に関する一連の問題が注目をあびた．この問題の場合，明白な著作権侵害であるが，コンテンツの流通による価値の「横取り」を行っている点では同様の問題を含んでいる． AI による創作物によってオリジナルの創作物の価値がスキミングされることを効果的に抑制する仕組みが構築できれば，それは当然，明白な著作権侵害である漫画村のような行為に対する有効な抑止手段としても利用できると考えられる．

Vol.2018-SPT-31 No.17
Vol.2018-EIP-82 No.17
2018/11/2

7. IoT 分野での応用

ここではメディア IoT 分野への block chain の利用について検討する．これらは既発表で block chain の応用の一つとてここで述べるが，標準化の提案を行っているわけではない．

Internet of Things (以下 IoT)の拡大が期待されている．IoT の応用および構成要素は様々であるが, ここではメディア IoT と呼ぶ分野に着目する．

メディア IoT は MPEG 作業グループ(ISO/IEC JTC 1/SC 29/WG 11)の中でこれまでいくつかの国際標準案が策定された[11]．筆者はこの MThing に要求されるセキュリティ機能を軽量に実装する手法について提案した[12]．

この提案は，確率的多面的安全性モデル(以下 PMLSM)とブロックチェーンという二つの手法を導入することでメディア IoT の柔軟で軽量なセキュリティフレームワークを実現しようとするものである．

図 1 において MThing #1 から#6 は Hardware H1～H3, OS O1～O2 そしてソフトウエアコンポーネント S1～S6 から構成されている. 各 MThing は様々な Hardware を採用でき，Hardware の仕様に応じて様々は OS やソフトウエアコンポーネントを登載可能とする．

図の左半分は Verifier と認証を示す．Verifier V1～V3 は Hardware, OS そしてソフトウエアコンポーネントを評価し認証する.「Authentication」と書かれた部分の矢印は認証がなされたことを表している．すなわち矢印で結ばれた対象を各認証期間が検査し，基準を満たしたとして認証していることを示す．

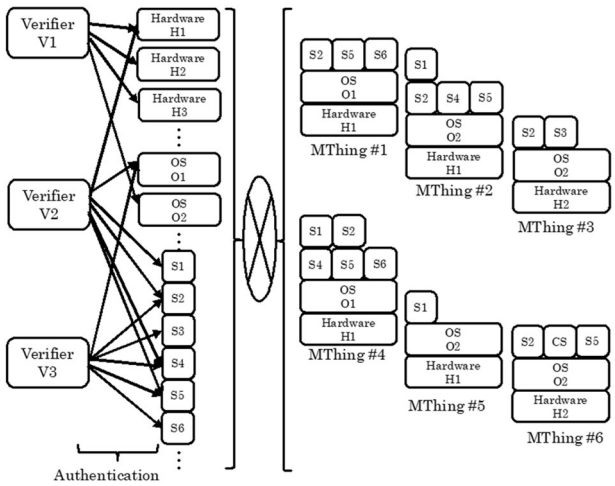

図 1 メディア IoT 向けセキュリティフレームワークの構成

Verifier V1～V3 は Hardware, OS そしてソフトウエアコンポーネントを評価し認証する．「Authentication」と書かれた部分の矢印は認証がなされたことを表している．すなわち矢印で結ばれた対象を各認証期間が検査し，基準を満たしたとして認証していることを示す．

本手法ではこれら認証の結果を block chain で署名された台帳として共有することを想定している．分散管理された台帳を用いているので各 Verifier は，他の Verifier の評価を参照することができる．その結果分散管理された環境の中で Verifier 同士の相互監視，相互評価が可能になる．

システム中の各モジュールは複数の Verifier の評価を受けることになるので，一つの Verifier の評価に依存するよるよりも多重化による安全性が確保される．Verifier 同士も相互評価が可能だから一つの Verifier によるよりも安全性が高まると期待できる．

どのようなセキュリティを求めるかは応用分野毎に様々であるが応用分野毎のニーズに柔軟に応じることが可能である．

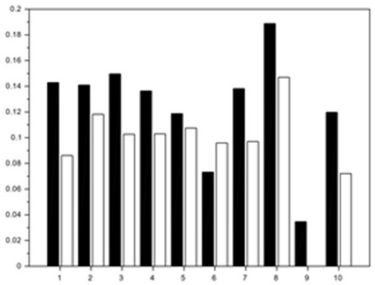

図 2 Verifier 相互評価の結果

Verifier の相互評価が可能かを簡単なシミュレーションで確認した結果を図 2 にしめす．ここでは verifier1～3 がそれぞれ固有の誤差を持つ場合に相互評価によって信頼性が確認できるかをシミュレーションによって確認した結果が示されている．図に示す黒が実際のモジュールの信頼度であり，白が推定値を現す．相互評価により実際の値に近い傾向を持つ推定値が得られている．

8. まとめ

本稿では block chain の利用拡大にむけ標準化を開始すべきタイミングにあることを述べ block chain の標準化に関する検討をまとめた．まず国際標準化，および筆者が主に参加をしている MPEG 標準化における動向を述べた．次に block chain の応用分野と技術課題をまとめた．次にメディア符号化分野における block chain の利用について第一の例として AI による創作の知的財産の対応に関して，次にメディア IoT 分野におけるセキュリティ確保への応用について検討を加えた．

Block chain の応用分野はきわめて多様で幅広く本稿はそのごく一部について検討しているにすぎないが，国際標準化の必要性がありそのメリットもあると考えられる．他分野における標準化動向とそれらとの関係については今回言及しなかったがすでに様々な活動が開始されている．今後引き続き block chain 技術の動向の把握，各応用分野での標準化動向の調査を行いつつ，MPEG においても適切な標準化が進むよう，意見投入を行っていく予定である．,

[参考文献]

[1] ブロックチェーンビジネス研究会，“60 分でわかる！ ブロックチェーン最前線”，技術評論社(2018)
[2] 青木秀一，“新たなメディアトランスポート方式の国際標準化”，NHK 技研 R&D/No.150/2015.3,(2015)
[3] 金子格，加藤木 正紀，”IT・ソフトウェア特許の新潮流 ～活用・防御から標準化まで～：6. IT・ソフトウェアの標準化と特許 -インターネットが変えた標準と特許の関係-“，情報処理,54(3),228-231 (2013)
[4] Leonardo Chiariglione，“IT・ソフトウェア特許の新潮流 ～活用・防御から標準化まで～：コラム．特許と MPEG の 25 年 -特許はどのように MPEG を助け，また妨げたか”，情報処理,54(3),228-231 (2013-02-15) -
[5] WTO, “Technical Barrier to Trade Agreement,” https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm
[6] 経済産業省，貿易の技術的障害に関する協定，http://www.meti.go.jp/policy/trade_policy/wto_agreements/marrakech/html/wto06.html
[7] 菅谷寿鴻，“DVD の国際標準化と標準化雑感,” 映像情報メディア学会誌 Vol. 64, No. 7, pp. 980～982（2010）
[8] 日本規格協会，“国際規格の作り方”，https://www.jsa.or.jp/datas/media/10000/md_2423.pdf,(2008)
[9] マンガ大好き読者さん,“【画像】AI の自動生成イラストが劇的に進化！！人間に匹敵する画力を手に入れた模様ｗｗｗｗｗｗ”，http://chomanga.org/archives/74711.html(2018)
[10] 金子格，“人工知能による著作物の創作性尺度に関するアルゴリズム情報理論から見た考察”，研究報告電子化知的財産・社会基盤（EIP）,2017-EIP-75(6),1-6 (2017-02-10)，2188-8647(2017)
[11] MPEG, IoMT Architecture, https://mpeg.chiariglione.org/standards/mpeg-iomt/iomt-architecture (2017)
[12] 金子格，確率的多面的セキュリティモデルとブロックチェーンを用いたメディア IoT 向け軽量セキュリティフレームワーク，電気学会論文誌Ｅ（センサ・マイクロマシン部門誌） 137(6), 796-801, 2017(2017)