暗号資産（ビットコイン）・ブロックチェーンの高信頼化へ向けての MELT-UP 活動

山澤 昌夫[3] 角田 篤泰[2] 藤田 亮[2] 近藤 健[1] 才所 敏明[3] 五太子 政史[3] 佐藤 直[2] 山本 博資[2]
辻井 重男[3] 野田 啓一[4]

概要：暗号資産の仕組みにおいて，ユーザが作成する秘密鍵が価値操作の基礎である．市場での暗号資産流通におけるインシデントの要因は，暗号資産仕組み上に秘密鍵保護の機能が入っていないという構造が起因している．さらに，暗号資産の安全性強固さを支える構造は，公開鍵暗号方式とハッシュ演算のチェイニングだが，構造部品が危殆化したときの安全性保全については検討されていない．
筆者等は，SCIS2018 において，秘密鍵の管理に物理プロセスを導入する事を特長とするセキュリティ実現方式を提案し，CSS2018 において取引所等への展開を検討した．さらに，SCIS2019 においては，部品危殆化時の構造問題に関する課題についての検討が必要であることを論じた．構造的問題を内包する価値操作系を総合的に機能するように構成するには，MELT (Management, Ethics, Law, Technology) がからむ自由と規制の相克を止揚（MELT-UP）するなかで，適用領域を広げた解を導くべく検討する必要がある．本論文では，課題検討の方向付けに対応し，秘密鍵保護機能と本人認証機能との関連を論ずる．

MELT-UP Activities To Enhance Security Of Crypto Assets and Blockchain

MASAO YAMASAWA[3] TOKUYASU KAKUTA[2] RYO FUJITA[2] TAKESHI KONDO[1]
TOSHIAKI SAISHO[3] MASAHITO GOTAISHI[3] NAOSHI SATO[2] HIROSUKE YAMAMOTO[2]
SHIGEO TSUJII[3] KEIICHI NODA[4]

1. はじめに（分散台帳システムにおける暗号資産のリスク）

暗号資産の仕組みにおいて，ユーザが作成する秘密鍵, 公開鍵ペアが価値操作の基礎である．これまで多数報告されている市場での暗号資産流通におけるインシデント [13], [15] の要因は，暗号資産仕組み上に秘密鍵保護の機能が入っていないという構造に起因している．このことも含んで，松尾らは [11] において以下の 4 課題を指摘した．

(1) 暗号技術としての安全性と，システム全体での安全性の検証が十分になされていない．すなわち，「脆弱性ハンドリング」がやはり必要という課題.
(2) 暗号技術を利用したシステムにおける運用が十分に検討されていないという課題．これこそがインシデントの主因でもある.
(3) スケーラビリティと非中央集権性のトレードオフという課題.
(4) ブロックチェーンの構造である分散したデータの更新に関する安全性という課題.

我々は，特に（2）に注目している．この課題については，佐藤が [10] で指摘しているように，鍵管理の問題とならんで，公開鍵ペアの更新の問題も根が深いと考えている．以下の章においては，この二つの問題について述べる

2. 鍵管理における秘密鍵保護機能と本人認証機能

SCIS2019 で述べたような秘密鍵の安全性保持機能 [6] は，まだ実装や運用が不十分な状況であり，そのための大きな暗号資産流出インシデントが起こっているのが実情で

1 セキュア IoT プラットフォーム協議会
2 中央大学研究開発機構
3 中央大学研究開発機構・セキュア IoT プラットフォーム協議会
4 慶應義塾大学 SFC 研究所

ある．

暗号資産を形成する「秘密鍵」ビット列は，ランダムな数であれば本来どんな値でもよい．しかし，そのままでは暗号学的な保護も運用上の保護もかからない．これまでの暗号資産簒奪さわぎは，種々の恣意的なサイバー攻撃だったと国連安保理のレポートにある．サイバー攻撃で奪取できてしまったということは，所有権を特定する秘密鍵がコピーされ使用されたということになる．

秘密鍵を分散化して管理することで，リスク低減を図る方法が種々考案されている．SCIS2018 で述べた方式は**図 1** に示すように，秘密鍵の秘密分散片を端末（スマートフォン等）と複数の USB メモリモジュールに格納し，盗難リスクを軽減するとともに紛失リスクにも対処できる．

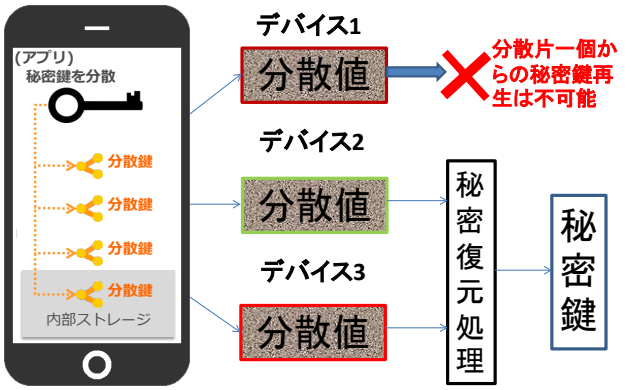

図 1　SCIS2018 で述べた方式 [7]．生成した分散値はデバイスに配布後一個を内部ストレージに残す．秘密鍵と残りの分散値は消去する．送金時はデバイス側の分散値と内部分散値から秘密鍵を再生する．

この方法では，分散値から元情報を復元して必要な署名データを作成する．このとき一時的に秘密鍵が陽に現れ，脆弱とされる．

この脆弱点に関しては，文献 [5] において，しきい値署名を使う方法が言及されている．しきい値署名とは，しきい値以上の個数の署名データにより検証可能となるデジタル署名である．すなわち，一つの署名鍵に対して，複数人によって承認し，複数人により管理するという方式となっており，しきい値未満の個数の署名データから正当な署名を生成することができないため，不正なユーザによる署名が生成されるのを防止することが可能なデジタル署名方式となっている．

これまでに提案されているしきい値署名としては，RSA 署名 [16] に対するしきい値署名 [17],[18],[19]，DSA/ECDSA 署名 DSS [20] に対するしきい値署名 [21],[22],[4],[23],[24]，ペアリングに基づいた署名 [25] に対するしきい値署名 [26] などがある．

これによると，ビット列を暗号傘の中に置いたままで必要な署名を生成することができる．

しかし，ここにも暗号方式と実装がからむ課題がある．この課題については，SCIS2014 にて問題提起がなされており，DSA 署名における秘密鍵の漏洩に関する問題が ECDSA 署名においても起こり得ることが指摘され，特に，Bitcoin において実装上の問題があった場合，現金詐取されることが示されている [3]．

したがい，現実には分散片の管理は秘密分散を用いた場合と同じく，運用で守ることが必要である（**図 2**）．

図 2　分散値からの秘密鍵再生においては，分散値を格納するデバイスにより分散値取り込み方法が変わる．

これに抗する暗号学的手法として，筆者等は，「由来の確たる証拠（たとえば SCIS2018 で筆者等が実装した秘密分散片の所有とか，否認できない情報の所有など）を有する秘密鍵」という考え方をとりいれた運用方式を検討している．

対抗する脅威は，秘密鍵の漏洩，盗難，紛失および誤操作，錯誤等による毀損だが，これまで述べた秘密鍵を暗号傘下化する，冗長化する，手順を直感的にする等では不十分と考えられる．

図 3 に示すように，秘密鍵を本人認証と結びつけた形で，安全性保持を行う機構が必要と考える．この機構の実現技術の候補として，任意のデジタル情報と秘密鍵とのリンクを証明する機構である．筆者らは基本とするデジタル情報として DNA の STR（Short Tundem Repeat）情報 [27], [28] が有力な候補と考えている．

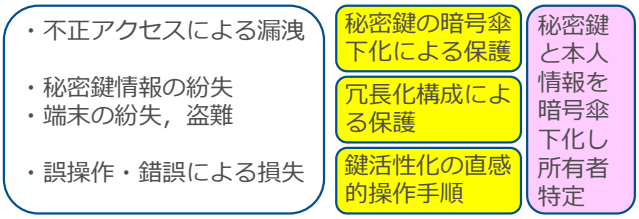

図 3　秘密鍵の保護機構として，暗号による保護を切らせないこと，秘密分散した分散値を冗長情報格納手段として運用すること，旧来からの直感が効くような操作方法とすることなどが有効と考える．それらに加えて所有者である査証情報を秘密鍵と暗号学的にリンクさせることが必要と考える．

3. 鍵管理における公開鍵ペア更新の問題

ビットコインシステムでは，通貨所有を確定させるために，公開鍵暗号方式を用いる．

通常，PKI での鍵ペアは安全性のため一定時限で無効化し，あらたな鍵ペアに置き換えるという運用を行っている．

しかし，ビットコインシステムでは，通貨を一旦作ると，それに関わる鍵ペアを永劫に（通貨を使う，すなわち，消費するまで）使い続けるという構造になっている（**図 4**）．同図は，個人間の資産のやりとりを時系列的に表現したものである．たとえば，慈子，五郎をとってみると，彼らはこの図の時間帯中，T_1 から T_8 まで最初から持っていた 10 円を使って居ない．こういう状態が続くと鍵ペアは更新されない．一方，T_7 における花子はそれまで保有していた 45 円を消費し，そのうちの 15 円を慈子に渡した．この時点で，花子は新しい鍵ペアを使い始めたことになる．

[10] では，安全性とか危殆化とか通常の暗号が対処しなければならない運用的操作について，課題があると指摘されている．ビットコインシステムでは**図 4** の慈子，五郎の状態が長期に続く場合 PKI 的な運用から外れて行くのだが，これを適切に取り扱うことは指摘のとおり難しいと考えられる．

その構造を変えて，通貨を作ったならば作った時点からタイマーが発火し，時限がきたならば，所有者にアラートを上げ（注 A），違う鍵ペアに置き換えるよう促す構造とする．それによって，PKI で行っているような安全性保持が可能となろう．（注 A：アラートの代わりに，時限が来ると「無効」と決めてもよい．無効になる前に，自分宛の同額の送金をすれば，所持する通貨は失わないで済む．全員がそういう処理をすれば，PKI のような管理が実質できたことになる．）

危殆化についても，一定時限で無効化する構造であれば，暗号方式を一斉に変えるという操作が可能なので，対処が可能と考えられる．

こういう構造とするとき，所有者と秘密鍵とのリンクの仕組みがあると，アラート先が特定できるので，実装が可能になる．ブロック構成要素としての公開鍵ペアは，全体的にはブロックチェーン構造によりブロックの連鎖に組み込まれた形態になっている．全体的に見るとブロック構成の暗号学的強度はブロック高に対して指数関数的に増大するとされている [1] ので，PKI の様な運用も危殆化対応も必要がないとする考え方もあるが，筆者等はこれも将来あきらかにされるべきと考えている．

前述の**図 4** で明らかであるが，資産移転時には古い「公開鍵・秘密鍵ペア」を廃してあらたな鍵ペアを作る．資産移転時には，価値は別の「公開鍵・秘密鍵ペア」に引き継がれる．引き継ぎに伴って，秘密鍵を扱うので，２章で取り上げた鍵管理に関する課題が再現すると考えられる．ここでは，前章では論じなかった永続性に焦点を当てる．

暗号資産の移転（出金）は，使用できる資産に入金を示す UTXO（Unused Transaction）のアドレスに対応する秘密鍵による署名を付すことで可能になる．UTXO の価値は，移転先へのトランザクションに置き換えられる．すなわち，『価値は別の「公開鍵・秘密鍵ペア」に引き継がれる』のである．ここで，署名の安全性すなわち，公開鍵・秘密鍵ペアの安全性が確保されなければならない期間は，恐らく「ある人への入金トランザクションがあってから出金されるまで」ということになるであろう．これは仮想通貨でなくウォレットの問題かも知れないが，仮に年金をビットコインで受け取っていた人が亡くなってその UTXO が貯まった状態にあるとき，それを知った者が時間をかけて署名を偽造し，ビットコインを自分宛に出金させてしまうことがあり得る．こう考えると，場合によっては 10 年位は偽造されないようにする必要があるとも考えられる [12]．

このようなセキュリティを考え，署名 (またはハッシュ) の安全性を考察するために，安全性を高める，または要求される安全度を定めることを検討しなければならない．また，睡眠口座や遺言書無しで亡くなった人の遺産処理のためにこの UTXO を鍵無しで処理するための仕組みも必要になるであろう．これも今後継続的に検討すべき課題と我々は考えている．

4. まとめ

ブロックチェーンの課題の一部について検討し，安全性向上が見込めることを示した．今後は具体例について，さらに実装検討を行いたい．

謝辞　本検討の対象となった実装例につき，情報を御開示頂いたことを深謝する．また，本研究開発は総務省 SCOPE(受付番号 181603006) の委託を受けたものである．

参考文献

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf

[2] https://github.com/bitcoinbook/bitcoinbook

[3] 須賀祐治，“Bitcoin の ECDSA 署名生成時にポカしたら現金詐取される，” *Proc. SCIS2014*, 4A1-3. Jan. 2014.

[4] Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan, “Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security,” Cryptology ePrint Archive, Report 2016/013, 2016, https://eprint.iacr.org/2016/013

[5] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[6] 山澤昌夫, 角田篤泰, 藤田亮, 近藤健, 才所敏明, 五太子政史, 佐藤直, 山本博資, 辻井重男, 野田 啓一 “暗号通貨（ビットコイン）・ブロックチェーンの高信頼化へ向けての MELT-UP 活動（III）-構造の精査-” *Proc. SCIS2019*, 4E2-3. Jan. 2019.

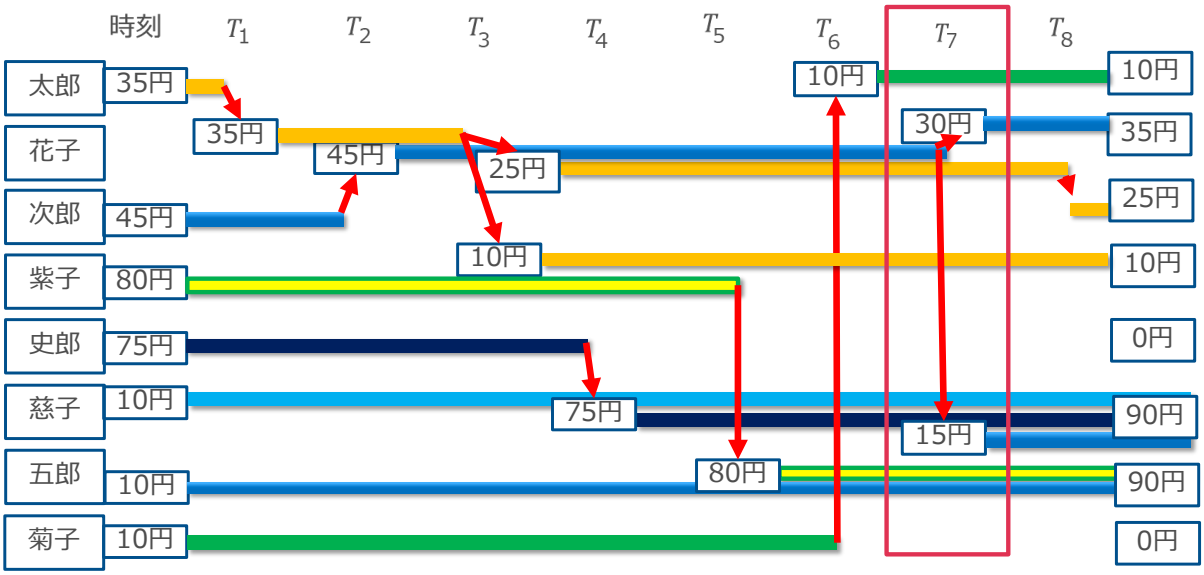

図 4 通貨所持の時間的変遷，タイムチャート

[7] 山澤昌夫，角田篤泰，近藤健，才所敏明，五太子政史，佐藤直，辻井重男，野田啓一，“暗号通貨（ビットコイン）・ブロックチェーンの高信頼化へ向けての MELT-UP 活動 — 秘密鍵管理を中心に —,” *Proc. SCIS2018*, 4F2-2. Jan. 2018.

[8] 山澤昌夫，角田篤泰，近藤健，才所敏明，五太子政史，佐藤直，山本博資，辻井重男，野田啓一，“暗号通貨（ビットコイン）・ブロックチェーンの高信頼化へ向けての MELT-UP 活動 (II) — 運用と倫理 —,” *Proc. CSS2018*, 3B3-5. Oct. 2018.

[9] `https://www.fsa.go.jp/news/30/singi/20181214.html`

[10] 佐藤雅史，“ ブロックチェーンの署名鍵を誰がどうやって管理するのか,” 日経 FinTech, 2016 年 12 月 12 日，セコム IS 研究所.

[11] 松尾真一郎，他，“ブロックチェーン技術の未解決問題,” 日経 BP, pp.50-54, 2018 年 1 月.

[12] 角田篤泰，山澤昌夫，白鳥則郎，“デジタル・アイデンティティの危殆化に抗う『デジタル寺院』構想, ” 日本セキュリティ・マネジメント学会第 32 回全国大会，2018 年 6 月 16 日

[13] 山澤昌夫, 角田篤泰, 近藤健, 才所敏明, 五太子政史, 佐藤直, 山本博資, 辻井重男, 野田啓一, “セキュリティマネジメントのコンテクスト，より深い理解へのの MELT-UP 活動現代の課題と啓蒙,” MELT-UP Activities To Develop Consistent Understanding of Security Management, Recent Issues and Solutions，日本セキュリティ・マネジメント学会第 32 回全国大会，2018 年 6 月 16 日.

[14] 辻井重男, 笠原正雄編著，「暗号理論と楕円曲線」, 森北出版, 2008 年 8 月.

[15] 警察庁広報資料，「平成 30 年におけるサイバー空間をめぐる脅威の情勢等について」，警察庁，平成 31 年 3 月 7 日.

[16] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol.21, no.2, pp.120-126, Feb. 1978.

[17] V. Shoup, “Practical Threshold Signatures,” *Proc. EUROCRYPT 2000*, Lecture Notes in Computer Science, vol.1807, pp.207-220, Springer, 2000.

[18] I. Damgård and M. Koprowski, “Practical Threshold RSA Signatures without a Trusted Dealer,” *Proc. EUROCRYPT 2001*, Lecture Notes in Computer Science, vol.2045. pp.152-165, Springer, 2001.

[19] I. Damgård and K. Dupont, “Efficient Threshold RSA Signatures with General Moduli and No Extra Assumptions,” *Proc. PKC 2005*, Lecture Notes in Computer Science, vol.3386, pp.346-361, Springer, 2005.

[20] FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013.

[21] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, “Robust Threshold DSS Signatures,” *Proc. EUROCRYPT 1996*. Lecture Notes in Computer Science, vol.1070, pp.354-371, Springer, 1996.

[22] R. Gennaro, S. Goldfeder, and A. Narayanan, “Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security,” *Proc. ACNS 2016*, Lecture Notes in Computer Science, vol.9696. pp.156-174, Springer, 2016.

[23] R. Gennaro and S. Goldfeder, “Fast Multiparty Threshold ECDSA with Fast Trustless Setup,” *Proc. ACM CCS 2018*, pp.1179-1194, 2018.

[24] Yehuda Lindell and Ariel Nof, “Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody,” *Proc. ACM CCS 2018*, pp.1837-1854, 2018.

[25] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” *Proc. ASIACRYPT 2001*, Lecture Notes in Computer Science, vol.2248, pp.514-532, Springer, 2001.

[26] A. Boldyreva, “Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme,” *Proc. PKC 2003*. Lecture Notes in Computer Science, vol.2567, pp 31-46, Springer, 2003.

[27] 辻井重男, 板倉征男, 山口 浩, 北沢 敦, 齋藤真也, 笠原正雄 “生体情報が秘密鍵に埋め込まれた構造を有する公開鍵暗号方式” 信学技報，*Proc.SCIS2000*,D07,2000.

[28] 板倉征男, 岩田 哲, 尾形わかは, 黒澤 馨, 辻井重男 “DNA 情報を組込んだ公開鍵暗号方式” 信学技報, *Proc.ISEC2000-42*,pp.137144, 2000.