ブロックチェーン米国市場調査　報告書

この報告書について

この報告書は、

IOTAについての調査 (10p)

IOTAプロジェクトの概要（1p）

- Goal
- Organization
- ICO
- Investors

IOTAプロトコルの概要（2p）

- Tangle (DAG)
- Curl Hash function
- Current status of security evaluation on Tangle and DAG
- evaluation of concept (if hash is good)

IOTAプロジェクトについて指摘された問題点と対応経緯（2p）

- Attack on Curl
- Real attack demo
- Timeline
- Responsible Disclosure

IOTA財団の対応における組織的な問題点（2p）

- Summary from tangle blog
  http://www.tangleblog.com/wp-content/uploads/2018/02/letters.pdf
- https://thebitcoinnews.com/mit-criticizes-iota-gaping-hole-in-its-software-and-deceptive-marketing/
- https://blog.iota.org/official-iota-foundation-response-to-the-digital-currency-initiative-at-

the-mit-media-lab-part-1-72434583a2

IOTAプロジェクトの現状（1p）

- Current software
- Development Roadmap

Alternative for IOT（1p）

- スケーラビリティ　機器数
- サプライチェーン
- トレーサビリティ
- Single Point

IOTAプロジェクトの新たな攻撃募集（1p）

- Call for attack to Troika
  http://blog.iota.org/678e741315e8
  http://blog.iota.org/615d2d79001

標準化動向 (5p)

ISO TC307の現状（3p）

ISO TC307は、ISOにおいてブロックチェーンおよびDLT(分散台帳技術）の標準化を行う技術委員会であり、2017年の4月にシドニーで第1回目の国際会議が開催されて以来、東京（2017年11月）、ロンドン（2018年5月）、モスクワ（2018年11月）と計4回開催されている。
現在、TC307の組織は以下のように構成されている。

- WG1: Foundations
- WG2: Security, privacy and identity
- WG3: Smart contracts and their applications
- JWG4: Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
- WG5: Governance
- SG2: Use Cases
- SG7: Interoperability of blockchain and distributed ledger technology systems

Current stats of documents

Future plan and schedule

日本国内での取り組み（1p）

CGTF (Cryptoasset Governance Task Force)

コインチェックによる暗号資産の流出事件が2018年1月に発生したことを契機に、仮想通貨交換取引所のセキュリティ確保とガバナンスの確立が急務となった。これを受けて、日本のセキュリティ専門家と一部のブロックチェーン事業者の有志で、任意団体VCGTF（Virtual Currency Governance Task Force）が設立された。その後、金融庁の研究会において、仮想通貨の代わりに暗号通貨という新しい呼称を用いる方針となったため、この任意団体の名称はCGTF（Cryptoasset Governance Task Force）に変更となった。金融庁は、仮想通貨交換取引所について、業界団体などによる自主規制を行う方針を取っている。一方で、

VCGTFが設立された当初から、

CGTFでは、主に仮想通貨交換取引所が、ISMS（ISO/IEC 27000シリーズ）に準拠したセキュリティマネジメントプロセスを実施することができるように、同標準に基づいたセキュリティ確保のためのプラクティスを記述した文書を作成している。その他に、暗号資産に関わる用語の定義を行う文書を作成している。

- Relationship to JVCEA

その他の動向（1p）

標準化団体

- ITU-T
- IETF
- W3C

学術会議

- FC
- Scaling Bitcoin