2F-04

ブロックチェーン上における ソフトウェア更新から考察するユーザーの振る舞い

今村 光良† 面 和成††‡

†筑波大学 大学院 システム情報工学研究科 ††筑波大学システム情報系 ‡情報通信研究機構

1 はじめに

ネットワークに接続された端末において，常に新しいソフトウェアを利用することは，セキュリティを向上させるためにも重要である．P2P ネットワークで構成されるブロックチェーンにおいては，中央集権的な管理方法と異なり，ソフトウェアのアップデートはユーザーに依存する．分散台帳に対する二重支払い攻撃など重大な問題を回避するために，常に新しいソフトウェアを利用するユーザーが多数を占める一方，何らかの理由により，脆弱な古いソフトウェアを利用し続けるユーザーも存在する．

本研究ではブロックチェーンを用いたサービスである Bitcoin を対象に，ブロックチェーン上におけるユーザーが振る舞う特徴として，ソフトウェアの更新状況に着目し，利用ソフトウェアの動態を観測した結果について報告する．

2 関連研究

ソフトウェアのライフサイクルにおける新規バージョンのリリースは，ソフトウェアの普及状況に影響を受けるビジネスプロセスにおいて，計画や意思決定に密接に関係する重要なイベントと認識され，観測結果に対する特徴分析やモデル化などが，研究課題として取り組まれている．

Cao らの研究 [1] では，ソフトウェアのライフサイクルに関する経験的法則 (リーマンの法則 [2]) が，ブロックチェーンで利用されるソフトウェアにも同様の傾向が確認できるかを検証している．

代表的なブロックチェーンとして， Bitcoin，Dogecoin，Ripple，Steem，Stellar，Tron の 6 種類を対象とした結果， 6 種類の経験則については有意な結果が得られ，品質の低下と複雑性の増加に関する 2 つの経験則については有意な結果が得られないことを報告している．

また，ブロックチェーンのソフトウェアについては，開発が成熟したソフトウェアと比較して，大幅な変更点が存在するため，開発における進捗が滑らかではない傾向を示す特徴について指摘し，ブロックチェーンの特性を表現するより適した経験則の適用が課題と報告している．

Dutta らの研究 [3] では，システムダイナミクスの観測結果を利用する経験的アプローチにより， Android と iOS を基本 OS としたスマートフォンの普及モデルを提案している．当該研究では，システムダイナミクスベースの普及モデルを用いると， Android と iOS が，長時間にわたり指数関数的な成長パターンを示し，その後に飽和と低下が続くことを報告している．また，この傾向に関する原因が明確になれば，ウェアラブル端末などを含む他のデバイスへ拡大する計画が立案でき，ビジネスにおける新たな成長機会の追求できる可能性について言及している．

3 分析

3.1 データ

本研究では，先行研究 [4] でも利用されている良く知られたデータでとして，Bitcoin のメインネットワークに関する完全なノードデータを公開している，`bitnodes.earn.com` より，1 時間ごとにノードが利用しているソフトウェアのデータについて収集した．当該データについては，1 日の 12 回のスキャンに 1 度でも存在することが確認できたノードを集約することで，日次データ化している．

データ収集期間は，2018 年 1 月 10 日から 2019 年 12 月 31 日までの 720 日間となる．これらの収集データは、IPv4，IPv6，TOR の 3 つの接続プロトコルタイプをサポートしている．なお，この調査では，ネットワーク上に公開状態であり，全て台帳を持つ完全ノードのソフトウェアである Bitcoin Core を対象としており，接続できないノードや全ての元帳を持たないライトノードのソフトウェアは含まない．さらに，ネットワーク観測において問題となるファイアウォールやネットワークアドレス変換（NAT）により隠れているノードには到達することができないため，この調査は先行研究 [4] と同様の潜在的な制限を持つ．

3.2 分析結果 1

本節では，Bitcoin ネットワークにて利用されている Bitcoin Core のバージョンについて確認する．観測期間中に確認した Bitcoin Core のバージョンのリリース時期を纏めたものが表 1 になる．

ネットワークにて観測できた Bitcoin Core については 2009 年 1 月 9 日に，メジャーバージョン 0.1.∗ がリリースされてから 9 年後の 2018 年 1 月 10 日の時点で，もっとも古いバージョンが 0.10.∗ になる．また，観測期間中

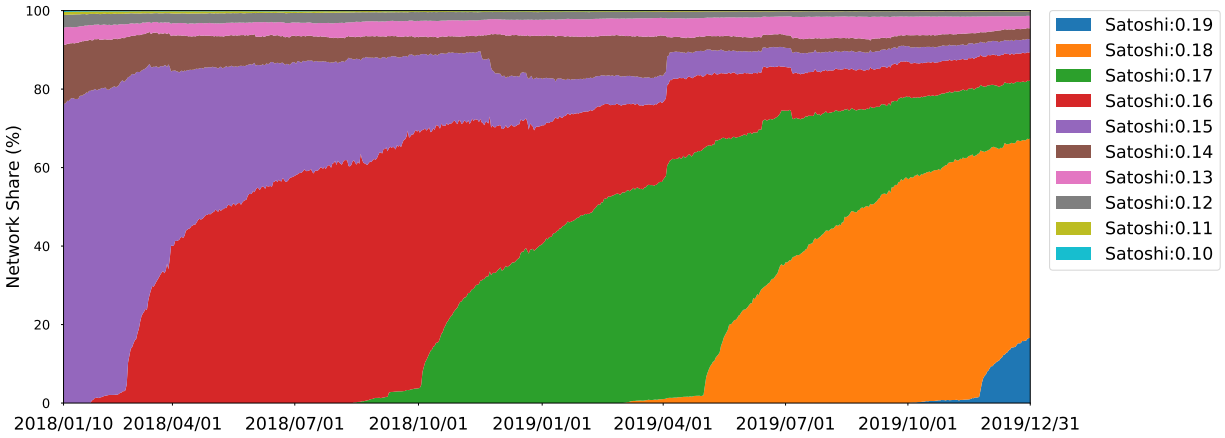

図 1: Bitcoin ネットワークにおける Bitcoin Core のバージョンの累積分布図

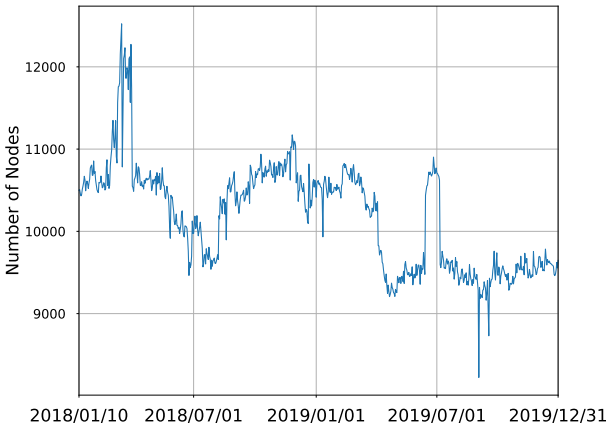

図 2: Bitcoin ネットワークにおける Bitcoin Core のノード数

にリリースされたバージョンには，0.16.∗，0.17.∗，0.18.∗，0.19.∗ の 4 種類が存在している．

表 1: Bitcoin Core のリリースバージョン

Major version	Release	Interval days
0.10.*	16 February 2015	0
0.11.*	12 July 2015	146
0.12.*	23 February 2016	226
0.13.*	23 August 2016	182
0.14.*	08 March 2017	192
0.15.*	14 September 2017	190
0.16.*	26 February 2018	165
0.17.*	03 October 2018	219
0.18.*	02 March 2019	150
0.19.*	09 October 2019	221

3.3 分析結果 2

本節では，ネットワークにおける Bitcoin Core のバージョンの普及状況について確認する．観測期間中に観測した Bitcoin Core の各バージョンのネットワークにおける普及状況を図 1 に示し，ノード数を図 2 に示す．

図 1 に示す通り，新規バージョンのリリース後における普及の傾向については，先行研究 [3] と同様に，指数関数的な成長後，飽和と低下の傾向を持つ．この時の全体のノード数については，図 2 に示す通り，10,000 ノードを平均に推移している．

一方で，普及の飽和に到達する位置については，観測開始時点において，80% 程度を占めている バージョン 0.15 が最も高い水準であり，その後の新規リリースされたバージョンについては，ネットワーク全体の 60 % 程度までの普及率に到達した時点で，次のメジャーバージョンがリリースされ，減衰している．過去のバージョンは新規バージョンのリリース後，シェア率が減衰していくが，一定数が滞留し続けていることが確認できる．

参考文献

[1] J. Cao, X. Wang, Z. Li, Q. Gu, and Z. Chen, “The evolution of open-source blockchain systems: An empirical study,” in *Proceedings of the 11th Asia-Pacific Symposium on Internetware*, 2019, pp. 1–10.

[2] M. M. Lehman, “Programs, life cycles, and laws of software evolution,” *Proceedings of the IEEE*, vol. 68, no. 9, pp. 1060–1076, 1980.

[3] A. Dutta, A. Puvvala, R. Roy, and P. Seetharaman, “Technology diffusion: Shift happens—the case of ios and android handsets,” *Technological Forecasting and Social Change*, vol. 118, pp. 28–43, 2017.

[4] M. Imamura and K. Omote, “Difficulty of decentralized structure due to rational user behavior on blockchain,” in *International Conference on Network and System Security*. Springer, 2019, pp. 504–519.