

関税・外国為替等審議会 外国為替等分科会

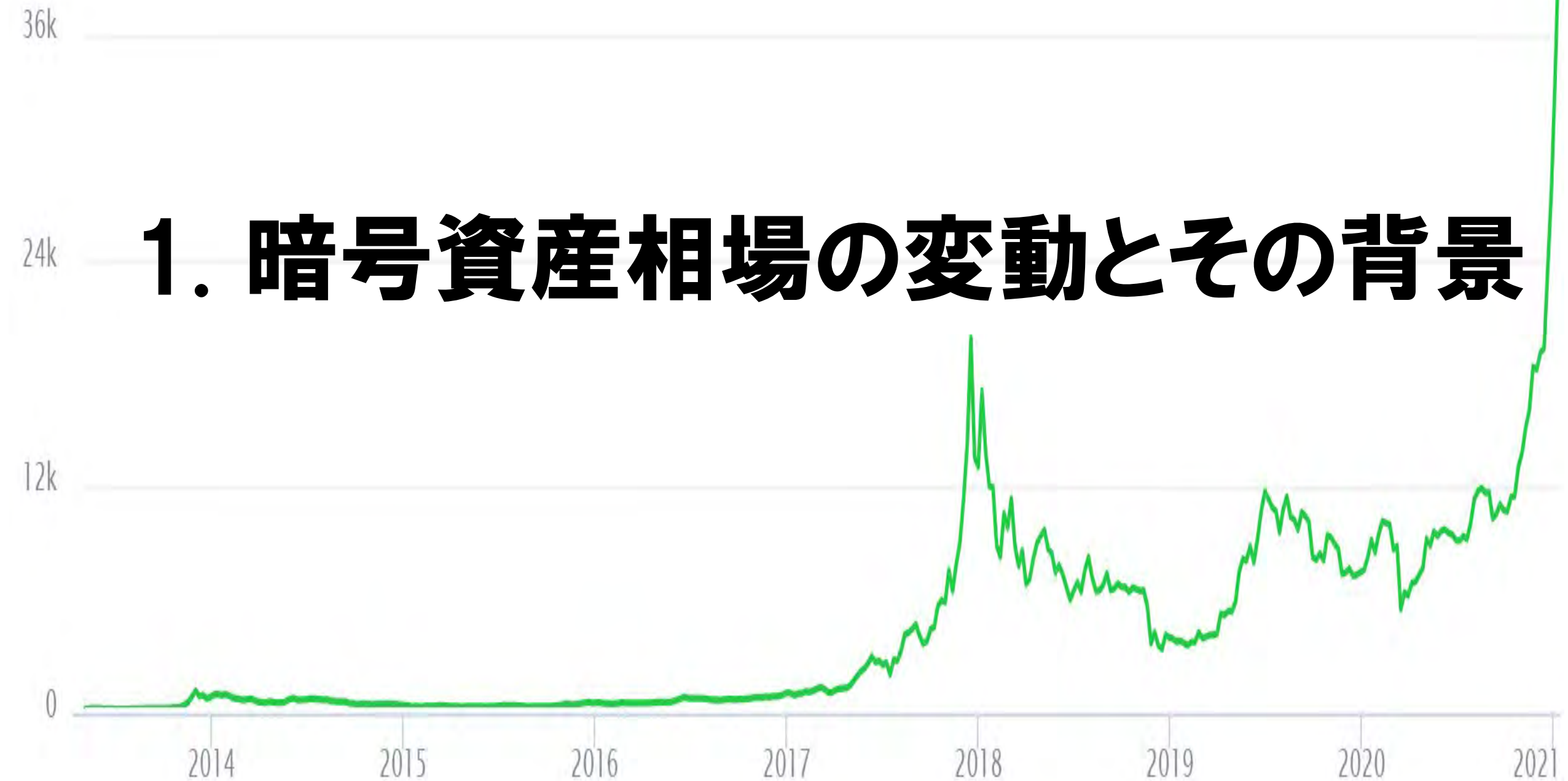
経済のデジタル化がもたらす国際金融上の課題・対応
～ステーブルコイン、CBDC等のデジタル通貨についての現状・展望、課題・対応

京都大学 公共政策大学院
岩下 直行

目次

1. 暗号資産相場の変動とその背景
2. ビットコインの構造とマイニング
3. 暗号資産の抱えるリスク
4. フェイスブックのリブラ構想
5. 中銀デジタル通貨(CBDC)

1. 暗号資産相場の変動とその背景



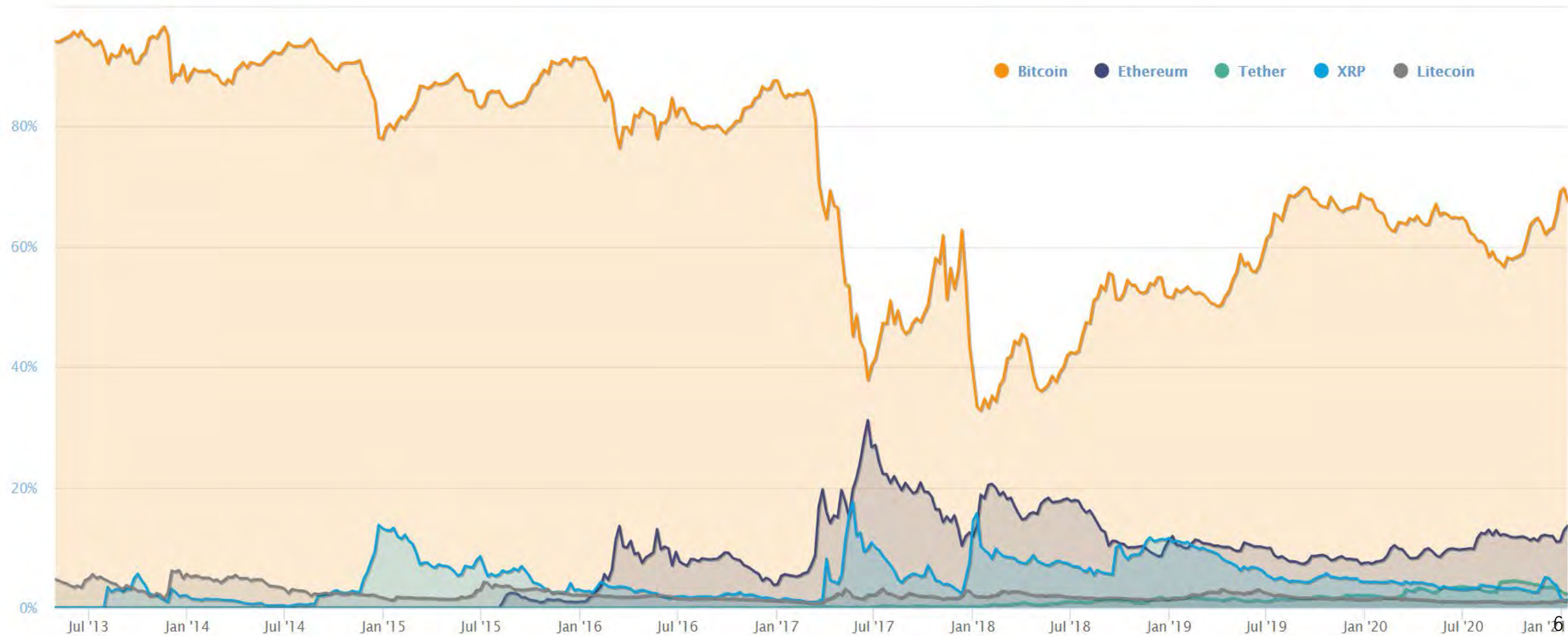
ビットコインの対ドル相場の推移



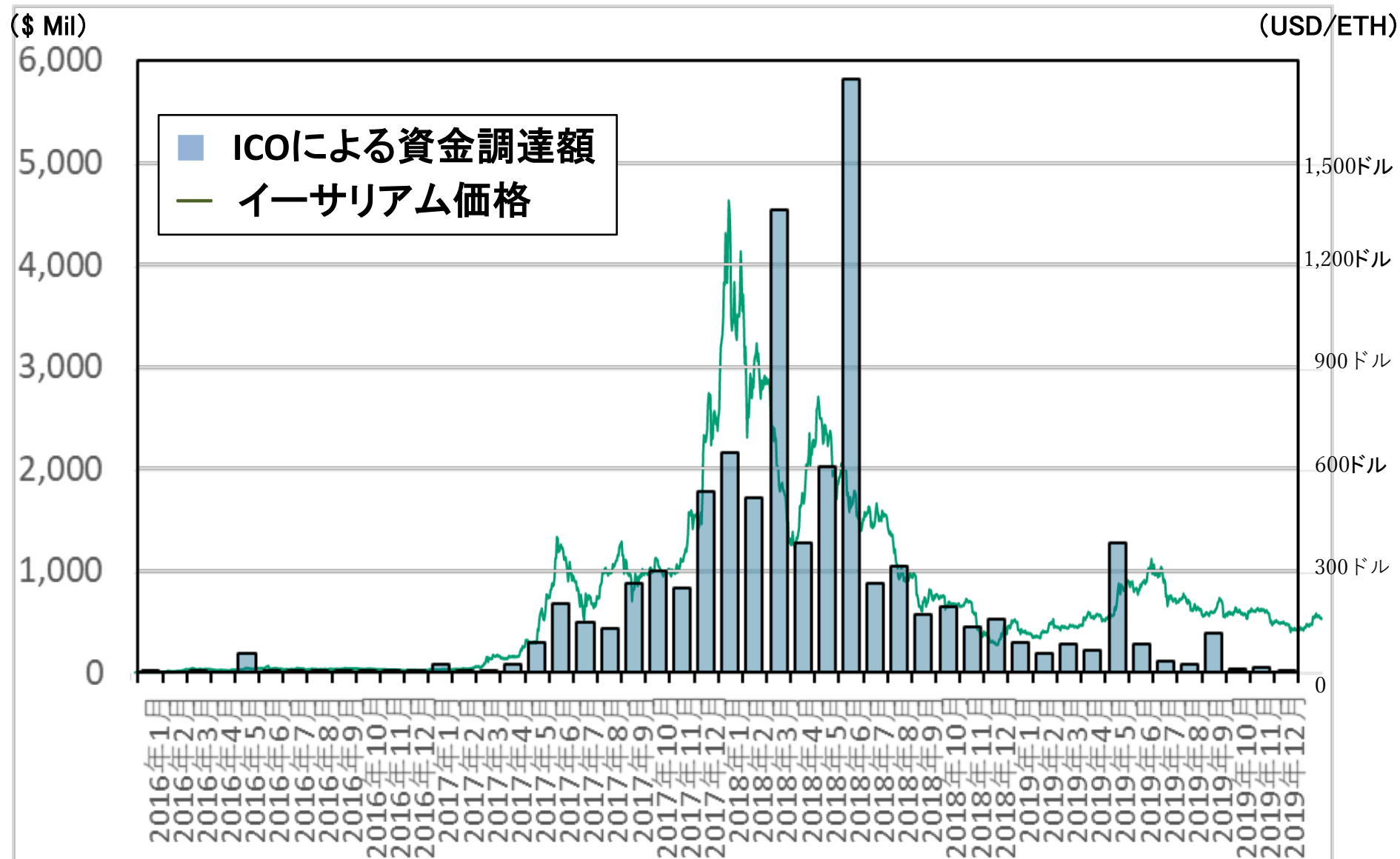
暗号資産全体の 流通総額の推移



暗号資産流通総額の 銘柄別シェアの推移



ICOによる資金調達額とイーサリアム価格の推移

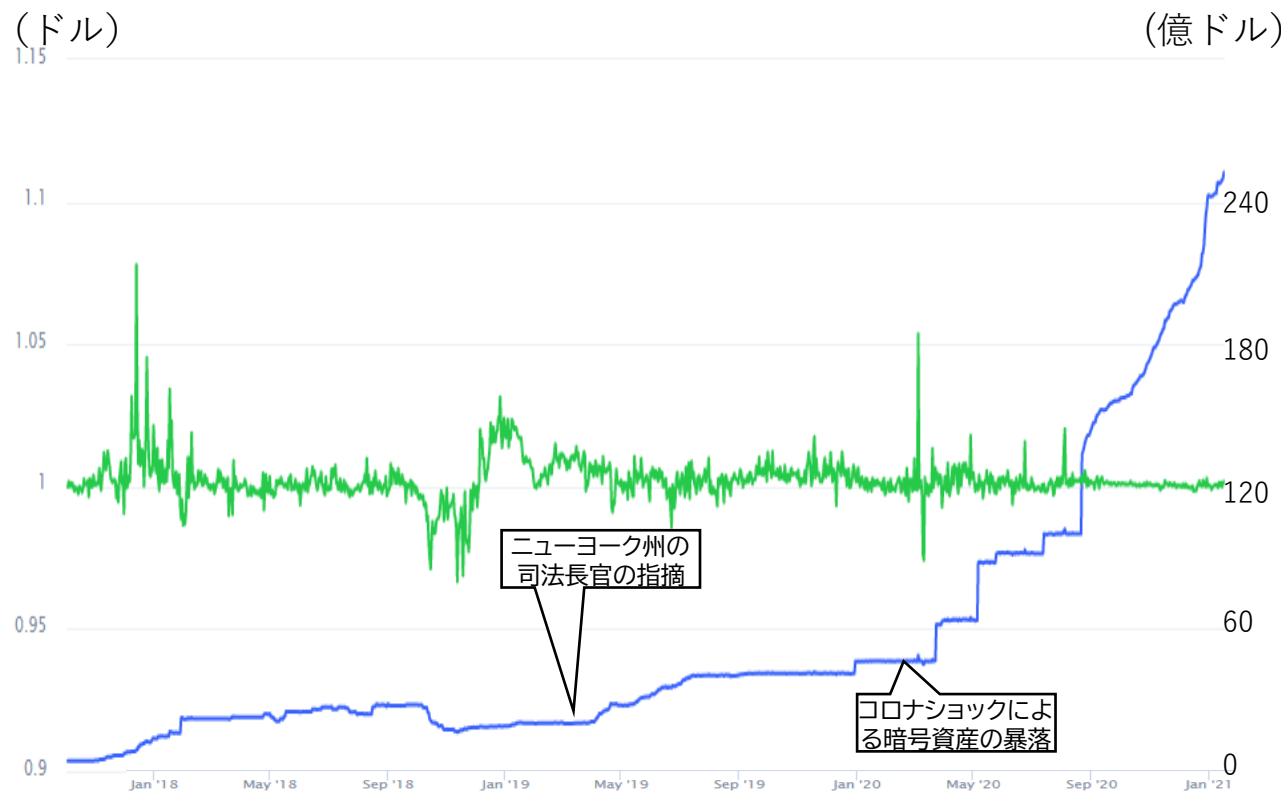


ステーブルコイン Tether (テザー)

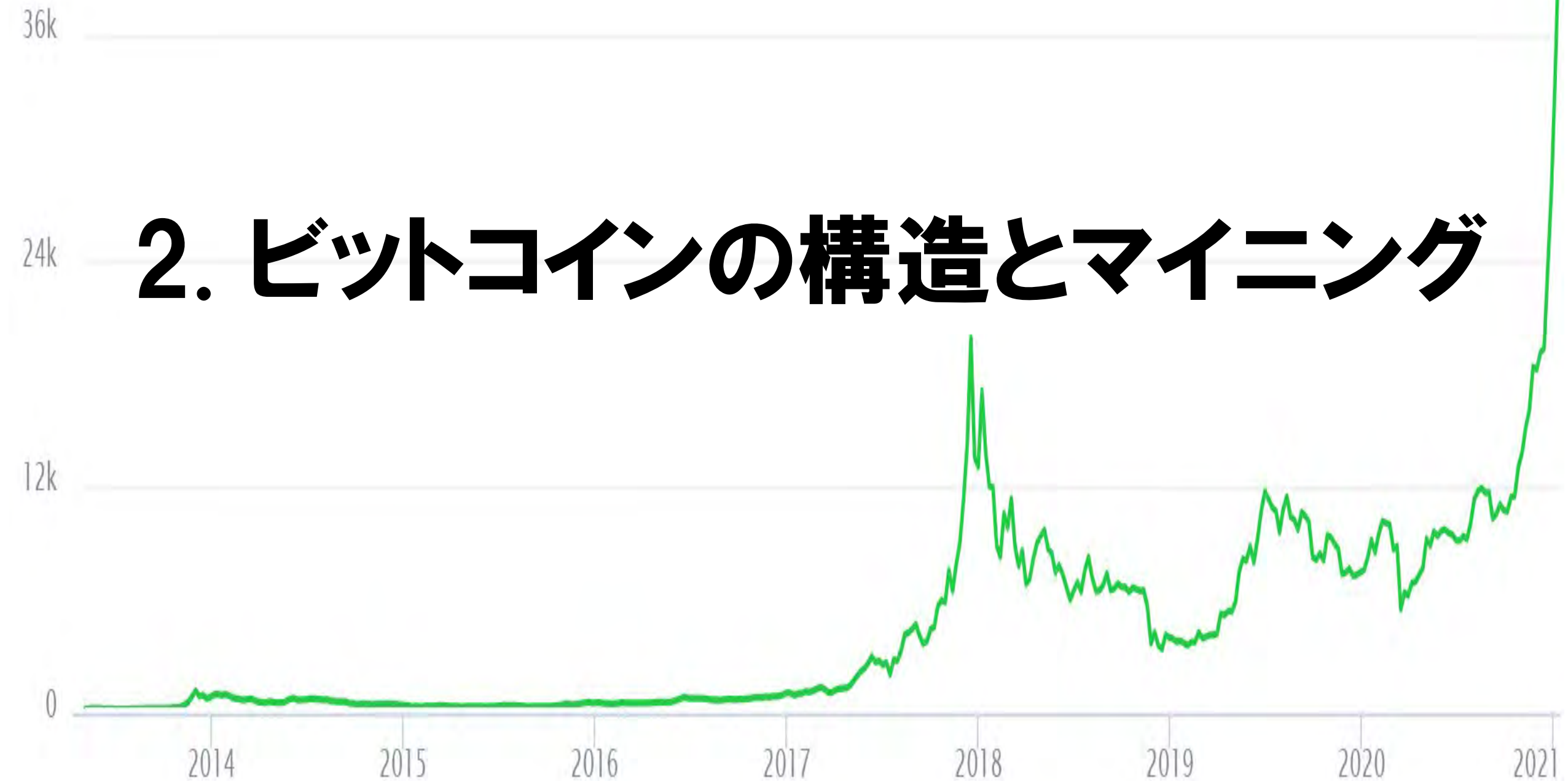
Tetherは、香港のBitfinex社と関係の深いテザー社が発行する暗号資産。「法定通貨（米ドル）との交換により発行され、その価格が法定通貨と等しい」ことをセールスポイントとするステーブルコイン。ただし、テザーはテザー社の負債ではなく、Bitfinex社の負債でもない。2018年頃から、テザーは暗号資産取引所がドルの代わりに利用する決済手段としての地位を確立し、日々の取引金額はビットコインを抜いて暗号資産の中で最大である。

2019年4月、米国ニューヨーク州の司法長官が、ビットフィネックス社が自らの損失を補填するためにテザーの裏付け資産を不正利用したとの捜査報告を受け、テザー社からビットフィネックス社への資金移動を禁止する旨の裁判所命令を取得したと発表した。これに対し、ビットフィネックス社側の法律事務所は、州司法長官の発表を無視して、テザーの発行をむしろ積極化させた。その発行額は、4月の20億ドルから倍増し、7月には40億ドルを超えた。ビットコインの価格が急上昇したのも同じ時期である。

2020年3月のビットコイン相場下落以降は、発行額を更に大幅に増加させ、2021年1月現在、発行額254億ドル、第3位の時価総額を持つ暗号資産となっている。



2. ビットコインの構造とマイニング



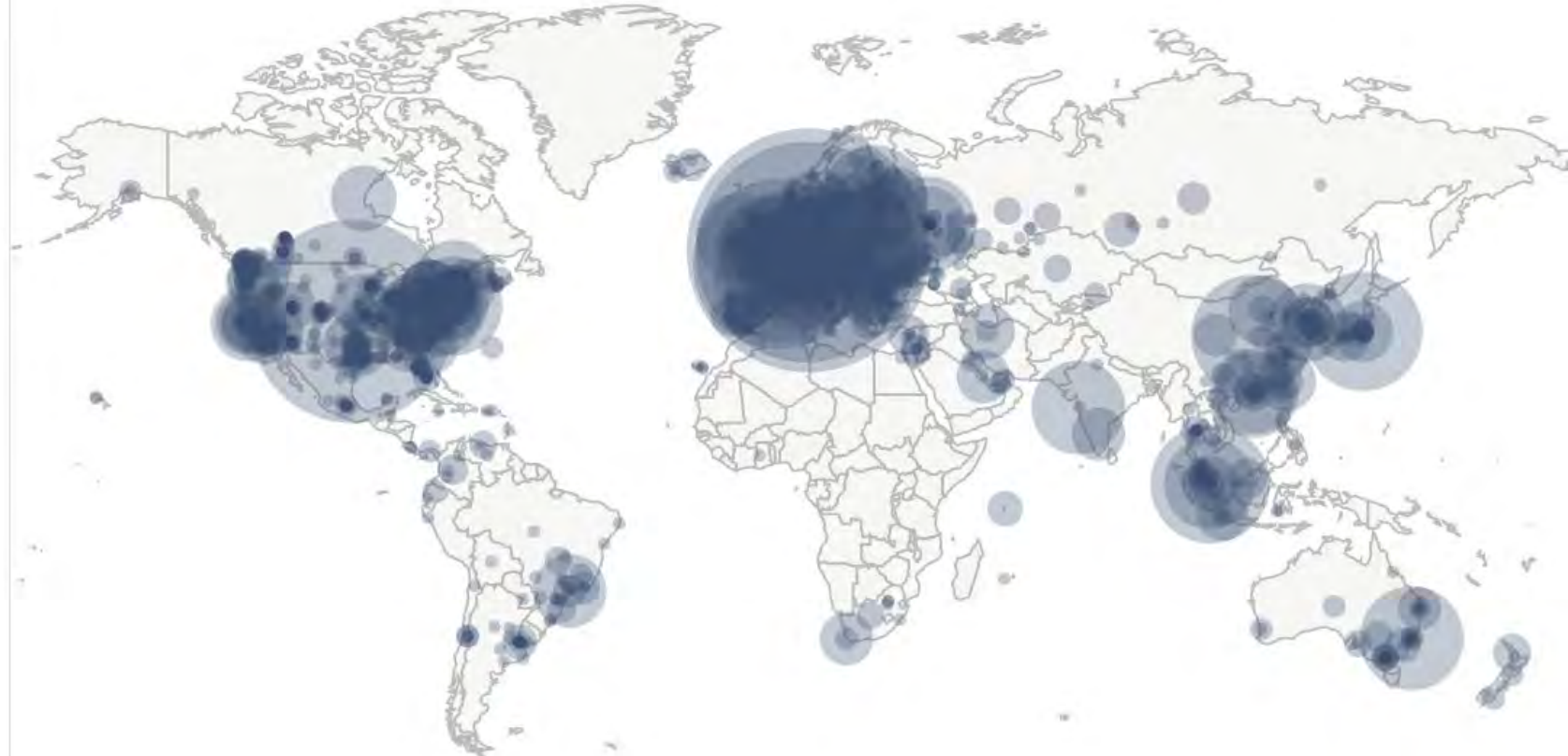
世界のビットコイン・ノードの分布

11575 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2703 (23.35%)
2	United States	1996 (17.24%)
3	Germany	1851 (15.99%)
4	France	617 (5.33%)
5	Netherlands	445 (3.84%)
6	Canada	371 (3.21%)
7	United Kingdom	361 (3.12%)
8	China	239 (2.06%)
9	Singapore	239 (2.06%)
10	Russian Federation	230 (1.99%)
11	Japan	220 (1.90%)



ハッシュ値が満たすべき条件と難易度調整

256ビットのハッシュ値がある
数字よりも小さいこと(例えば、
256桁の2進数で、上20桁が
ゼロである状態)。

【難易度調整】

2,106ブロック毎(約2週間)に一度、直前の2,106ブロックの生成状況から「上何桁をゼロにするか」を再計算。
相場ではなく、マイナーの計算能力に依存して変化。

例えば、難易度が

「上20桁がゼロ」である場合、

H1= “0100101101011010110101000111010101..” はNG。

H2= “00000000000000000000000010110101011011...” はOK。

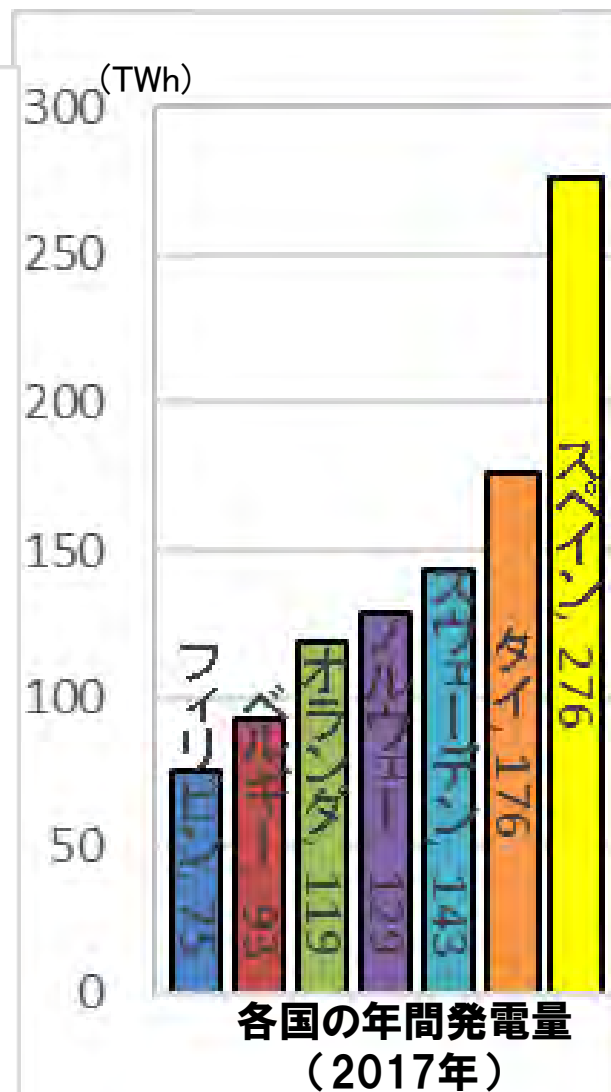
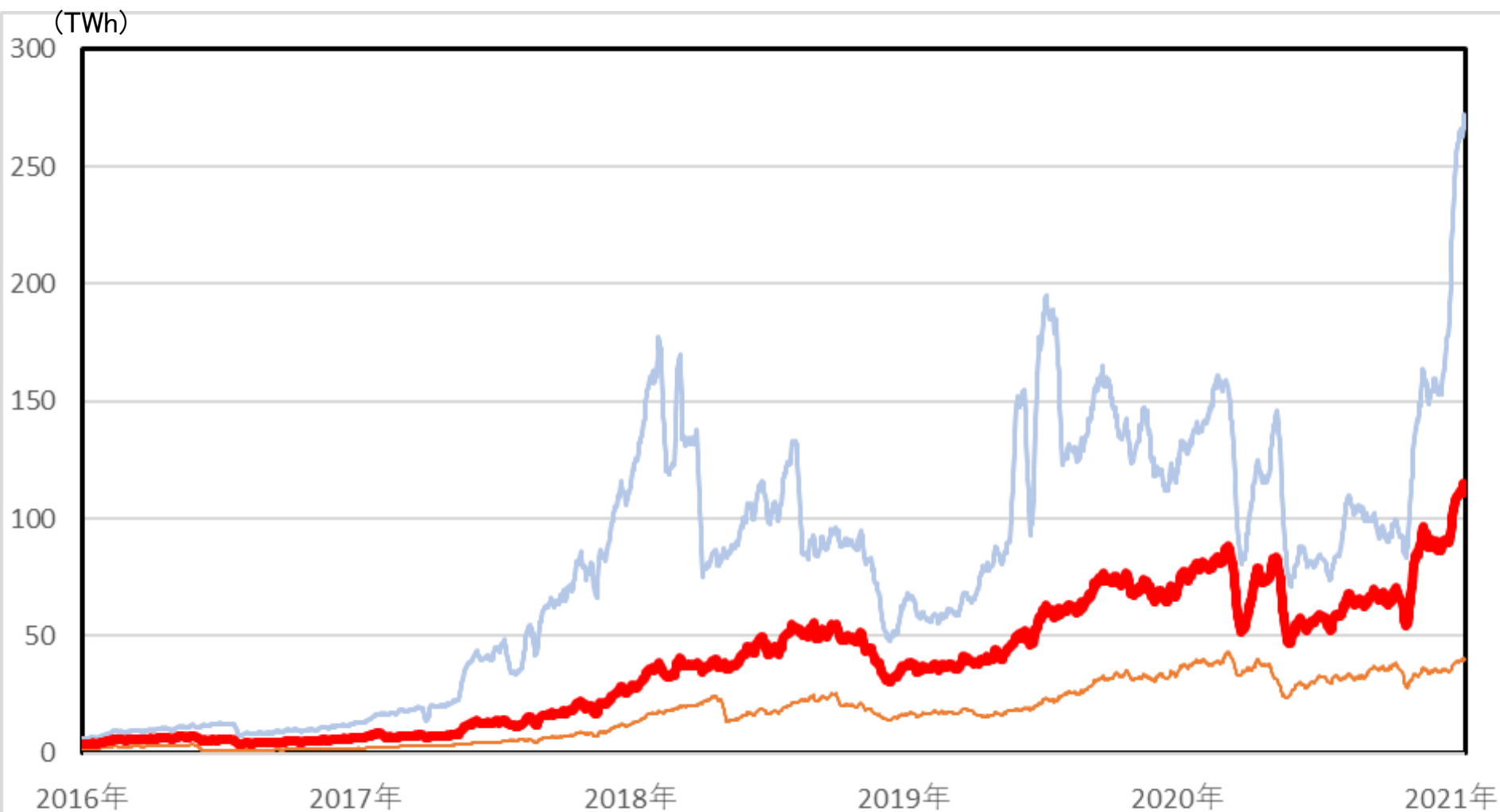
この0Kなハッシュ値が偶然に出る確率は、 $1/2^{20}$ 。

一人で試行を続けて偶然、OKなハッシュ値が出る確率が1/2を超えるには、72万回以上繰り返す必要がある。

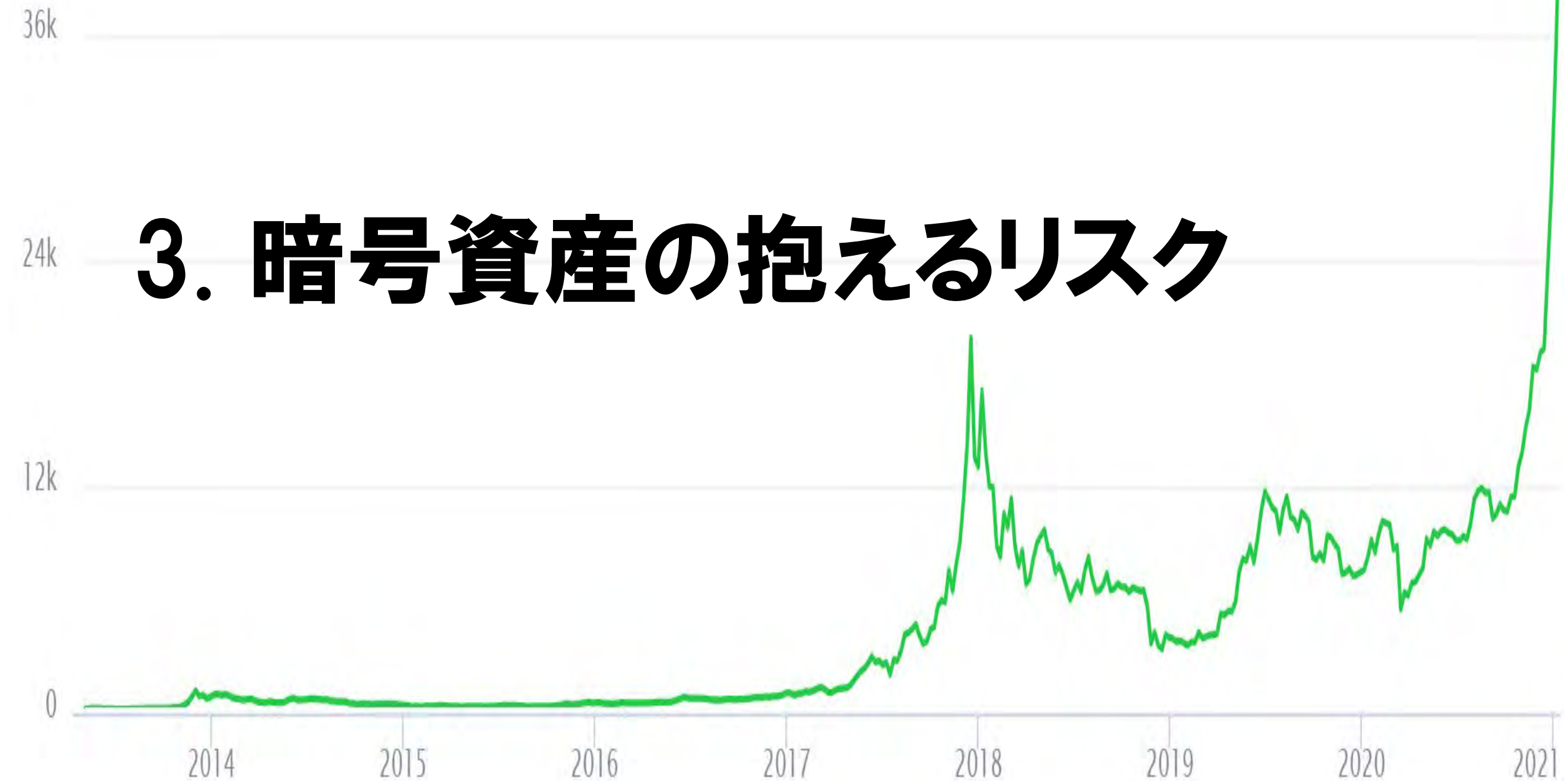


ビットコイン・マイニングの消費電力

Cambridge Bitcoin Electricity Consumption Indexの推計値(年間消費量換算値)



3. 暗号資産の抱えるリスク



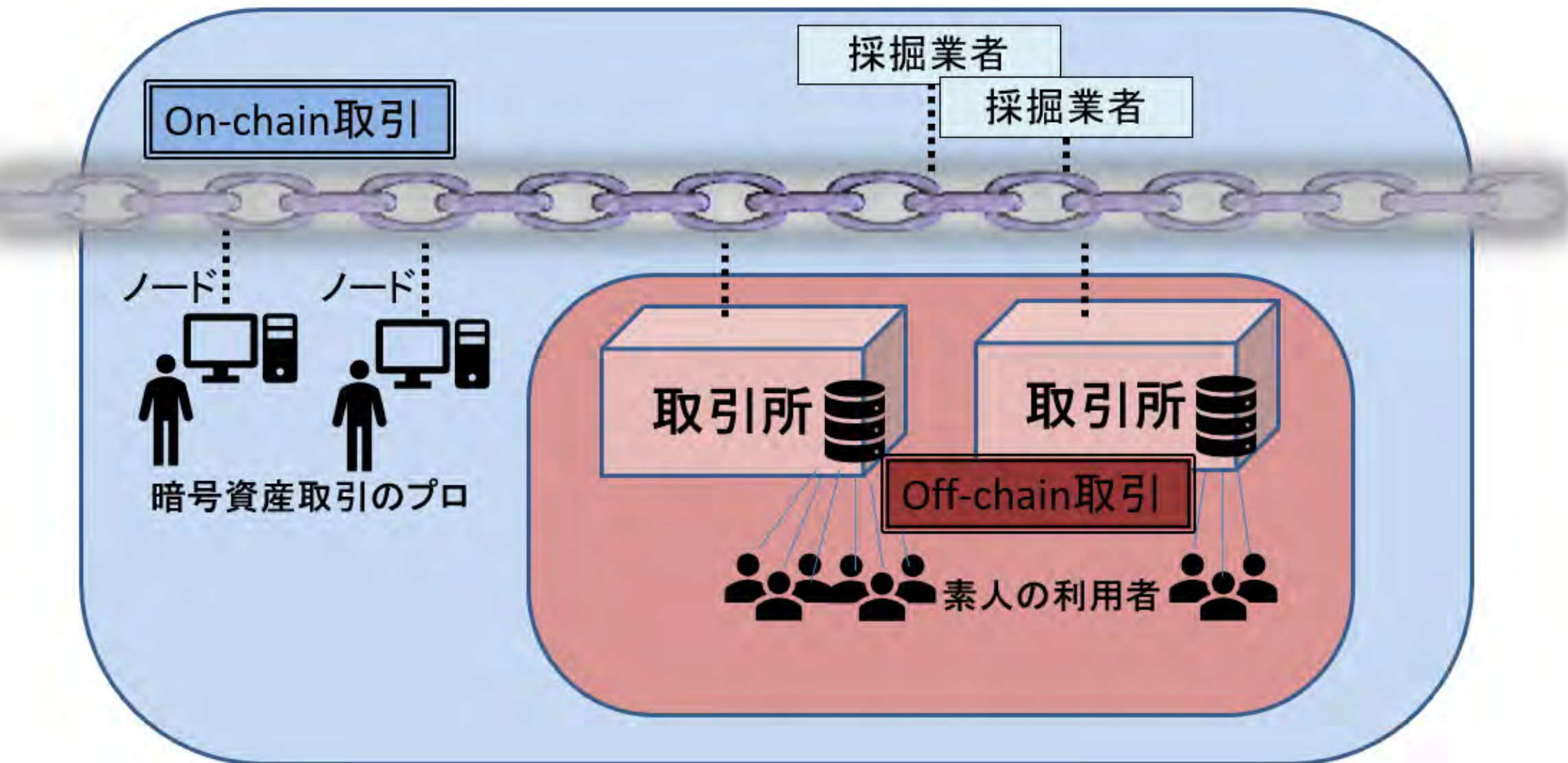
暗号資産交換業者へのサイバー攻撃等の事例

事件名	交換業者 の国籍	発生年月	被害額（報道等に基づく概数）		
			円建て	ドル建て	暗号通貨
Mt.GOX事件①	日本	2011年6月	7億円	875万ドル	－
Bitfloor事件	米国	2012年9月	0.2億円	25万ドル	24,000 BTC
Mt.GOX事件②	日本	2014年2月	480億円	4.8億ドル	850,000 BTC
Poloniex事件	米国	2014年3月	0.6億円	55万ドル	－
BitStamp事件	イギリス	2015年1月	5.8億円	500万ドル	19,000 BTC
Bitfinex事件	香港	2016年8月	66億円	6,600万ドル	119,756 BTC
CoinCheck事件	日本	2018年1月	580億円	5.3億ドル	526,300,010XEM
BitGrail事件	イタリア	2018年2月	182億円	1.7億ドル	1700 XRB
Coinrail事件	韓国	2018年6月	44億円	4,000万ドル	NXPS,ATC,NPER
Bithumb事件	韓国	2018年6月	35億円	3,100万ドル	XRP ?
Zaif事件	日本	2018年9月	70億円	6,200万ドル	BTC,MONA,BCH
Cryptopia事件	ニュージーランド	2019年1月	3.5億円	320万ドル	ETH ?
QuadrigaCX事件	カナダ	2019年1月	220億円	2億ドル	BTC、ETH、BCH
BitPoint事件	日本	2019年7月	32億円	3000万ドル	BTC、ETH、XRP

コインチェック事件におけるNEMの動き

時刻	金額(XEM)	送金元	送金先
2018/1/26 8:26	800,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 4:33	1,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:35	1,500,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:29	92,250,000	NC4C6PSUW5	NA6JSWNF24Y
2018/1/26 3:28	100,000,000	NC4C6PSUW5	NDDZVF32WB
2018/1/26 3:18	100,000,000	NC4C6PSUW5	NB4OJJCLTZW
2018/1/26 3:14	100,000,000	NC4C6PSUW5	NDZZJBH6JZP
2018/1/26 3:02	750,000	NC4C6PSUW5	NBKL OYXFIVE
2018/1/26 3:00	50,000,000	NC4C6PSUW5	NDODXOWFI7
2018/1/26 2:58	50,000,000	NC4C6PSUW5	NA7SZ75KF6Z
2018/1/26 2:57	30,000,000	NC4C6PSUW5	NCTWFIQOVIT
2018/1/26 0:21	3,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:10	20,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:09	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:08	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:07	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:06	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:04	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:02	10	NC3BI3DNMR2	NC4C6PSUW5

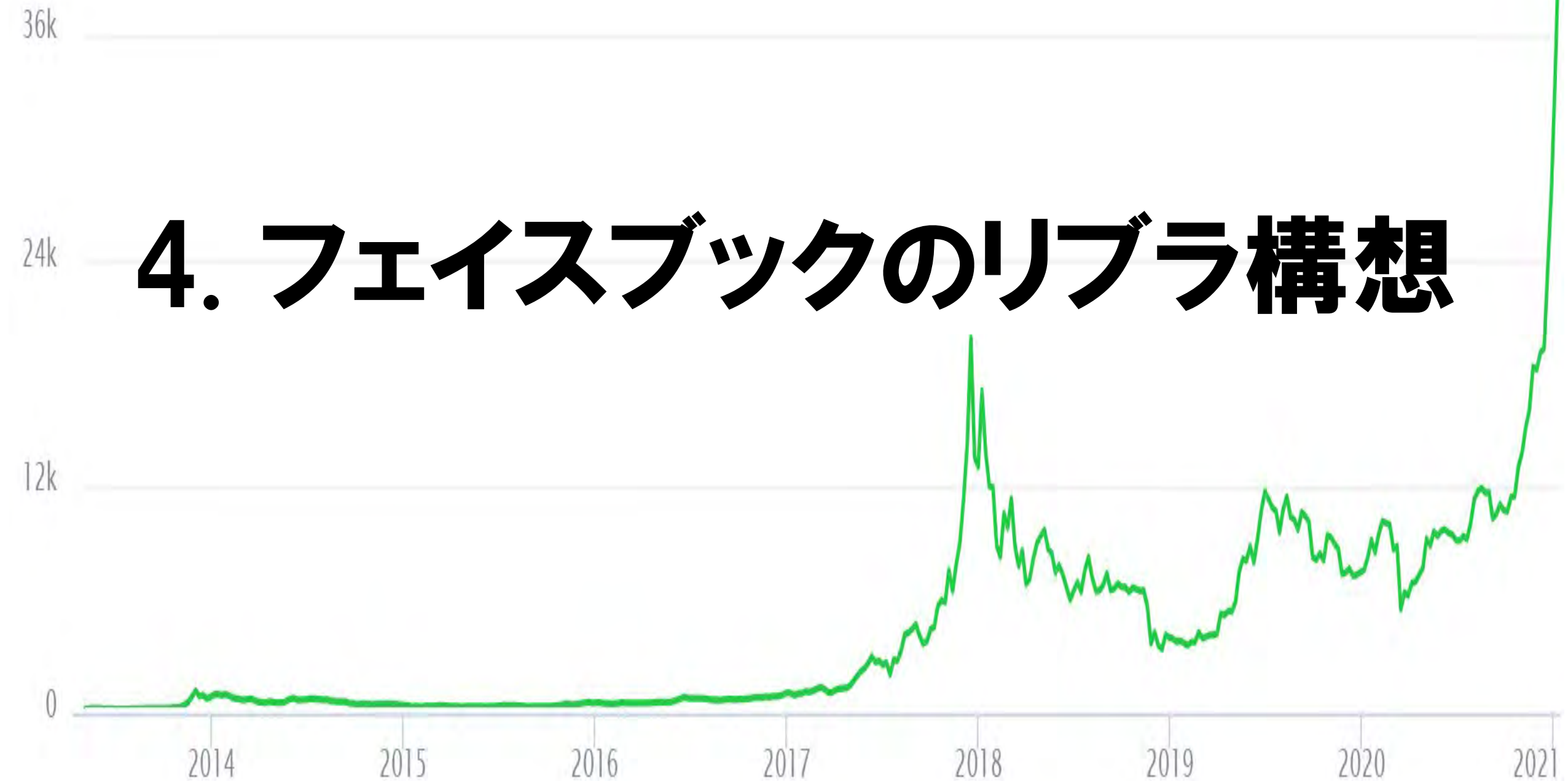
暗号資産取引の2つの類型



暗号資産取引の2つの類型の特徴

類型	On-chain取引	Off-chain取引
概要	ビットコインの黎明期から続けられてきた取引方法。利用者が自ら管理する秘密鍵でデジタル署名を生成し、自らのアドレスを含む取引記録がブロックチェーンに記録され、ブロックが伸延すれば書き換えが事実上不可能になる。	2013年頃から増えてきた暗号資産の交換業者を利用する取引方法。暗号資産は交換業者名義のまま、交換業者のRDBで振替決済を行う。利用者は秘密鍵やアドレスを持たず、ID、パスワード等で認証する。
利用者	ビットコイン黎明期に参加した愛好家、匿名による取引を希望する利用者、国境を跨いで送金・支払をする利用者、取引所間取引、採掘業者	暗号資産取引については素人である個人投資家、暗号通貨の交換業者の顧客
メリット	取引がブロックチェーンに書かれるので取り消されることがない。（ほぼ）匿名での取引が可能。仮に交換業者にトラブルがあったとしても、ブロックチェーンに記録された暗号資産は安全。	投資家自らが秘密鍵を管理する必要がなく、秘密鍵の紛失や漏洩の被害を受けない。パスワード等の簡便な認証手段で取引できるため、素人でも取引できる。
デメリット	利用者自らがデジタル署名の秘密鍵を安全に管理する必要があるため、技術に詳しい必要。秘密鍵の紛失や不正利用があれば、暗号資産を失う。	取引は交換業者のRDBに書かれるだけなので、交換業者だけが頼り。サイバー攻撃等で交換業者が被害を受けると、資産を失うリスクもある。

4. フェイスブックのリブラ構想



Libra White Paperの概要

- Libraは、世界通貨として数十億人もの人々の金融基盤となることを目的とする。
- Libraは、ブロックチェーンの技術を利用して発行される暗号資産（仮想通貨）である。
- Libraは、法定通貨（ドル、ユーロなど）のバスケットの価値に連動するステーブルコインとして設計される。為替相場の変動により、円建てやドル建てのLibraの価格は変動するが、その価格は市場取引に任せる。
- Libraは、スイスに本拠を持つ独立組織であるLibra Associationによって運営される。
- Libraは開始から5年後にpermissioned blockchainからpermissionless blockchainに移行する。

2019年10月19日

グローバル・ステーブルコインに関する G20プレスリリース(仮訳)

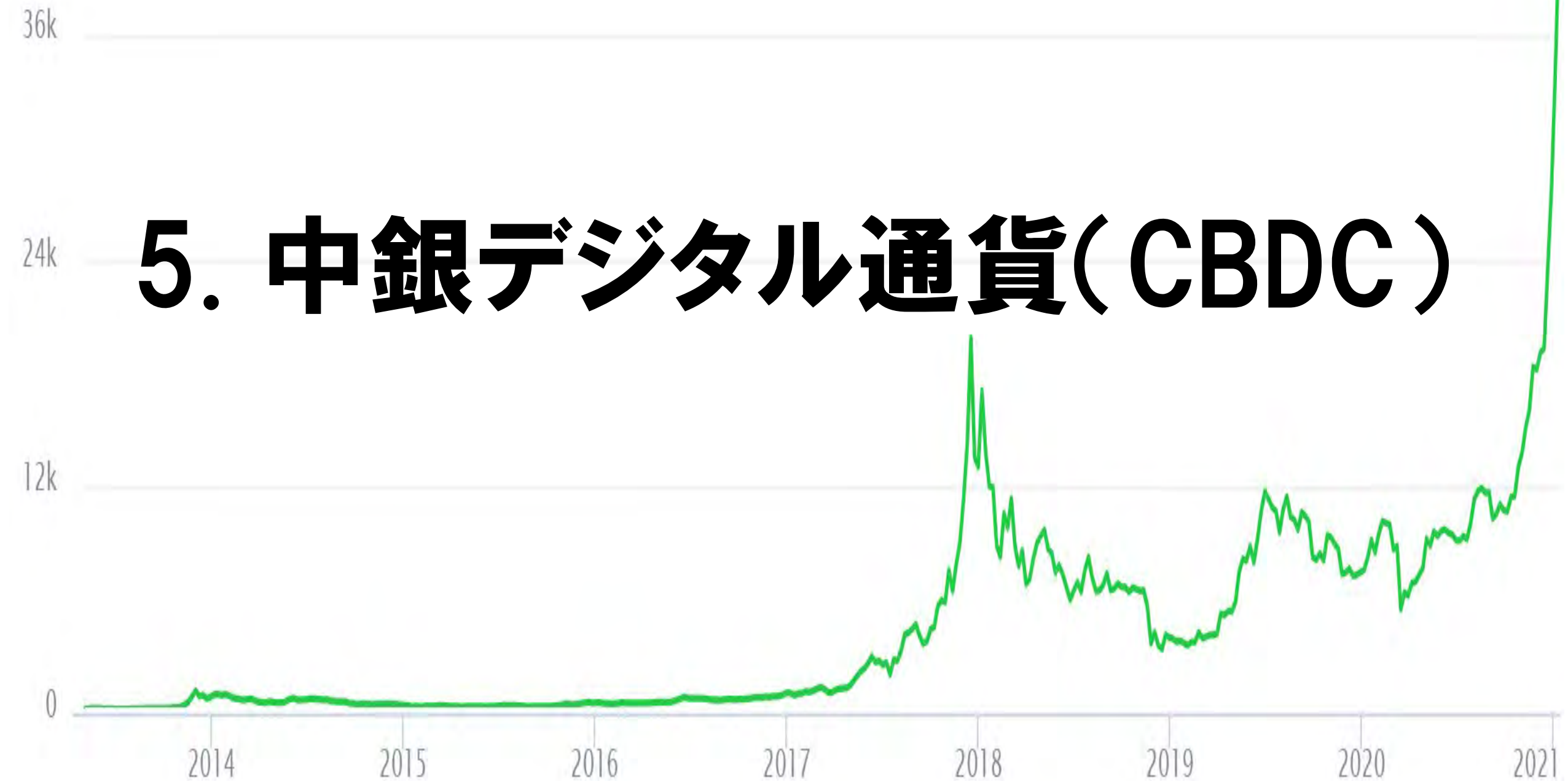
1. 我々は、基準設定主体が現在行っている金融技術革新から生じる既存の及び生じつつあるリスクについての作業を支持するとともに、大阪サミット首脳宣言を受けて金融安定理事会(FSB)および金融活動作業部会(FATF)から提出された、グローバル・ステーブルコインに関する報告を歓迎する。
2. 我々は、2020年におけるFSBおよびFATFの更なる報告を期待する。我々はまた、IMFに対し、現在行っている作業に立脚して、加盟国の通貨主権に係る問題を含むマクロ経済上のインプリケーションについて、各国の特徴を考慮しつつ、検討することを要請する。
3. 我々は、金融技術革新による潜在的な便益を認識しつつも、グローバル・ステーブルコイン及びその他のシステム上大きな影響を与えうる類似の取組が政策及び規制上の一連の深刻なリスクを生じさせることになるということに同意する。そのようなリスクは、特に、マネーロンダリング、不正な金融、消費者・投資家保護に関するものを含め、こうしたプロジェクトのサービス開始前に吟味され、適切に対処される必要がある。

2019年10月23日 FacebookのザッカーバーグCEOが 米国議会公聴会に出席



(米国議会のLivestreamより)

5. 中銀デジタル通貨(CBDC)



中国によるデジタル人民元構想の発表

中国、デジタル通貨発行か 人民銀行、「世界初」の可能性

【北京共同】中国政府系シンクタンク、中国国際経済交流センターの黄奇帆副理事長（元重慶市長）は28日の講演で、中国人民銀行（中央銀行）が「世界で初めてデジタル通貨を発行する中央銀行になる可能性がある」と述べた。中国メディアが伝えた。

デジタル通貨には、暗号資産（仮想通貨）の基盤技術「ブロックチェーン」を活用する。国際金融の仕組みも今後、本格的なデジタル化の時代を迎える。中国がデジタル通貨で先行すれば、欧米主体の体制に波紋を投げ掛けそうだ。

ニュースサイト新浪網によると、黄氏は「（人民銀行は）すでに5～6年の研究を重ね、技術は成熟している」と話した。（2019/10/28）

CCIEE Vice Chairman Says PBOC Will Be First to Roll Out Digital Currency

INDUSTRY David Lee October 28, 2019



中国国際経済交流センター黄奇帆氏の発言要旨

ビッグデータ、クラウドシステム、人口知能やブロックチェーン技術、これらの最新技術は相互作用しながら社会を構築しており、ブロックチェーン技術は情報伝達や堅牢性、柔軟性など技術の基本レベルを大幅に向上させる。

現在でも、AlipayとWeChatPayは世界をリードするデジタル支払い手段だが、ブロックチェーン技術の浸透により国境を超えた個人間の送金技術も進化している。これまでの国際送金は多くの中継点が必要で非効率だったが、ブロックチェーン技術は決済や商業銀行のインターフェイスとして利用できる。国境を超えた送金は処理効率の向上が実現する。

70年代から運用されている国際金融ネットワークのSWIFTやCHIPSシステムは、世界の銀行を結びつける大きな役割を果たしたが、現在は時代遅れになりつつある。またこれらのネットワークは米国が世界的に覇権を行使するツールになっている。SWIFTおよびCHIPSシステムに将来性はなく、ビッグデータとブロックチェーン技術を使った新たな国際決済ネットワークの構築は、各国の共通認識となっている。80年代からお金のデジタル化が発展しクレジットカードや携帯電話での決済などが発展してきたが、今日ではビットコインやフェイスブックのリブラ、そして中央銀行が発行するデジタル通貨の時代が到来している。

米ドルは70年代から強力な軍事力と経済力で事実上の世界通貨となっているが、世界の中央銀行の総資産は70年代の1,000億ドルから21兆ドルに膨らんでいる。特に米国はここ10年で金融危機を乗り越えるため、債務残高が9兆米ドルから22兆米ドルに増えており、もし信用を失えば新たな世界的な金融危機は避けられない。また、こういった問題に直面しているにも関わらず、各国にていい解決方法を見出せていない。一部の専門家は金本位制への回帰を唱えるがこれも現実的ではないだろう。

ビットコインや、一部の企業はリブラを発行してソブリン通貨に挑戦しようとしているが、これらは国家の信用からは切り離されており、発行が保証されず安定化することは困難だ。リブラが成功するとは思えない。

主権国家にとっての最良の方法は、政府と中央銀行が主権デジタル通貨を発行することだ。

中国の中央銀行が立ち上げるデジタル通貨(DCEP)は、ブロックチェーン技術に基づいた新しい暗号化電子マネーシステム。2層のオペレーティングシステムを採用しており、まず銀行への発行、そして一般国民へ流通が想定されている。重要な点は既存の通貨のデジタル化ではないことで、これにより人民元の流通と国際化が促進される。

中国人民銀行は5年、6年の間DCEPを研究しており、成熟している。中国人民銀行はデジタル通貨を導入する世界初の中央銀行となる可能性がある。5G時代はすべてのものがインターネットにつながり、特に金融技術の発展は重要となる。新しい金融システムは経済と社会全体の発展をもたらす。(FINTIDE、2019年10月29日)

マーシャル諸島共和国の中央銀行デジタル通貨計画 “SOVEREIGN” の事例



SOV

[What is Money](#)

[Protocol](#)

[RMI](#)

[Media](#)

[Read the Law](#)

money that is digital

On February 26, 2018 the Republic of the Marshall Islands issued the [Sovereign Currency Act of 2018](#) introducing a new blockchain based currency called the Sovereign ("SOV") as "legal tender of the Marshall Islands for all debts, public charges, taxes and dues."

Declaration and Issuance of the Sovereign Currency Act 2018

BILL No: 125ND2 P.L. 2018-⁵³
Index

NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS
39TH CONSTITUTIONAL REGULAR SESSION, 2018



Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

DECLARATION AND ISSUANCE OF THE SOVEREIGN
CURRENCY ACT 2018

2018年、IMFは SOV発行の再考 を提言



INTERNATIONAL MONETARY FUND

REPUBLIC OF THE MARSHALL ISLANDS

STAFF REPORT FOR THE 2018 ARTICLE IV CONSULTATION

August 10, 2018

11. Considering the significant risks, staff recommends that the authorities seriously reconsider the issuance of the digital currency as legal tender. The potential benefits from revenue gains appear considerably smaller than the potential costs arising from economic, reputational, AML/CFT, and governance risks. While technology may help to address some of these risks, others would need to be mitigated through institutional changes. Furthermore, the use of the SOV as a means of exchange in transactions would require significant additional costs to upgrade the RMI's telecommunication infrastructure.

² The SOV is not equivalent to a central bank digital currency, which is a digital form of the central bank's liability (cash and reserves) because RMI uses the U.S. dollar as a legal tender and the SOV's exchange rates would be determined on global cryptocurrency exchanges.

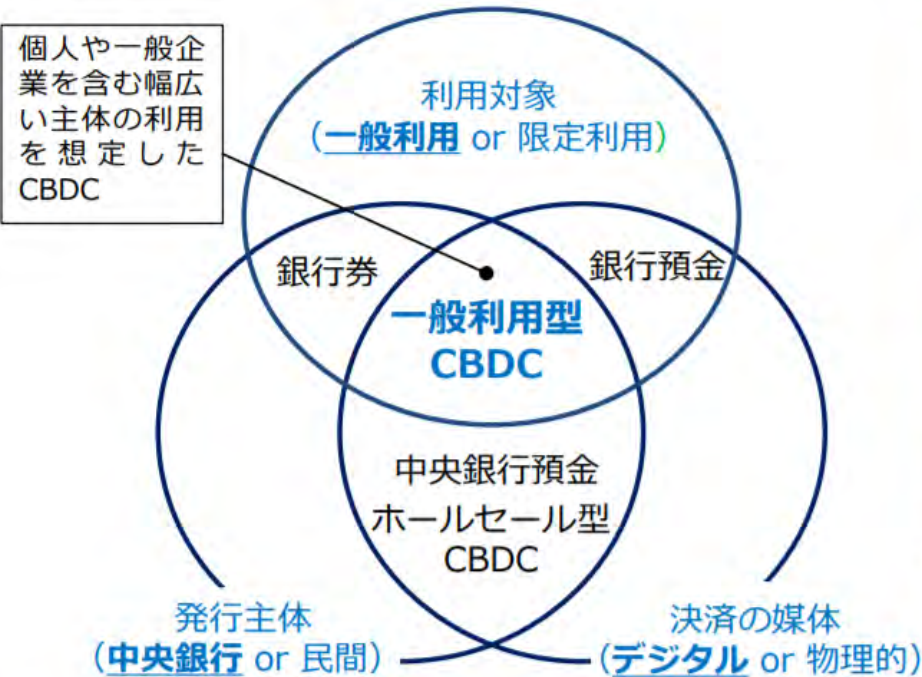
³ For example, if the SOV was issued at the price of about \$50 as targeted at the Initial Coin Offering and distributed to resident RMI citizens as planned, it would be equivalent to a transfer to households of about 11 percent of GDP per year over the next five years.

日銀はCBDCについてのレポートを発表

中央銀行デジタル通貨とは

- 「中央銀行デジタル通貨」(Central Bank Digital Currency : **CBDC**) とは、既存の中央銀行預金とは異なる、新たな形態の電子的な中央銀行マネー。
- 現時点でCBDCを発行する計画はないが、今後の様々な環境変化に的確に対応できるよう、しっかり準備しておくことが重要。

通貨の分類



一般利用型CBDCに期待される機能と役割

1. 現金と並ぶ決済手段の導入
 2. 民間決済サービスのサポート
 3. デジタル社会にふさわしい決済システムの構築
- 現金に対する需要がある限り、現金の供給についても責任をもって続けていく。

日銀はCBDCについてのレポートを発表

今後の取り組み

- 今後は、これまでのようなリサーチ中心の検討にとどまらず、**実証実験**の実施を通じて、より具体的・実務的な検討を行っていく。
- 実証実験と並行して、CBDCの発行に関して考慮すべきポイントなどを踏まえ、**制度設計面の検討**を深めていく。内外関係者との連携も重要。

実証実験の流れ

概念実証
フェーズ1

システムのな実験環境を構築し、CBDCの基本機能（発行、流通、還収）に関する検証を行う。
→2021年度の早い時期の開始を目指す。

概念実証
フェーズ2

フェーズ1で構築した実験環境にCBDCの周辺機能を付加して、その実現可能性などを検証する。

パイロット
実験

概念実証を経て、さらに必要と判断されれば、民間事業者や消費者が実地に参加する形でのパイロット実験を行うことも視野に入れて検討。

考慮すべきポイント



物価の安定や金融システムの安定との関係



イノベーションの促進



プライバシーの確保と利用者情報の取扱い



クロスボーダー決済との関係

当面の情報技術に基づくCBDCの課題

そもそもホールセールCBDCは、既存のRTGSシステムなどと同じ役割となるので、銀行間決済システムの技術的な更新に過ぎない。しかし、もし先進国がリテールCBDCを発行したら、

1. 民間銀行の預金業務との競合。民業圧迫。誰が信用創造するか。
2. 全国民に中央銀行当座預金口座を与えて、リアルタイムで取引するのと同じ。中央銀行システムが大きなシステムリスクを背負い込む。
3. 金融危機発生時には一斉にCBDCへのbank run（とりつけ）が起きる。
4. 国際的な利用を可能にする場合、AML / CFTにどう対処するか。
5. 個人の消費行動の取引履歴が全て中央銀行に集まってしまう。
中央銀行はそれを活用できない。
民間による情報活用を妨げる。
中央銀行による国民のプライバシー侵害のリスク。