Goldman Sachs | Global Macro Research

ISSUE 98| 2021年05月21日 午後6.00PM EDT

TOP of MIND

暗号資産：新たな資産クラスとなるのか？

信用度の高い投資家からの関心が高まり、従来型の金融機関ー当社含むーが新たな暗号商品やサービスを開始するなかでも暗号通貨価格の極端な変動が続いており、暗号資産は間違いなく「最大の関心事(Top of Mind)」となっている。最近の乱高下のなか、暗号資産は制度化された資産クラスとみなしうるのか、またみなすべきなのかをギャラクシーのマイケル・ノボグラーツ氏(イエス；暗号通貨に関わる信用度の高い投資家の数がクリティカルマスに達した事実だけでもそれは確固たるものとなった)、NYUのヌリエル・ルービニ氏(ノー；暗号通貨にはインカムや実用性、経済のファンダメンタルズとの関連性が全くない)、グレイスケールのマイケル・ソネンシャイン氏(イエス；2020年の力強い反発は投資家に資産クラスとしての弾力性を改めて保証した)、当社マシュー・マクダーモット(「イエス」と答える投資家が増えている)などの専門家に尋ねた。また、当社リサーチ・アナリストもこの議論に参加している。続いて、アラン・コーエン元SEC顧問やトレイル・オブ・ビッツのダン・グイド氏、チェインアリシスのマイケル・グロネガー氏とともに機関投資家による採用が一段と進む上での規制や技術、セキュリティ面での障害を探る。

「[暗号資産に]関与する機関がクリティカルマスに達した。大手行からPayPal、Squareに至るあらゆる機関が関与を深めており、これは暗号資産が今や正式な資産クラスとなったことを明確に示している。」

マイケル・ノボグラーツ

「ビットコインその他の暗号通貨は資産ではない。資産にはファンダメンタルな価値を判断するのに使用可能な多少のキャッシュフローまたは実用性がある…ビットコインや他の暗号通貨にはインカムも実用性もない。」

ヌリエル・ルービニ

「暗号資産に関する研究で、その資産クラスとしての可能性に心から驚嘆していないものはまだみたことがない。」

マイケル・ソネンシャイン

目次

アリソン・ネーザン | allison.nathan@gs.com　ガブリエル・リプトン・ガルブレイス | gabe.liptongalbraith@gs.com　ジェニー・グリムバーグ | jenny.grimberg@gs.com

暗号資産：新たな資産クラスとなるのか？

暗号資産への信用度の高い投資家からの関心が高まり、従来型の金融機関－当社含む－が新たな暗号商品を市場投入するなかでも、規制による取り締まりや環境上の懸念、課税強化のニュースを受けて暗号通貨価格の極端な変動が続いており、暗号資産は間違いなく「最大の関心事(Top of Mind)」となっている。当社が初めてビットコインに関するリサーチを作成したのは2014年で、2018年には暗号資産全般について調査を行い、暗号エコシステムの可能性とリスクを探った。最近の乱高下のなか、今回は暗号資産を制度化された資産クラスとみなしうるのかに重点を置く。

まず、ギャラクシー・デジタル・ホールディングスの共同創立者であるマイケル・ノボグラーツCEOの話を聴く。同社は暗号資産の投資や取引、資産運用、ベンチャー・ファイナンスに携わっている。氏は暗号資産に関与している信用度の高い投資家や金融機関の数がクリティカルマスに達した事実だけでも、正式な資産クラスとしての暗号資産の地位を確固たるものにしたと考えている。また、価格の乱高下にもかかわらず、現在の－FRBが主に資金を供給している社会問題への支出を停止する必要性を政府が感じていない－マクロ環境や政治情勢が続く限り、ノボグラーツ氏が価値保存の便利な手段とみなすビットコインへの機関投資家の関心が薄れる様子はなく、暗号資産の採用は続くと考えている。

世界最大のデジタル資産運用会社、グレイスケール・インベストメントのマイケル・ソネンシャインCEOも同様に、機関投資家はデジタル資産が普及するであろうことを今では概ね正しく認識しており、インフレや通貨下落へのヘッジ手段として、またはリスク調整後リターンの向上を追求するなかでのポートフォリオ多様化手段として、ビットコインのような－非常に希少であることが検証可能な－資産の有限性にますます魅力を感じていると考えている。暗号資産の過去1年間の値動きは多様化手段とは程遠かった–新型コロナウイルスのパンデミックが始まって以来、伝統的な資産以上に下落した–が、ソネンシャイン氏は2020年の急速かつ力強い反発は資産クラスとしての弾力性を投資家に改めて保証するのみであったと述べている。

しかし、ビットコインのような–インカムも実用性もなく、ボラティリティの高い–暗号資産を妥当な価値保存手段としているのは何なのだろうか。ノボグラーツ氏の答えは、そうであると「信じるのを世界が認めた」こと。ザック・パンドル(当社グローバル為替、金利、新興国投資戦略共同統括)もほぼ同意見で、安全性やプライバシー、譲渡性といった性質に加え高いブランド力、またデジタルである事実からビットコインは将来の世代に適した価値保存手段となっており、社会で幅広く採用される可能性があると述べている。また、パンドルは現代の機関投資家はビットコインを金のようなマクロ資産として扱うべきであると考えている。

当社コモディティ・アナリストのミハイル・スプロギスとコモディティ調査チームのグローバル統括ジェフ・カリーは暗号資産は価値保存手段として機能しうるが、それも価値の創出と価格のボラティリティ緩和につながるような現実世界の用途を持つ場合に限られると述べている。この理由から、二人はブロックチェーンがそうした用途の可能性を最大限に高めているイーサ(Ether)のような暗号資産がデジタルの主要な価値保存手段となるのに有利な立場にあると述べている。より広範には、暗号資産は正当性が立証されつつある情報およびネットワークの規模や成長から価値を引き出す新しい資産クラスだが、分散型という性質や匿名性から将来の成長には法的課題が大きく立ちはだかっているとカリーは主張している。

また、ニューヨーク大学スターン経営大学院のヌリエル・ルービニ経済学教授は、インカムも実用性も経済のファンダメンタルズとの関連性もない何かを価値保存手段、あるいはそもそも資産とみなせるという考えに真っ向から異議を唱えている。暗号資産を巡る最近の熱狂にもかかわらず、同教授は暗号資産のボラティリティやリスクを引き受けようとする大半の金融機関の意志を疑問視しており、最近の激しい価格変動はそのリスクをはっきりと思い出させる結果になったと考えている。

続いて、当社シニア・マルチアセット・ストラテジストのクリスチャン・ミュラーグリスマンが、ポートフォリオに価値を付加するには暗号資産は魅力的なリスク/リワード、または他のマクロ資産との低相関、できればその両方を兼ね備えていることが望ましいとの考えを示す。標準的な米国の60/40ポートフォリオに2014年以降、ビットコインをわずかに組み入れると、S&P 500や米国10年債よりも高いビットコインのリスク調整後リターンと、他の資産との相対的に低い相関がもたらす多様化効果の両方により、強力なアウトパフォーマンスにつながることがわかった。だが、このアウトパフォーマンスの大半はごく限られたビットコイン独自の上昇に起因するため、ビットコインの短く、変動の激しい取引実績では、それがバランスト・ポートフォリオにどれだけの価値を付加できるか判断するのは早計であるとの結論に至った。

しかし、価値保存手段や投資可能な資産としての議論の余地の残る役割以外に、広範な暗号エコシステムは投資家に価値の上昇を約束してくれるのだろうか。暗号資産に無数の潜在的用途があることを踏まえ、ノボグラーツ氏とソネンシャイン氏はその答えがイエスであると強く信じている。特にノボグラーツ氏は暗号エコシステムの3大進化–決済、分散型金融(DeFi)、非代替性トークン(NFTs)–が主にイーサリアム(Ethereum)ネットワーク上に構築されつつあり、これはイーサリアムやDeFiの様々なアプリケーションに多大な価格上昇余地があることを示唆していると考えている。しかし、ルービニ氏はブロックチェーン・テクノロジーのアプリケーションにほとんど成功例はないと主張する。さらに、企業がブロックチェーンを“BINO”－Blockchain In Name Only(名ばかりのブロックチェーン)として利用する可能性は大きいとみている。要するに、ルービニ氏は「テクノロジーが信用の問題を解決できるという考えは妄想である」という理由で、ブロックチェーン・テクノロジーが革命的と証明されることに懐疑的である。

次に、当社デジタル資産グローバル統括のマシュー・マクダーモットが、当社が暗号資産に(再び)関わるようになった理由–顧客の需要－と、暗号資産への関心が顧客の種類－ポートフォリオの多様化を求めるアセット・マネジャーから暗号資産の幅

広い使用例へのエクスポージャーをますます追及するようになった富裕層の顧客、主に現物のロングと先物のショートのベーシスの差ー今も残る市場へのアクセスの難しさを反映したアービトラージーから利益を得ることを目指すヘッジファンドーでどのように異なるかを説明する。

最後に、この市場の分断問題以外に、機関投資家による暗号資産の採用拡大の妨げとなる他の要因を考える。規制当局が現在、暗号資産をどのように考えているかをジェイ・クレイトン前 SEC 委員長の元上級政策顧問で当社コンプライアンス部門のグローバル統括でもあったアラン・コーエン氏が説明する。ブロックチェーン調査会社チェインアリシスの共同創立者で CEO のマイケル・グロネガー氏は、暗号通貨の違法取引が全体の 1%に満たないことを発見した同社の分析に何が含まれているかーそして何が含まれていないかーを説明する。ソフトウエア・セキュリティ会社トレイル・オブ・ビッツの共同創立者ダン・グイド CEO は、暗号エコシステムの全投資家が知っておくべきテクノロジーやセキュリティ上のブラックスワン・シナリオを論じる。

アリソン・ネーザン、編集者

Email: allison.nathan@gs.com
Tel: 212-357-7504
Goldman Sachs and Co. LLC

Interview with Michael Novogratz

Michael Novogratz is CEO of Galaxy Digital Holdings Ltd. Below, he discusses the potential for crypto assets and their ability to transform the financial system and beyond.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: How does Galaxy invest in the crypto universe?

Michael Novogratz: Galaxy Digital grew out of my family office, which operates like a merchant bank, and has become a nearly full-service business for the digital asset and blockchain technology communities. Being involved across the ecosystem is important to us, namely so that we can be positioned to help grow the industry that we believe will transform the way we live and work globally. We own and trade coins, have a large venture business, and invest in the virtual world that will be used not by finance, but by consumers—the metaverse, gaming studios, and non-fungible token (NFT) projects. We believe you learn by being at the frontier and that's why we started the company—to learn about the crypto space and share that knowledge with our institutional customers as we create the next generation of financial services companies.

Allison Nathan: You've been involved in and excited about the crypto space for a while now, but it's had fits and starts, including the dramatic price rise and collapse in 2017/18. What makes this time different?

Michael Novogratz: 2017/2018 was the first-ever truly global and retail-driven speculative mania. It was blind excitement. It's not that there are no excesses, knuckleheaded Twitter comments, cheerleading, or tribalism today, but that's all there was back then. And crypto's market cap cratered 98.5%. But out of that mania grew a much smarter investor base that took the lessons learned and is more willing to differentiate between the different use cases for crypto—from stores of value to decentralized finance (DeFi) to stablecoins and payment systems. And in turn, the community has built up a more logical investment process.

Importantly, that price downturn didn't result in a downturn in investments being made in the underlying crypto infrastructure, so the custody and security infrastructure necessary to attract institutions has been built. As a result, we've now hit a critical mass of institutional engagement. Everyone from the major banks to PayPal and Square is getting more involved, which is a loud and clear signal that crypto is now an official asset class. There's still a lot of volatility, so people will wash in and out. But crypto is not going away. And a core group of crypto people see this as—and I quote the Blues Brothers here —"a mission from god". They want to rebuild the infrastructure of the financial markets in a way that's more transparent and egalitarian and doesn't rely on governments who make bad decisions with our finances. They will never sell. And because of that, bitcoin and ether can't go to zero.

Allison Nathan: But can the crypto ecosystem survive if it isn't intertwined with the traditional financial system?

Michael Novogratz: No. Institutions need to participate because they have most of the money in the world and there's actually a symbiotic relationship between the two. The advisor model that Galaxy possesses is important because many people don't have time to learn to become investors. And as traditional financial advisors and asset managers understand the space and become crypto preachers, they bring more people into the tent, which is key for the future of crypto.

That said, payments will be an interesting battleground. The money transfer business is a very high margin one for legacy financial institutions and it's under threat from new payment systems that are faster, more transparent, and cheaper. Facebook is coming out with their Dollar-based payment system, the Chinese government is coming out with theirs, and stablecoins are gaining traction. At some point, I believe our phones will have crypto wallets that will replace bank accounts. The competition to see who dominates payments is just starting along with the competition between exchanges and derivative markets. So the question is, how fast will banks iterate and compete?

"A core group of crypto people see this as—and I quote the Blues Brothers here —"a mission from god"… They will never sell. And because of that, bitcoin and ether can't go to zero."

Allison Nathan: But will it be bitcoin that's transformative in payments?

Michael Novogratz: No. Bitcoin isn't set up to process thousands of transactions per second. Paying for a diet coke with bitcoin would be like paying for it with gold. That won't happen. But payment rails will be built on other blockchains. Right now, if I want to send money to my sister in Holland, it would be painful, costly, and slow. But soon, I'll be able to send her a Dollar stablecoin and transferring money will become free. Most of this will be built on the Ethereum network, which is why ethereum prices have been rising. The three biggest moves in the crypto ecosystem—payments, DeFi, and NFTs—are mostly being built on Ethereum, so it's going to get priced like a network. The more people that use it and the more stuff that gets built on it, the higher the price will ultimately go.

Allison Nathan: What's the value proposition of bitcoin, then?

Michael Novogratz: Bitcoin is a really convenient way to store value. One of the main reasons people have gotten excited about bitcoin recently is that they're worried that we currently have an unsustainable balance of monetary and fiscal policy

that will eventually set off an inflationary spiral. And that worry isn't going away anytime soon. More and more Americans are in favor of paying for college for people whose families earn less than $100k annually. President Biden just gave half of the $1.9tn fiscal package directly to people who needed it, which was very well-received. Some version of universal basic income (UBI) is coming; it may not be called UBI, but capital will be taxed and given to labor. None of that is fiscally prudent, but there's no political imperative to say stop spending money. Even before COVID-19, deficits were bad, but now they're insane. And monetary policymakers are financing everything the government wants to spend, not just in the US but all over the world. So the main reason everyone got into bitcoin is the same reason they got into gold—the current macro backdrop is tailor-made for it. And, as long as that macro and political backdrop persists and crypto remains in the adoption cycle, it's crazy to get out.

> "The three biggest moves in the crypto ecosystem—payments, DeFi, and NFTs—are mostly being built on Ethereum, so it's going to get priced like a network. The more people that use it, the more stuff that gets built on it, and the higher the price will ultimately go."

Allison Nathan: But why is bitcoin, which has no income and no other uses, a good store of value?

Michael Novogratz: Bitcoin is one of the few uniform stores of value in the world. It's the most widely distributed asset in history outside of the Dollar and Euro; 140 million people own some bitcoin. And it's easily stored and transported, unlike gold. Stores of value are social constructs—they have value because we believe they do. There has never been a more successful brand created in such a short period of time. It's like they floated the baby in the river and the community raised the baby, and now it's worth around $1tn. Today, it's recognized and believed in by exceptionally credible people. So the world has voted that they believe bitcoin is a store of value. People still make stubborn arguments against it, but every single bank we know of is building a wealth channel for crypto, 14 entities have bitcoin ETFs in line at the SEC, and most tech companies are building bitcoin into their wallet and interface. To think we're going to have less people believing in bitcoin isn't logical.

Allison Nathan: Haven't people been buying bitcoin and other cryptos just because their prices were rising?

Michael Novogratz: Of course that's part of the equation. People in general are momentum investors. All great fortunes on this planet have been made by trends—I learned that from Paul Tudor Jones thirty years ago and Jeff Bezos and Bill Gates are proof points to this as well. Bitcoin adoption and the macro factors behind it are a mega bull trend.

Allison Nathan: So what are the remaining roadblocks to further institutional adoption?

Michael Novogratz: Institutions need a little more regulatory clarity, which they'll likely get soon. Former SEC Chair Jay Clayton didn't want crypto to be his legacy, and so he punted. But Gary Gensler is very knowledgeable about and interested in the crypto space. Within his first nine months, a clear regulatory framework will likely emerge that will make it easier for institutions to get involved. For example, institutions have a hard time using DeFi products right now due to uncertainty around how Know Your Customer (KYC) requirements are applied to smart contracts and DeFi companies that are comprised of code. With a little more innovation and regulator understanding over the next few years, DeFi protocols and projects will probably explode. Uniswap could become a bigger exchange than the CME or the NYSE which will pull people in. More clarity on the tax side would also be helpful. But policymakers today are rational and have high intellectual integrity, so I don't see them singling out cryptocurrencies and do expect they will be taxed like any other asset. I'm much more confident than I've ever been that this is inevitable.

Allison Nathan: What do you make about the rise of Dogecoin and other meme coins?

Michael Novogratz: Dogecoin is a very speculative asset, much more so than bitcoin. It likely doesn't have long-term legs because no institution is buying it and at some point, retail will lose interest. Dogecoin started as a joke and grew for two reasons. First and foremost is tribalism in the investing community. It's the same thing we saw with the rise in GameStop, which was driven by a young community of investors who have been empowered as financial players through trading apps and social media platforms. Second, value is showing up in new places because the government is printing a lot of money. It's important to keep that in mind when thinking about some crypto assets and equities like GameStop that have short-term potential but no long-term viability.

> "People in general are momentum investors. All great fortunes on this planet have been made by trends… Bitcoin adoption and the macro factors behind it are a mega bull trend."

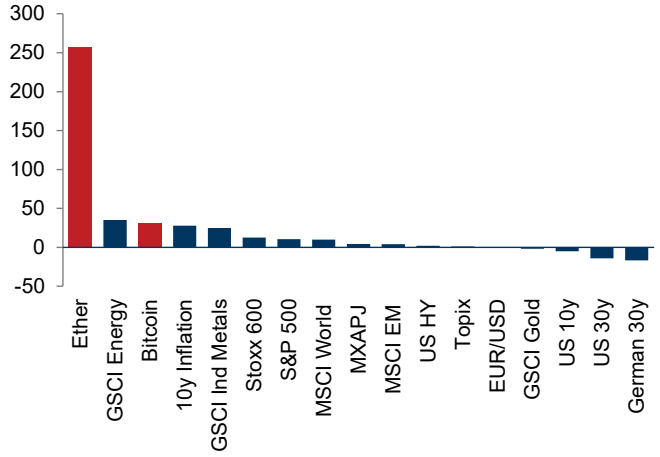
Allison Nathan: What would make enthusiasm for the asset class diminish?

Michael Novogratz: I am not sure what could dent enthusiasm for the broader ecosystem at this point. But, at least for bitcoin, the biggest risk in this cycle is, in the words of Ray Dalio, a beautiful de-leveraging. If the Fed successfully taps the brakes, pulls back liquidity, and slows the economy down just enough to ensure inflation doesn't run away and deficits come down, then the impetus for having a store of value will fall. But this is the hardest macro environment policymakers have ever dealt with, and only a tiny window exists to get it right. And even if they do, bitcoin won't just collapse into oblivion. Why has gold been a mediocre asset to own this year and bitcoin's generally been a great one? Because gold isn't in the adoption cycle. Bitcoin is.

Cryptos: sizing the surge

Bitcoin and ether have performed strongly YTD

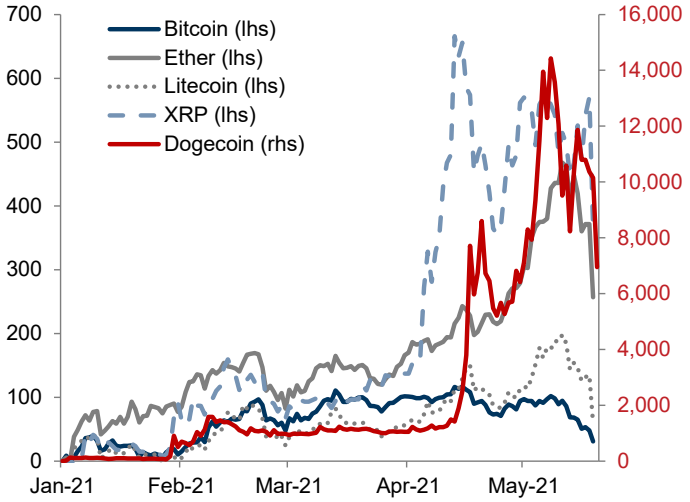
Total returns YTD, %



Note: Total returns in USD; all market prices as of May 19, 2021.
Source: Bloomberg, Goldman Sachs GIR.

And other cryptocurrencies have seen even larger rallies

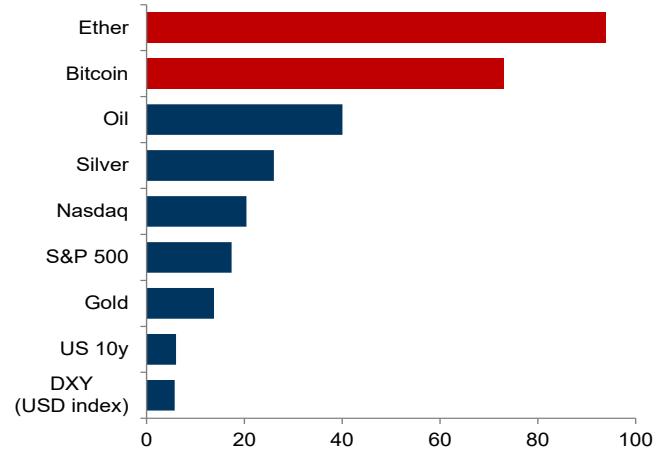
Total returns YTD, %



Note: Total returns in USD.
Source: Bloomberg, Goldman Sachs GIR.

But crypto returns remain very volatile

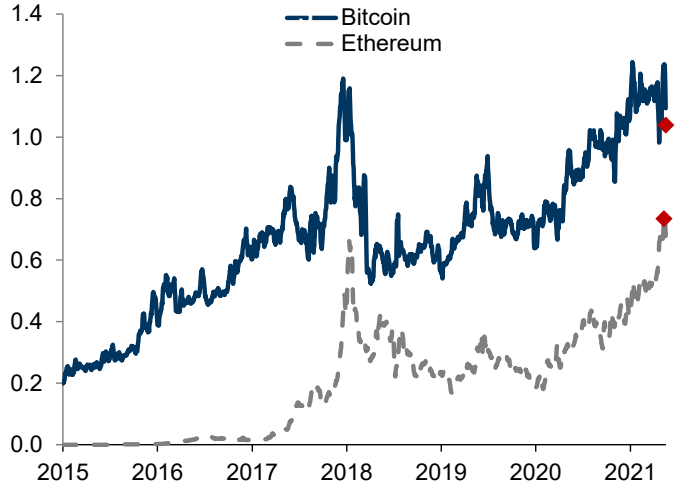
Average daily volatility in ann. terms, %



Note: Based on returns since 2014 and since 2015 for ether.
Source: Bloomberg, Goldman Sachs GIR.

Activity on Bitcoin and Ethereum networks is around 2018 highs

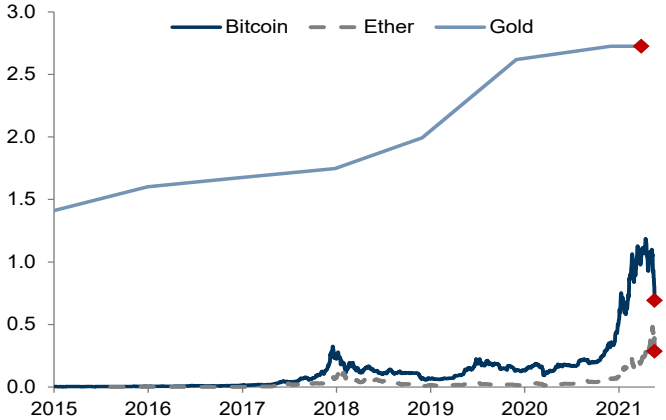
Total active addresses, million



Note: Includes unique addresses active in the network as a sender or receiver.
Source: Glassnode, Goldman Sachs GIR.

The market cap of bitcoin had surged above $1tn

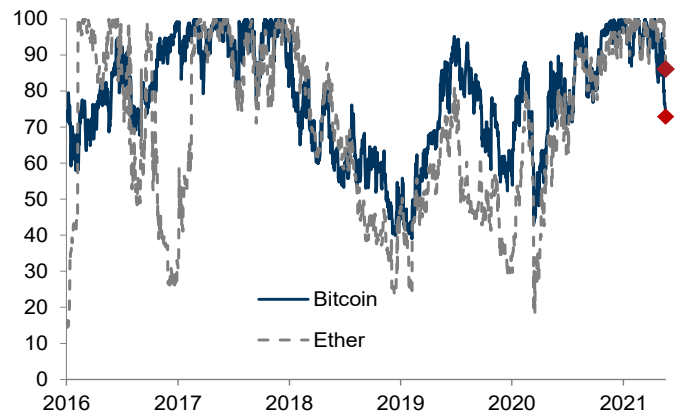
Crypto market cap. vs private investment gold stock, $tn



Note: Private investment gold stock based on ETFs and bars/coins held privately.
Source: World Gold Council, CoinMarketCap, Goldman Sachs GIR.

Around 70% of bitcoin and 85% of ether is held in profit today

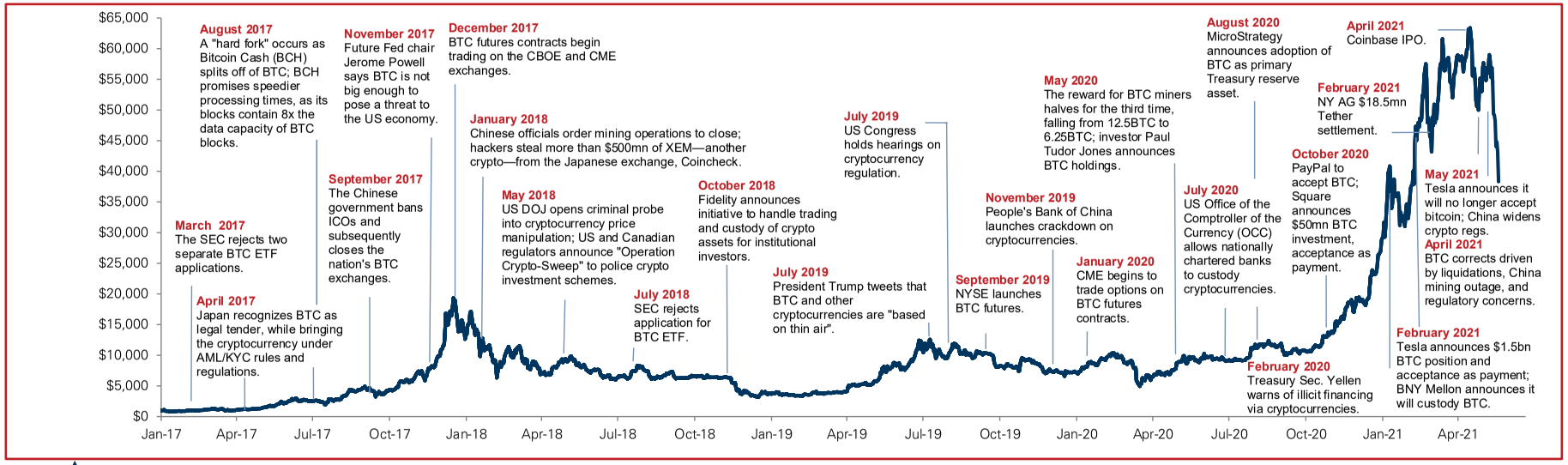
Percent of total supply in the network with positive balance, %



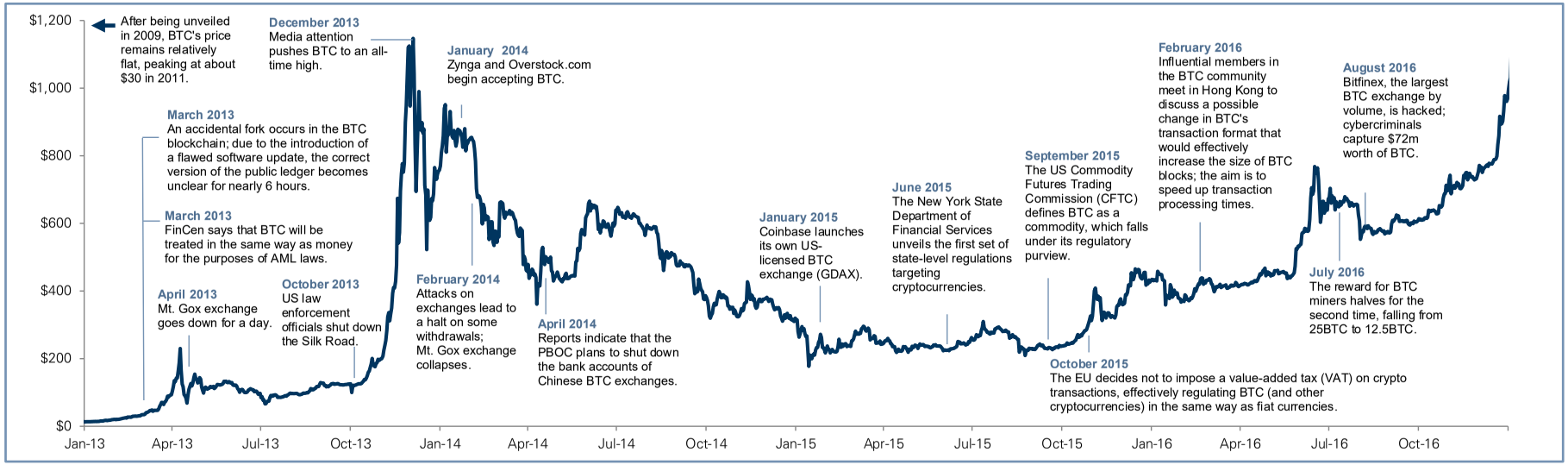
Note: The percentage of circulating supply bought below the current market price. See more detail here; as of May 19. 2021.
Source: Glassnode, Goldman Sachs GIR.

Tracking bitcoin's volatile ride

2017-2021



2013-2016



Note: Market pricing as of May 19, 2021.
Source: CoinDesk, 99bitcoins, Bloomberg, various news sources, Goldman Sachs GIR.

Interview with Nouriel Roubini

Nouriel Roubini is a professor of economics at New York University's Stern School of Business. He is CEO of Roubini Macro Associates, LLC, a global macroeconomic consultancy firm. Below, he discusses his skepticism about the value of cryptocurrencies and their ability to radically transform the financial system.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: Why do you think bitcoin and other cryptocurrencies are in a bubble?

Nouriel Roubini: To start, calling them currencies is a misnomer. Currencies must have four qualities: they must be a unit of account, a means of payment, a stable store of value, and act as a single numeraire. Bitcoin and most other cryptocurrencies have none of these features. It's not a unit of account; nothing is priced in bitcoin. It's not a scalable means of payment; the Bitcoin network can only complete seven transactions per second, versus the Visa network that can conduct 65,000. It's not a stable store of value for goods and services; even the crypto conferences I've attended don't accept bitcoin for payment because the price volatility could wipe out their profit margin overnight. And the crypto universe doesn't offer a single numeraire in which the prices of different items can be denominated because there are thousands of tokens and thus limited price transparency. Even the Flintstones had a more sophisticated system by using shells as a single numeraire to compare the price of different goods.

Bitcoin and other cryptocurrencies also aren't assets. Assets have some cash flow or utility that can be used to determine their fundamental value. A stock provides dividends that can be discounted to arrive at a valuation. Bonds provide a coupon, loans provide interest, and real estate provides rent or housing services. Commodities like oil and copper can be used directly in different ways. And gold is used in industry, jewelry, and has historically been a stable store of value against a variety of tail risks, including inflation, currency debasement, financial crisis, and political and geopolitical risk. Bitcoin and other cryptocurrencies have no income or utility, so there's just no way to arrive at a fundamental value. A bubble occurs when the price of something is way above its fundamental value. But we can't even determine the fundamental value of these cryptocurrencies, and yet their prices have run up dramatically. In that sense, this looks like a bubble to me.

Allison Nathan: Why are more institutions interested in getting involved in cryptocurrencies if they are in a bubble, and will this help stabilize and credentialize the market?

Nouriel Roubini: Given the large trading volumes, it pays to facilitate trading activity, custodial services, etc. But do institutional investors really want to get more involved? Maybe some do, but I don't see it becoming mainstream. There's an argument that because only a fraction of institutional money is currently invested in bitcoin relative to gold, the price of bitcoin could go to the moon as a result of asset re-allocation from gold. But I'm doubtful institutions want exposure to an asset that can drop by 15% overnight. There's also always the risk that something else backed by real assets might end up completely replacing bitcoin as an alternative store of value. Bitcoin could disappear one day, but gold won't. And the idea of corporate treasurers allocating to crypto assets is totally crazy. No serious company would do that because treasury accounts must be invested in stable assets with minimal risk, even if they provide a very low return. Any treasurer who invests in something that falls 15% in value overnight will be fired. Sure, Elon Musk can do it because he's the boss, although he's since backtracked somewhat on bitcoin due to environmental concerns. But few other people are in that position.

Allison Nathan: But didn't gold also have highly volatile periods before it matured as an institutional asset?

Nouriel Roubini: While gold has experienced periods of volatility, a set of economic fundamentals generally drove those price swings. Gold rises with inflation and inflation expectations because it's an inflation hedge, and it falls when the Fed tightens monetary policy and rates rise, not just in nominal but also in real terms, for the same reason. Gold is inversely related to the value of the Dollar, because a falling Dollar leads to higher commodity production costs and prices, including for gold. When there's serious political or geopolitical risk or a financial crisis, the value of gold rises because it serves as a safe haven asset, as does the Swiss Franc, the Japanese Yen and US Treasuries. A whole set of variables can be used to determine the demand for gold relative to its supply, which makes it possible to establish a fundamental price. In contrast, the prices of bitcoin and other cryptos don't have a consistent relationship with economic fundamentals that explains their volatility or suggests it will eventually subside.

Allison Nathan: But couldn't bitcoin serve as an inflation hedge similar to gold given that it doesn't have exposure to currency debasement?

Nouriel Roubini: It's true that inflation and inflation expectations have moved higher, the Dollar has started to weaken, and US breakevens are now well above 2%. But while the price of gold and other inflation hedges has reflected these shifts to a limited extent, at their peak, bitcoin's price had increased by more than tenfold from a low of $5K to more than $60K in a year. That can't be explained by a fear of currency debasement, because if there was really such a strong worry, gold and other assets like TIPS would likely have rallied more. So, something else must account for the rise in bitcoin and other crypto prices.

Does bitcoin offer protection against debasement? At least among the cryptos, it can't be debased because a cryptographic rule determines the increase in supply and caps total supply at 21mn. But just because something is scarce doesn't mean it has fundamental value. It's not difficult to create something with limited supply, and there's no reason artificial scarcity is

valuable in and of itself. Beyond bitcoin, the supply of most cryptocurrencies is determined by a bunch of whales and insiders based on random rules that can be used to increase supply ad-hoc. And their supply has actually increased at a much faster rate than the balance sheet of any central bank given the proliferation of the number of coins. Scarcity also doesn't make something a reliable store of value. It took a hundred years for the value of the Dollar to fall by 90% in real terms. In 2018, it only took 12 months for thousands of cryptocurrencies to lose the same amount of value, and even bitcoin fell by more than 80%. That's currency debasement.

Bitcoin isn't even a reliable hedge for risk-off events, let alone inflation shocks. It's actually highly pro-cyclical. During the peak of the COVID-19 shock in early 2020, US equities fell by about 35%, but bitcoin collapsed by around 50%. Other top 10 crypto currencies fell by even more. In difficult times, crypto assets don't go up; they go down. If investors want inflation hedges, a wide variety of assets have proven to be good inflation hedges for decades, including commodities and their stocks, gold, TIPS, inflation-adjusted and other forms of inflation-indexed bonds. I do worry that monetized deficits might eventually lead to fiscal dominance and higher inflation. But I wouldn't recommend bitcoin or other cryptocurrencies to protect against this risk.

Allison Nathan: Nascent technologies are often volatile in their adoption phase. What makes this moment for crypto any different than the early days of the internet?

Nouriel Roubini: More than a decade on from the advent of Bitcoin, it's nowhere near as transformative as the internet was at a similar stage. The World Wide Web already had around a billion users ten years in. While it's difficult to know the total number of crypto users today, active users for the most traded coins probably amount to a maximum of a hundred million. Transaction growth for cryptocurrencies has been slower than in the case of the internet, and transaction costs remain very high, with mining revenues as a share of the total volume of transactions still very high. After ten years of the internet, there was email, millions of useful websites and apps, and technologies like the TCP and HTML protocols with broader applications. In the case of cryptocurrencies, there are so-called "dApps", or decentralized apps, but 75% of dApps are games like CryptoKitties or literally pyramid or Ponzi schemes of one sort or another. And the other 25% are "DEXs", or decentralized exchanges, that for now have few transactions and little liquidity. So the comparison with the internet just doesn't ring true.

Allison Nathan: Doesn't the concept of decentralized ledgers and networks have value, though?

Nouriel Roubini: I am not sure it does, but the reality is that the crypto ecosystem is not decentralized. An oligopoly of miners essentially controls about 70-80% of bitcoin and ether mining. These miners are located in places like China, Russia, and Belarus, which are strategic rivals of the US and have a different rule of law. That's why the US National Security Council is starting to worry about the risks that could pose for the United States. And 99% of all crypto transactions occur on centralized exchanges. Many crypto currencies also have a concentrated group of core developers who are police, judge, and jury whenever updates to or conflicts over the blockchain arise. Rules assumed to be fixed have been changed in these situations. So the blockchain isn't even immutable.

There's some evidence that the ownership of crypto wealth is also highly concentrated. Less than 0.5% of addresses own around 85% of all bitcoin, based on CoinMarketCap data. There's also evidence that whales holding a large amount of the total supply of bitcoin and other cryptocurrencies actively manipulate their prices. Tons of news articles have detailed active manipulation in chat rooms in the form of pump-and-dump schemes, spoofing, wash trading, front-running, etc. This behavior is much worse than even penny stocks, which suggests a high likelihood of an eventual regulatory crackdown.

Allison Nathan: Does any innovation in the crypto ecosystem look promising to you?

Nouriel Roubini: Not really. The next decade will see radical financial innovation across many dimensions, disrupting the traditional financial system. But it will have nothing to do with cryptocurrencies. Driving this innovation will be a revolution in fintech owing to some combination of AI, machine learning, and the use of the Internet of Things (IoT) to collect big data. Fintech is already transforming payment systems, borrowing and lending, credit allocation, insurance, asset management, and parts of the capital markets. In the context of payment systems, billions of transactions are made every day using AliPay and WeChat Pay in China, M-Pesa in Kenya and most of Sub-Saharan Africa, and Venmo, PayPal, and Square in the United States. These are all great companies that are scalable, secure, and are disrupting financial services. They're not based on decentralized finance (DeFi), and have nothing to do with crypto or blockchain.

I've honestly spent a lot of time looking at this because more and more people are saying that while maybe these aren't currencies, blockchain technology could be revolutionary. There are now all these buzzwords like "enterprise distributed ledger technology (DLT)" or "corporate blockchain." But I call most of these projects BINO—"Blockchain In Name Only". Something truly based on blockchain technology should be public, decentralized, permissionless, and trustless. But looking at DLT and corporate blockchain experiments, almost all of them are private, centralized and permissioned—because a small group of people has the ability to validate transactions—and most are authenticated by a trusted institution.

And even among these projects, few have actually worked. One study looking at 43 applications of blockchain technologies in the non-profit sphere for reasons such as banking the unbanked, giving IDs to refugees, and transferring remittances found that zero actually worked. The fundamental problem with this whole space is that it assumes the idea that technology can create trust. But that's mission impossible. Resolving the challenge of authenticating ownership or quality requires due diligence and testing. Why should I trust a DLT that says my tomatoes are organic? I trust Whole Foods that actually tests the tomatoes for chemicals. The idea that technology can resolve the question of trust is delusional. So, I'm deeply skeptical that blockchain, DLT, and cryptocurrencies for that matter will be the revolutionary technologies that their proponents suggest.

Bitcoin as a macro asset

Zach Pandl argues that institutional investors should treat bitcoin as a macro asset, akin to gold, going through a social adoption phase

Although bitcoin is now seeing wider institutional adoption, many sophisticated investors still struggle to understand why a digital asset should have any value—much less a market capitalization of more than $500bn. And because of the parabolic price increases and high retail participation, many treat the cryptocurrency phenomenon as a classic speculative mania or "bubble". Regardless of whether bitcoin will prove to be a good investment over time, this perspective is too narrow. Bitcoin is a medium which is beginning to serve the functions of money—primarily as a "store of value". Virtually anything can serve this purpose as long as it gains widespread social adoption, and bitcoin has made meaningful progress down that path.

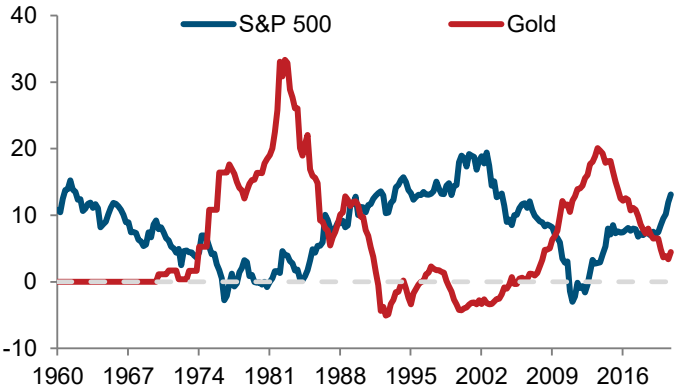
The need for stores of value

To understand bitcoin, it is best to begin with gold. Gold serves a unique function in the global financial system. It is both a useful commodity and a money-like, "store of value" asset. However, unlike conventional money mediums, it is not issued by a government and does not denominate any transactions in goods or assets. In effect, gold serves as an alternative fallback money instrument for adverse states of the world—when investors are unsure about the safety of conventional assets or fiat money in general (e.g. due to the risk of inflation or confiscation). In foreign exchange markets, gold behaves like an "inverse currency": its price tends to fall when the fundamentals of major currencies improve, and tends to rise when the fundamentals of major currencies worsen. Over time, the most important driver of nominal exchange rates is the relative rate of inflation between two economies. Because gold has a quasi-fixed supply, its nominal value tends to rise at the rate of inflation in major markets. These correlation and store of value properties allow gold to play a very useful diversification role in portfolios.

Originally, gold was likely adopted as a money medium due to its elemental properties. Gold and copper are the only metals which are not greyish in color in their natural state[1], and they have captivated humans since ancient times. Gold is also relatively dense, malleable, and ductile (stretchable), and unlike many other metals it does not tarnish, rust, or corrode. These features have underpinned gold's use as a money instrument throughout human history.

But the use of gold today has as much to do with inertia as it does with the metal's physical properties. After all, US Dollar notes are also a store of value, and they are made of paper[2]. Money, like language, is a social device—it is closer to a *concept* than a *thing*. Money is a social device that facilitates commerce, in much the same way that language is a social device that facilitates other aspects of our lives. It is useful for society to have a type of money that is not issued by a sovereign government. But the specific medium used for that purpose is partly arbitrary. Throughout history, a diverse array of objects has functioned as money, dictated by the demands of place and time—as Bitcoiners and monetary historians are fond of pointing out. Classic examples include the tobacco-based money standards of the early American colonies, and the regular use of mobile phone minutes as money throughout Africa. Gold serves a money function today primarily as an artifact of history, not because it is literally the best possible medium for society's store of value needs.

Gold plays an important diversification role in portfolios
10-year annualized returns



Source: Bloomberg, MeasuringWorth, Goldman Sachs GIR.

When inflation accelerated in the mid-20th century and investors sought out options to protect the real value of their assets, gold was the natural choice. At the time, major currencies were pegged to gold via the US Dollar through the Bretton Woods gold exchange standard, and, before the Great Depression, most currencies, as well as most US Treasury notes, were directly backed by gold. The US government provided an official price of gold in Dollars, which changed only twice in the nearly two centuries between the 1790s and 1970s. During the 1960s, under the gold exchange standard, gold trading above its official stated price was the clearest way to observe depreciation pressure on the US Dollar. In short, over much of the post-WWII period, there was a close association between the price of gold, currency stability, and the real value of money—making it the obvious inflation hedge for portfolios.

But the official link between the Dollar and the price of gold was severed 50 years ago when President Nixon ended the convertibility of Dollars into gold in August 1971. As a result, a generation of asset holders have grown up in a world without a tight connection between gold and money. So when the need for a store of value asset arises, could it be that they reach for something else?

Gold for the digital generation

This is where bitcoin comes in. Any alternative medium would need to be secure, privately held, have a fixed or quasi-fixed supply, and be transferable, ideally outside the traditional payments system. In our modern globalized society, where a substantial portion of social interaction and commerce occurs online (especially among younger people), it may also need to be digital. But, most importantly, it would need to have the potential for widespread social adoption—*anything* can be money, as long as it has that. Bitcoin is therefore a plausible

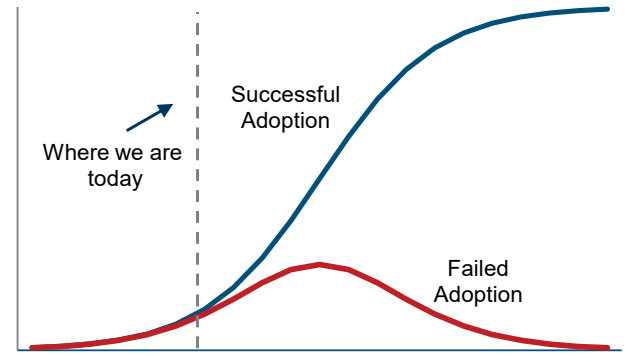
[1] Gold's periodic symbol AU comes from the Latin word *aurum*, meaning "shining dawn."
[2] Technically a 75% cotton-based and 25% linen-based material.

alternative store of value medium to gold and, at the moment, the best candidate among cryptocurrencies with a similar structure because of its broader social adoption (i.e. its "name brand").

In equilibrium, a store of value as volatile as bitcoin would not be very useful. But cryptocurrencies are in their infancy; it is better to think of today's prices as reflecting some probability that bitcoin or another coin/token could achieve greater adoption in the future, at which time its price could be extremely high. Therefore, small changes in those probabilities can result in high price volatility today. Bitcoin investors are speculating that it will eventually achieve near-universal acceptance as a non-sovereign money, with high returns (and high volatility) along the way.

Today's bitcoin prices reflect some probability that cryptos could achieve greater adoption in the future

Time (x-axis) vs. price (y-axis)



Source: Goldman Sachs GIR.

The critical ingredient to bitcoin's success—widespread social adoption—has now crossed many notable thresholds: Tesla, the sixth largest company in the S&P 500, is carrying bitcoin on its balance sheet; storied macro hedge fund Brevan Howard has begun investing in cryptocurrencies; and Coinbase is now listed on the Nasdaq. Other blockchain networks, especially Ethereum, are developing decentralized banking platforms, Facebook is expected to introduce its stablecoin Diem later this year, and many central banks are exploring distributed ledger technology for their own digital currencies. Whether bitcoin will succeed as a store of value in the long run remains an open question—and its consumption of real resources may be a headwind over time—but for now social adoption of cryptocurrencies appears to be moving forward.

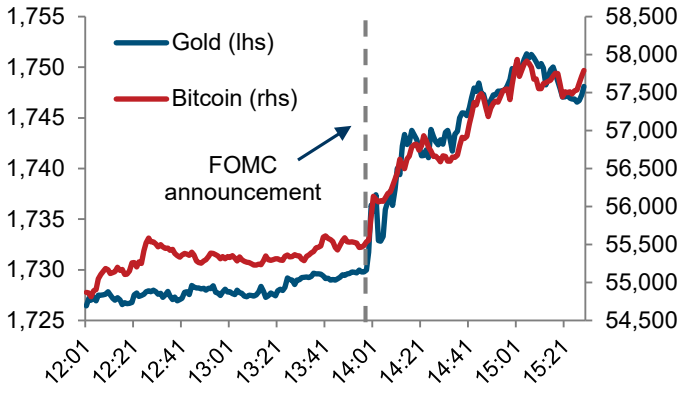
Bitcoin as a macro asset

Bitcoin has also matured enough that its price behavior resembles that of other macro assets. For example, at its March 17th meeting, the Federal Reserve said that most policymakers did not expect to raise interest rates until after 2023—later than financial markets had expected. Macro assets reacted in the conventional way to a "dovish policy shock": shorter-maturity Treasury yields declined, the yield curve steepened, the Dollar fell, and stock prices increased. Bitcoin rose, just like gold, but with about four times the volatility.

Investors should treat bitcoin in this way. Gold is a *commodity* that serves a *money* function and behaves like a *currency*. Bitcoin is exactly the same, even though it is a digital commodity created through cryptography, rather than a physical commodity found in the Earth's crust. From a markets standpoint, the main difference between the two assets is that bitcoin is going through a one-time social adoption phase—which may succeed or fail. When social adoption is rising, bitcoin should offer superior returns compared to gold. When social adoption is declining (e.g. due to adverse regulatory changes), bitcoin will likely offer inferior returns compared to gold. Because of the speculative nature of the asset class and high uncertainty around valuation, investors should be prepared for prices to overshoot fundamentals in both directions. While bitcoin has generally appreciated in value over time, there have already been several waves of speculative excess followed by large drawdowns.

Bitcoin behaved like gold following the March FOMC announcement

Prices on March 17, 2021, $

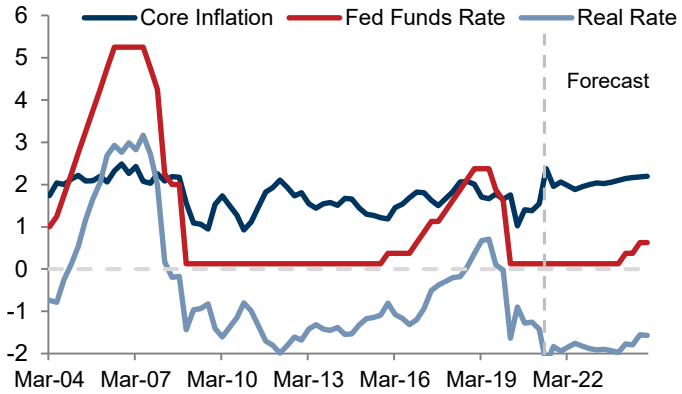


Source: Bloomberg, Goldman Sachs GIR.

Technological issues aside, the current macroeconomic outlook appears favorable for store of value assets, whether physical or digital. The Federal Reserve has adopted a more ambitious labor market goal of "broad and inclusive" full employment, and seems more tolerant of above-target inflation than in the recent past. Our economists expect real cash yields to remain negative across developed market economies for a number of years to come. Equity market multiples are at historic highs. Many developing countries will struggle with the fiscal hangover from the COVID-19 crisis for years to come. In this environment, unless investors can find other sources of real returns, demand for assets that protect purchasing power should remain high.

Low real interest rates should support high demand for "store of value" assets over the next several years

%



Source: Goldman Sachs GIR.

Zach Pandl, Co-Head of Global FX, Rates, EM Strategy

Email: zach.pandl@gs.com *Goldman Sachs and Co. LLC*
Tel: 212-902-5699

Crypto is its own class of asset

Jeff Currie argues that cryptos are a new class of asset that derive their value from the information being verified and the size and growth of their networks, but legal challenges loom large

The term "cryptocurrencies"—which most people take to mean that crypto assets act as a digital medium of exchange, like fiat currency—is fundamentally misleading when it comes to assessing the value of these assets. Indeed, the blockchain that underlies bitcoin was not designed to replace a fiat currency—it is a trusted peer-to-peer payments network. As a cryptographic algorithm generates the proof that the payment was correctly executed, no third party is needed to verify the transaction. The blockchain and its native coin were therefore designed to replace the banking system and others like insurance that require a trusted intermediary today, not the Dollar. In that sense, the blockchain is differentiated from other "digital" transactional mechanisms such as PayPal, which is dependent upon the banking system to prevent fraud like double-spending.

In order to be trustworthy, the system needed to create an asset that had no liabilities or contingent claims, which can only be a real asset just like a commodity. And to achieve that, blockchain technologies used scarcity in natural resources—oil, gas, coal, uranium and hydro—through ever-increasing computational-power consumption to "mine" a bit version of a natural resource.

From this perspective, the intrinsic value of the network is the trustworthy information that the blockchain produces through its mining process, and the coins native to the network are required to unlock this trusted information, and make it tradeable and fungible. It's therefore impossible to say that the network has value and a role in society without saying that the coin does too. And the value of the coin is dependent upon the value and growth of the network.

That said, because the network is decentralized and anonymous, legal challenges facing future growth for crypto assets loom large. Coins trying to displace the Dollar run headlong into anti-money laundering laws (AML), as exemplified by the recent ransoms demanded in bitcoin from the Colonial Pipeline operator and the Irish Health service. Regulators can impede the use of crypto assets as a substitute for the Dollar or other currencies simply by making them non-convertible. An asset only has value if it can either be used or sold. And Chinese and Indian authorities have already challenged crypto uses in payments.

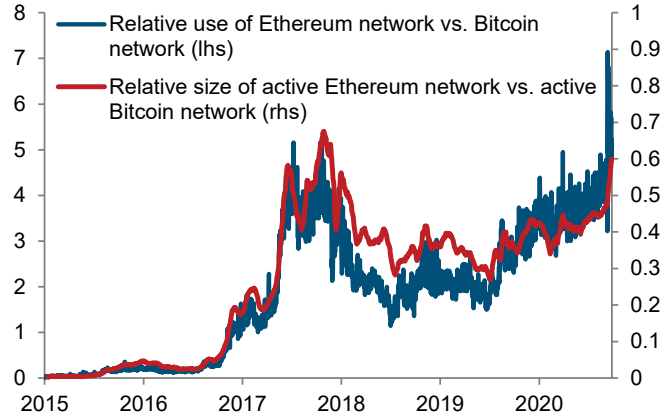
As a result, the market share of coins used for other purposes beyond currencies like "smart contracts" and "information tokens" (see pgs. 26-27) will likely continue to rise. However, even these non-currency uses will need to be recognized by courts of law to be accepted in commercial transactions—a question we leave to the lawyers.

The network creates the value, unlike other commodities

Unlike other commodities, coins derive their entire value from the network. A bitcoin has no value outside of its network as it is native to the Bitcoin blockchain. The value of oil is also largely derived from the transportation network that it fuels, but at least oil can be burned to create heat outside of this network. At the other extreme, gold doesn't require a network at all.

Non-currency crypto assets are starting to dominate use

Transactions on the Ethereum blockchain vs. transactions on the Bitcoin blockchain, ratio (lhs); Number of active nodes on Ethereum network vs. active nodes on Bitcoin network, ratio (rhs)



Source: Bloomberg, Goldman Sachs GIR.

Derived demand leaves the holder of the commodity exposed to the risk of the network becoming obsolete—a lesson that holders of oil reserves are now learning with decarbonization accelerating the decline of the transportation network, and, in turn damaging oil demand. Likewise, bitcoin owners face accelerated network decay risk from a competing network, backed by a new cryptocurrency.

As the demand for gold is not dependent on a network, it will ultimately outlive oil and bitcoin—gold entropy lies at the unit, not the network, level. Indeed, most stores of value that are used as defensive assets—like gold, diamonds and collectibles—don't have derived demand and therefore only face unit-level entropy risk. This is what makes them defensive. The world can fall apart around them and they preserve their value. And while they don't have derived demand, they do have other uses that establish their value, i.e. gold is used for jewelry and as a store of value.

Transactions drive value, creating a risk-on asset

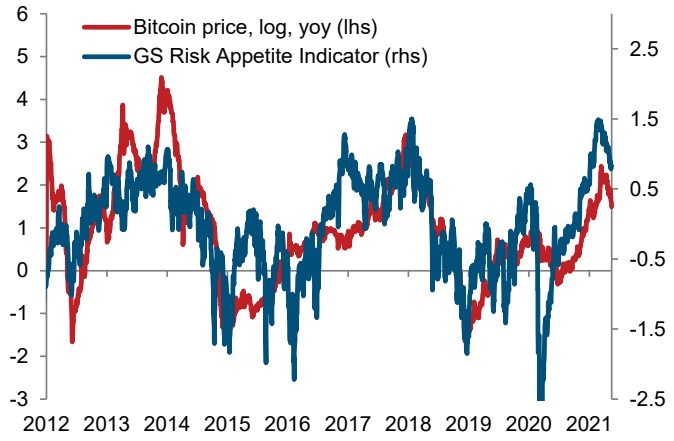
Crypto doesn't trade like gold and nor should it. Using any standard valuation method, transactions or expected transactions on the network are the key determinant of network value. The more transactions the blockchain can verify, the greater the network value. Transaction volumes and the demand for commodified information are roughly correlated with the business cycle; thus, crypto assets should trade as pro-cyclical risk-on assets as they have for the past decade. Gold and bitcoin are therefore not competing assets as is commonly misunderstood, and can instead co-exist.

Because the value of the network and hence the coin is derived from the volume of transactions, hoarding coins as stores of value reduces the coins available for transactions, which reduces the value of the network. Because gold doesn't have this property, it is the only commodity that institutional investors hold in physical inventory. Nearly all other commodities are held in paper inventory in the form of futures to avoid disrupting the network. This suggests that, like oil,

crypto investments will need to be held in the form of futures contracts, not physically, if they are to serve as stores of value.

Crypto assets aren't digital oil, either, as they are not non-durable consumables and can therefore be used again. This durability makes them a store of value, provided this demand doesn't disrupt network flows. The crypto assets that have the greatest utility are also likely to be the dominant stores of value—the high utility reduces the carry costs.

Payment networks—and hence cryptocurrencies—are pro-cyclical, as greater use drives value



Source: Bloomberg, Goldman Sachs GIR.

So what is crypto? A powerful networking effect

The network provides crypto an extremely powerful networking externality that no other commodity possesses. The operators—miners, exchanges and developers—are all paid in the native coin, making them fully vested in its success. Similarly, users—merchants, investors and speculators—are also fully vested. This gives bitcoin holders an incentive to accommodate purchases of their own products in bitcoin, which in turn, creates more demand for the coins they already own. Similarly, ether holders have an incentive to build apps and other products on the Ethereum network to increase the value of their coins.

Because the coin holders have a stake in the network, speculation spurs adoption; even during bust periods, coin holders are motivated to work to create the next new boom. After the dot-com bust, the shareholders had no commodity to promote. In crypto assets, even when prices collapse, the coin holders have a commodity to promote. They will always live for another boom, like an oil wildcatter.

It's all about information

As the value of the coin is dependent on the value of the trustworthy information, blockchain technology has gravitated toward those industries where trust is most essential—finance, law and medicine. For the Bitcoin blockchain, this information is the record of every balance sheet in the network, and the transactions between them—originally the role of banks. In the case of a smart contract—a piece of code that executes according to a pre-set rule—on Ethereum, both the terms of that contract (the code) and the state of the contract (executed or not) are the information validated on the Ethereum blockchain. As a result, the counterparty in the contract cannot claim a transfer of funds without the network forming a consensus that the contract was indeed executed. In our view, the most valuable crypto assets will be those that help verify the most critical information in the economy.

Over time, the decentralized nature of the network will diminish concerns about storing personal data on the blockchain. One's digital profile could contain personal data including asset ownership, medical history and even IP rights. Since this information is immutable—it cannot be changed without consensus—the trusted information can then be tokenized and traded. A blockchain platform like Ethereum could potentially become a large market for vendors of trusted information, like Amazon is for consumer goods today.

Crypto beyond this boom and bust cycle

By many measures—Metcalfe's Law or Network Value to Transactions (NVT) ratio —crypto assets are in bubble territory. But does the demand for "commodified information" create enough economic value at a low enough cost to be scaled up in the long run? If the legal system accommodates these assets, we believe so. While many overvalued networks exist, a few will likely emerge as long-term winners in the next stage of the digital economy, just as the tech titans of today emerged from the dot-com boom and bust. This transformation is happening now—there are already an estimated 21.2 million owners of cryptocurrencies in the US alone. However, technological, environmental and legal challenges still loom large.

Ethereum 2.0 is expected to ramp up capacity to 3,000 transactions per second (tps), while sharding—which will scale Ethereum 2.0's Proof of Stake (PoS) system through parallel verification of transactions—has the potential to raise capacity to as much as 100,000 tps. For context, Visa has the capacity to process up to 65,000 tps but typically executes around 2,000 tps. PoS intends to have validators stake the now scarce and valuable coins to incentivize good behavior instead of having miners expend energy to mine new blocks into existence, as under Proof of Work, making crypto assets more ESG friendly. PoS also can significantly boost computational time in terms of transactions per second, which will further incentivize technological adoption. Ironically, this is likely where the value of and demand for bitcoin will come from—being used as the scarce resource to make the PoS system work instead of natural resources.

While overcoming the economic challenges will likely be manageable, the legal challenges are the largest for many crypto assets. And this past week was challenging for crypto assets with confirmation that the 75 bitcoin ransom over the Colonial Pipeline was actually paid. This is a reminder that cryptocurrencies still facilitate criminal activities that have large social costs. For Ethereum, new companies which aim to disrupt finance, law or medicine by integrating information stored on the platform into their algorithms are likely to run into problems with being legally recognized. If crypto assets are to survive and grow to their fullest potential, they need to define some concept of "sufficiently decentralized" that will satisfy regulators; otherwise, the technologies will soon run out of uses.

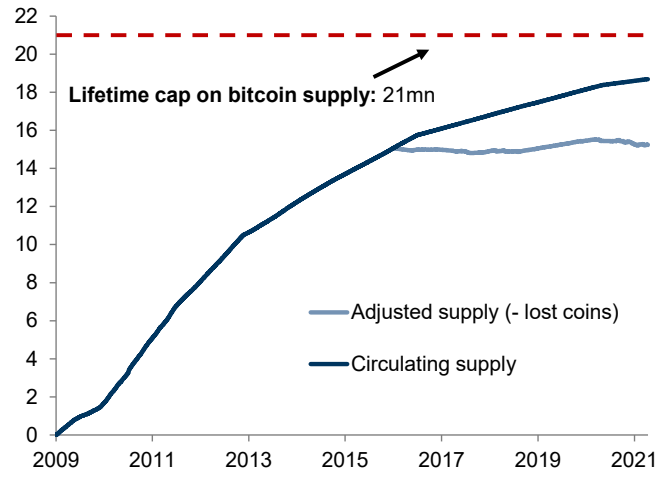
Jeff Currie, Global Head of Commodities Research

Email: jeffrey.currie@gs.com *Goldman Sachs and Co. LLC*
Tel: 44-20-7552-7410

Bitcoin: sizing the market

Around 90% of all bitcoin that will ever exist is in circulation

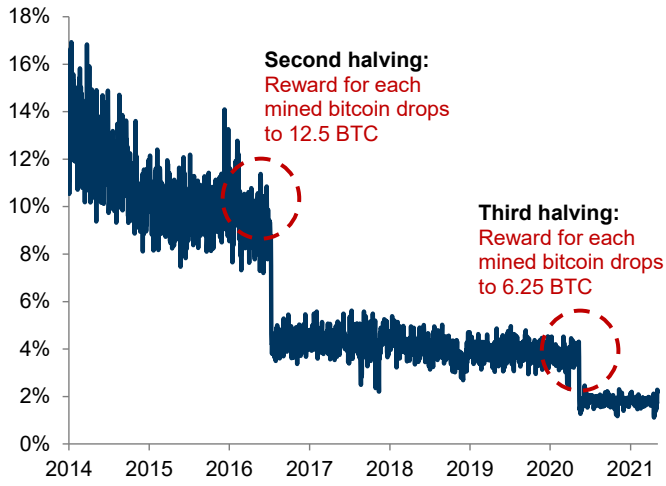
Total circulating and adjusted supply, million



Note: Adjusted supply includes estimate of lost coins based on those that haven't moved in over seven years.
Source: Glassnode, Goldman Sachs GIR.

Artificial scarcity is programmed into the bitcoin market

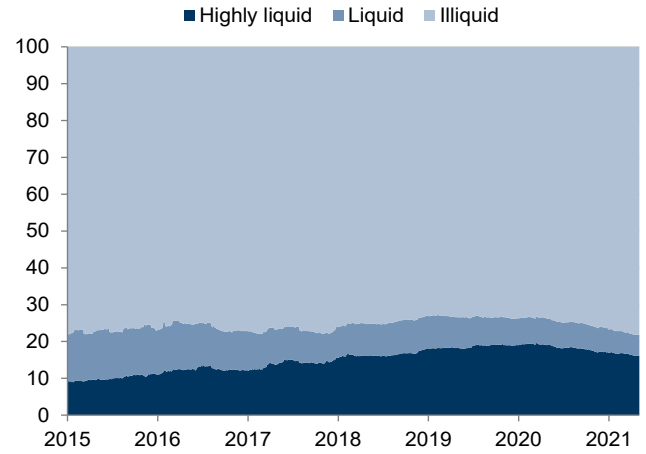
Annual bitcoin inflation rate (new units as % of current supply), %



Source: Glassnode, Goldman Sachs GIR.

One measure suggests that 80% of bitcoin supply is illiquid

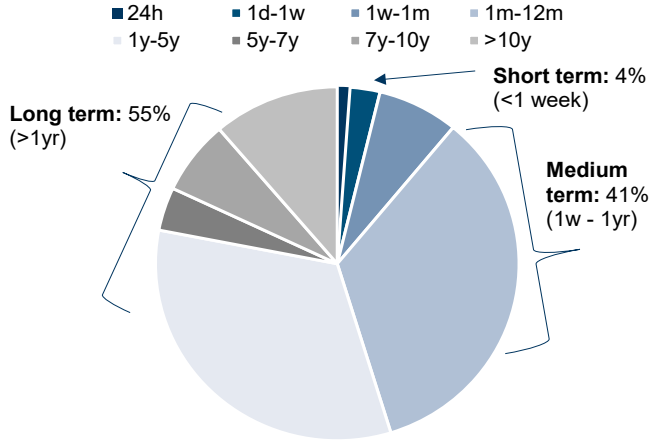
Percent of total supply by liquidity, %



Note: Based on the ratio of the cumulative inflows/outflows of all entities in the Bitcoin network. See more details here.
Source: Glassnode, Goldman Sachs GIR.

The footprint of short-term bitcoin holders is fairly small

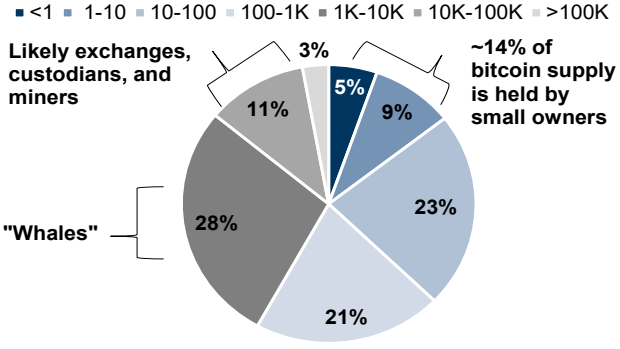
Age distribution of bitcoin supply based on last transaction



Note: Based on the percentage of bitcoin in existence that was last moved within each given time period. See more detail here.
Source: Glassnode, Goldman Sachs GIR.

One measure that looks at network addresses suggests bitcoin holdings are fairly concentrated

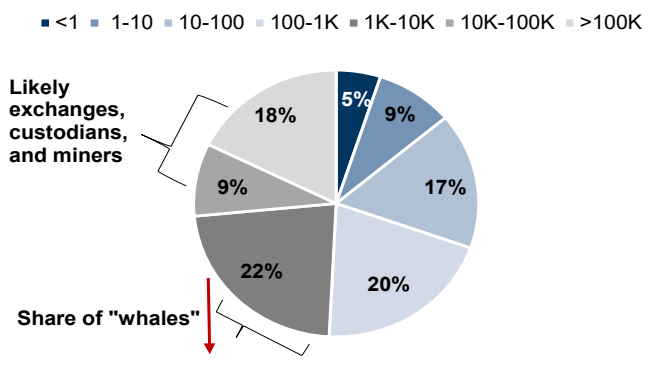
Total supply held by size of addresses' coin holdings, % total



Note: Shows share of total bitcoin supply held by the balance of different addresses. See more detail here.
Source: CoinMarketCap, Goldman Sachs GIR.

A measure that looks at bitcoin entities shows less concentration among "whales", because entities can own many addresses

Total supply held by size of entities' coin holdings, % total

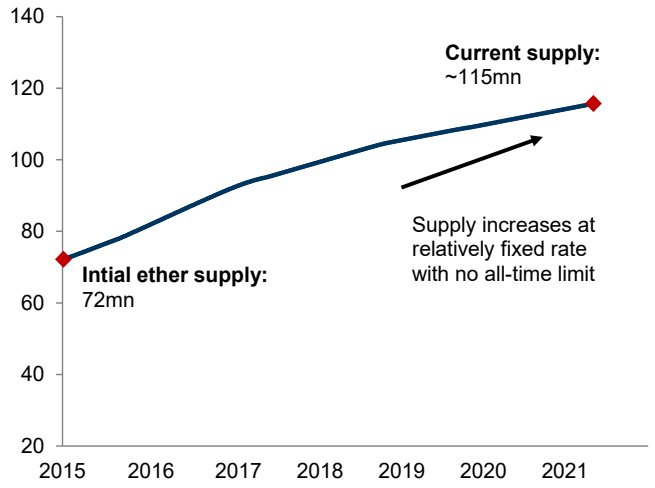


Note: Shows share of total bitcoin supply held by the balance of different entities. See more detail here.
Source: Glassnode, Goldman Sachs GIR.

Ethereum: sizing the market

Unlike bitcoin, the all-time supply of ether isn't capped

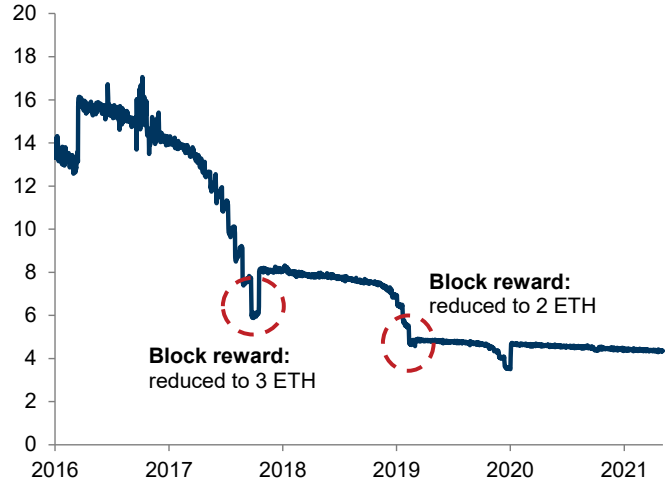
Total circulating supply, million



Note: A recently approved network update could reduce supply; see here.
Source: Glassnode, Goldman Sachs GIR.

But the pace of new supply creation has come down

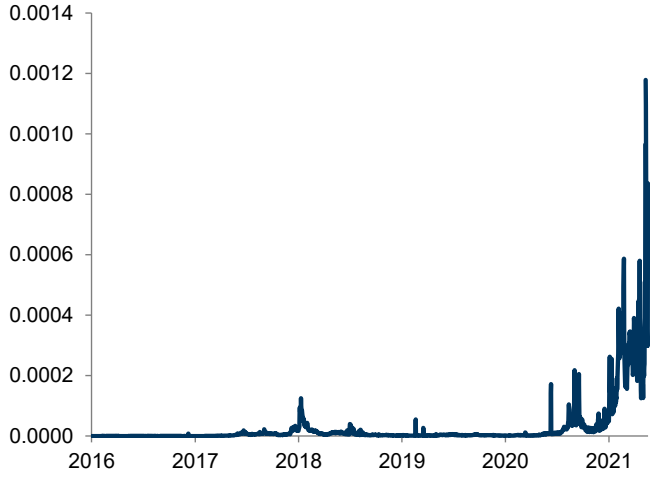
Annual ETH inflation rate (new units as % of current supply), %



Source: Glassnode, Goldman Sachs GIR.

Fees on the Ethereum network have risen with transactions

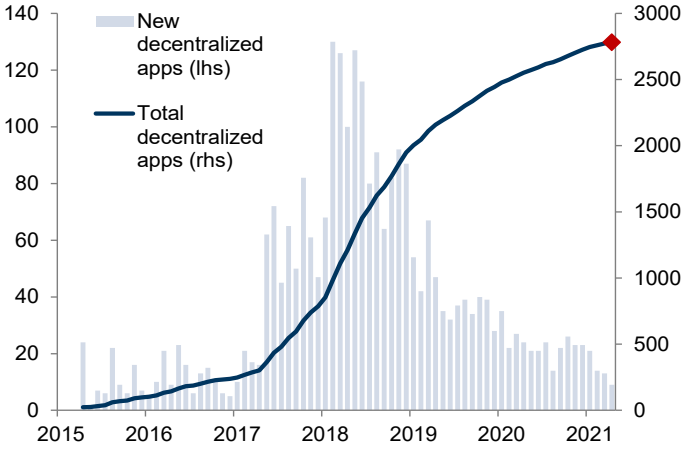
Average price paid per transaction ("gas"), $



Note: For more details on Ethereum transaction fees see here.
Source: Glassnode, Goldman Sachs GIR.

More than 2.5K decentralized apps are built on Ethereum

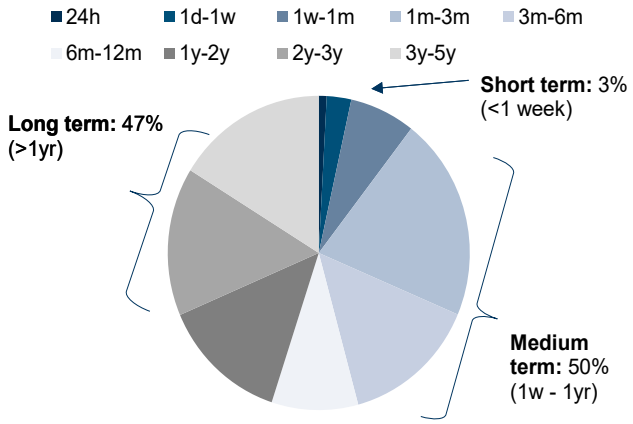
New and total decentralized apps, count



Source: stateofthedapps.com, Goldman Sachs GIR.

Ether holdings are modestly shorter duration than bitcoin

Age distribution of ether supply based on last transaction



Note: Based on the percentage of ether in existence that was last moved within each given time period.
Source: Glassnode, Goldman Sachs GIR.

More than 20% of ether supply is held in smart contracts

Ether supply held in smart contacts, % total supply

Source: Glassnode, Goldman Sachs GIR.

Interview with Michael Sonnenshein

Michael Sonnenshein is CEO at Grayscale Investments. Below, he discusses the evolution of the digital asset ecosystem and the factors behind rising institutional interest in the space.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: How does Grayscale and its parent company, Digital Currency Group, engage in the digital asset universe?

Michael Sonnenshein: Grayscale Investments is a digital currency asset manager with AUM of about $45 billion today spread across a family of 14 unique investment products, the largest of which is the Grayscale Bitcoin Trust. The Grayscale business model is predicated on providing investors access and exposure to digital currencies while avoiding the challenges involved in buying and safely storing digital currencies themselves. Our parent company, Digital Currency Group, is a conglomerate that seeks to invest in, build, and purchase businesses related to digital currency and blockchain technology, and has invested in about 170 digital currency/blockchain-related businesses in over 40 countries.

Allison Nathan: How do your products differ from a crypto ETF, which has yet to gain regulatory approval in the US?

Michael Sonnenshein: All of our products are passive, long-only funds that are directly invested in the referenced digital asset for each product. So a $100 investment in the Grayscale Bitcoin Trust is backed by $100 worth of bitcoin, which is bought in the market and then stored in cold storage with a qualified custodian that is a fiduciary under New York state banking laws, and who also insures the assets. Today, six out of the 14 funds are also publicly quoted and traded on the OTCQX markets, where the ADRs of many foreign companies trade. These represent a secondary market that in some ways mimic the attributes of an ETF because they trade every day, but they are not ETFs. The two largest differences between them and an ETF are, one, they do not trade on a national securities exchange, like NYSE or NASDAQ, and two, they do not have ongoing creation and redemptions like ETFs. So they operate more like a closed-end offering than an ETF.

Allison Nathan: You have a bird's eye view on the digital asset investor base. How has it evolved?

Michael Sonnenshein: In 2013/14, when I got my start in the digital currency space, only Silicon Valley VCs, and maybe some forward-thinking family offices, were speaking about digital assets. Over time, interest in digital assets began to trickle down to retail investors who were gaining access to crypto through trading platforms and order books. And, more recently, the most meaningful shift has been increased interest from institutional investors. Several years ago, digital assets were generally considered a taboo asset class among institutional investors because of perceived reputational risks, regulatory concerns and a view that engaging in digital assets was just too much of a departure from the other strategies they typically employ.

Today, not only is there a general appreciation amongst all investors, including the institutional community, that digital assets are here to stay, but also all of those preconceived notions have been shrugged off. We no longer hear concerns about nefarious activity on the blockchain. We no longer hear about reputational concerns; investors now want their fiduciaries to participate in crypto. And we no longer hear concerns about regulatory risk; regulators have provided enough clarity for investors to feel comfortable participating.

Over just the last 12 to 18 months, the asset class has really turned the corner as some well-known and experienced investors have publicly come out in support of crypto, corporations have begun to allocate to crypto on their balance sheet as a reserve asset, and participation from legacy financial institutions has materially increased. All of these developments signal that, across the spectrum, the investment community wants to participate in the crypto ecosystem, and is as smart as ever on the asset class. I have yet to find somebody who has really done their homework on crypto assets that isn't truly amazed by the potential for the asset class.

That being said, in the same way that not every investment opportunity will be right for all investors, digital assets are not necessarily the best fit for all institutions. It's also important to remember that the asset class is only 10-12 years old and so is still in its very early days. But we are now at a point where the crypto market is as robust as it's ever been in terms of being a two-sided market, having the ability to engage in derivatives, lending and borrowing, and offering many of the same kinds of products as traditional asset classes.

Allison Nathan: Why do institutional investors want to be involved in the market?

Michael Sonnenshein: The potential for significant upside is certainly an attraction. But more than anything, investors realize the significant diversification benefit of adding crypto to their portfolios, which can help them achieve higher risk-adjusted returns. As policymakers have injected substantial stimulus into the financial system in order to jumpstart the economy from the COVID-related slowdown, investors have become increasingly attracted to the finite quality of assets like bitcoin—which is verifiably scarce—as a way to hedge against inflation and currency debasement. Investors are starting to move out of assets like gold, which historically have served as stores of value or inflation hedges, as they realize that assets like bitcoin can also serve those roles in their portfolios.

Allison Nathan: But given the short history of bitcoin/digital assets, isn't it too soon to conclude that these assets provide diversification benefits or are a hedge against inflation, especially since they seemed to act more like risky assets during the depths of the pandemic recession?

Michael Sonnenshein: We've found that during some macro shocks, like the devaluation of the renminbi in 2015 or the unexpected Brexit vote in 2016, crypto outperformed. However, during periods of broad-based selloffs or de-leveraging, like we saw in March 2020 when COVID-19 brought the global economy to a grinding halt, nothing was safe from what was taking place in the system. Everything sold off—bonds, currencies, equities,

and crypto. But crypto snapped back much faster and more significantly than other asset classes over the course of 2020. After probably the hundredth time of pronouncing crypto "dead", that resiliency and staying power has solidified for a lot of investors that this is a space they want to be in.

Allison Nathan: But can bitcoin survive as a store of value since it has no other uses—compared to gold that is used for jewelry, art, wine, etc.—which could temper its volatility and put a floor on its value?

Michael Sonnenshein: People have largely left behind the idea that bitcoin needs to be used in everyday commerce in order to be successful, and since it hasn't yet replaced the Dollar nor am I yet buying my latte with it, it has failed. Again, it's important to drive home the notion that we are still in the early days of the development of crypto assets and use cases for them. Today, the developed world use case for bitcoin is primarily as a digital store of value that is more suitable to today's digital world compared to the physical world in which gold may have historically served a better purpose.

Many investors also think of digital asset exposure as an early stage technology investment or as a conduit to the next generation of payment systems and the way in which value may be moved around the world, potentially disrupting remittance networks, cross border payments, etc. But they have the potential to unlock all kinds of other use cases, including areas like microfinancing and micropayments, and leveraging the underlying blockchain technology for commerce, shipping, manufacturing, etc. This technology is truly the most secure and most widely utilized consensus mechanism the world has ever had. And when you think about how powerful consensus can be, we're not yet anywhere close to utilizing the full capabilities of what the protocol may offer.

Allison Nathan: But isn't it now well-known that transaction speeds on the Bitcoin blockchain are too slow for it to be useful in the payment system and other commercial uses?

Michael Sonnenshein: You're right to call out that one of the flaws of Bitcoin is its relatively slow transaction speed. The transactional nature of bitcoin is akin to what you see on Black Friday when many payment networks are bogged down because so many people are shopping and using their credit cards. But slower-than-desirable transaction speeds are also a sign of Bitcoin's success; the quantity of transactions transpiring on the network was never conceived to be as high as it is today. A variety of efforts have been and are underway to challenge that attribute, and I believe we will continue to find ways to increase transactional throughput.

Allison Nathan: There are already some offshoots of the Bitcoin blockchain that improve upon this flaw. So isn't it likely that improvements won't be captured by bitcoin itself, but by another crypto asset?

Michael Sonnenshein: Bitcoin is an open source protocol, which means that people are able to take its source code, copy it over, tweak one attribute, and then launch it as a new digital currency. Some of those currencies, like bitcoin cash, have had staying power and have developed a real user base. That said, the success of one crypto asset over another really boils down to the value of the network built into them. Today, bitcoin has a $700bn market cap, which represents 700 billion dollars of switching costs that would need to be monetized for users to move from bitcoin to something else. Bitcoin's open source nature provides reassurance that over time as it is challenged, it will integrate new and better features that prevent it from becoming the Myspace to an eventual Facebook.

Allison Nathan: Do you hear institutional investors expressing concerns over the high concentration of crypto holdings or the environmental aspects of mining?

Michael Sonnenshein: There is certainly concentration within the crypto ecosystem among a relatively small number of entities, but that's not unique to crypto. And we do sometimes hear concerns about the energy consumption of bitcoin miners, but there's quite a lot of misinformation out there around this. While mining is very energy intensive, it is extremely competitive, and one way that miners can beat out others for mining rewards is to utilize the lowest cost energy. So miners have moved to lower-cost renewable energy sources as much as possible, including solar, wind, hydro, etc.

Allison Nathan: So what are the remaining roadblocks to further institutional adoption and how likely are they to be overcome?

Michael Sonnenshein: The biggest obstacles primarily relate to the plumbing around crypto assets, and the remaining gap between the crypto asset ecosystem and the traditional financial system, but both are actively being addressed. The underpinnings of the crypto ecosystem are still maturing, but tremendous work is underway in terms of improving order management systems, tax lot reporting, algorithms, application programming interfaces (APIs), custodial solutions, and all of the nuts and bolts that digital assets need to thrive. Investors also still can't access digital assets as easily—or, for the most part, through the same channels—as they do traditional instruments. Recent and future potential developments that bridge the gap between these two ecosystems, such as being able to buy crypto through your prime broker or leveraging a bitcoin ETF, will go a long way in enabling greater participation in digital assets.

Allison Nathan: How much of the interest in digital assets is now being directed beyond bitcoin to other cryptos?

Michael Sonnenshein: There is a meaningful bid for other digital assets from investors who appreciate not only the diversification benefits from owning crypto as an asset class, but also the benefits of diversifying their crypto allocation. As investors have seen the advent of new use cases on top of blockchains like Ethereum, whether that be the proliferation of decentralized finance (DeFi), non-fungible tokens (NFTs), etc., they have increasingly moved beyond just allocating to bitcoin and instead are seeking exposure to the entire ecosystem.

Allison Nathan: Dogecoin: a blessing or a curse for cryptos?

Michael Sonnenshein: Dogecoin is a demonstration of just how easy it is to create a digital asset. It, along with a slew of other digital assets, was created by enthusiasts basically for fun. That drills home the point that it's important for investors to scrutinize use cases and whether the asset is viable and has the potential to gain real world traction by solving a real world problem versus a solution in search of a problem that may not exist.

What is a digital store of value?

Mikhail Sprogis and Jeff Currie argue that other cryptocurrencies besides bitcoin are better positioned to become the dominant digital store of value

Based on emerging blockchain technology that has the power to disrupt global finance, yet with limited clear use today, bitcoin has been labeled a solution looking for a problem. Many investors now view bitcoin as a digital store of value, comparable to gold, housing, or fine wine. But all true stores of value in history have provided either income or utility, and bitcoin currently provides no income and only very modest utility.

However, unlike bitcoin, several other crypto assets have clear economic rationales behind their creation. Bitcoin's first-mover advantage is also fragile; crypto remains a nascent field with shifting technology and consumer preferences, and networks that fail to adjust quickly could lose their leadership. We therefore see a high likelihood that bitcoin will eventually lose its crown as the dominant digital store of value to another cryptocurrency with greater practical use and technological agility. Ether looks like the most likely candidate today to overtake bitcoin, but that outcome is far from certain.

What is a store of value?

A store of value is anything that preserves its value over time. While financial stores of value like equities and bonds hold their value because they produce a given cash flow, yield is not a prerequisite for value. Art, wine, gold, and non-yielding currencies are widely used as stores of value too. Yet all of these non-yielding assets have a clear material use besides being stores of value. This usefulness generates a "convenience yield"—the incentive for people to own them—that reflects both the utility a consumer derives from using these assets and the relative scarcity of that utility—a fact captured by Adam Smith's famous Diamond-Water paradox.

We place assets on a continuum across time by their store of value properties. We identify *stores of future value*, like financial assets that offer the owner the right to future yields or the promise of growing value over time, *stores of present value*, like consumable commodities such as oil and grains for which the utility of driving and eating today imparts a convenience yield, and *stores of past value*, like gold, art or even housing in which the assets store value generated in the past because of their duration.

Value always stems from use

The key to *stores of past value* like gold and houses is that someone demanded these assets in the past and placed value in them by exchanging something of value, usually currency, for them. Indeed, all important non-yielding stores of value developed real uses before becoming investment assets. For instance, gold was first used as jewelry to signal permanence, commitment or immortality. The economic problem was a need to signal permanence, and gold's durable and inert elemental properties solved that problem. Given the state of technology at the time, gold was the only solution for this problem, which explains why so many societies adopted it for this use.

Economic value is created when marginal benefit exceeds marginal cost, and crypto fails this test

Store of Value	Asset	Marginal Cost of Carry	Measure of Marginal Cost	Marginal Benefit of Carry	Measure of Marginal Benefit	Annualized Vol	Vol adjusted net benefit
Financial	S&P	0.6%	LIBOR	1.4%	Dividend Yield	18.4%	0.04
	Tesla	0.6%		0.0%		69.9%	-0.01
	US 10y bond	0.6%		1.6%	Interest Rate	5.6%	0.17
	10y Bund	0.6%		-0.2%		4.0%	-0.21
	10y JGB	0.6%		0.1%		1.3%	-0.40
	3m US T-bill (cash)	0.6%		0.04%		0.04%	-14.87
Commodity	Crude oil	7%	Commodity Storage Cost	3.3%	Spot Front - Third Roll Yield, Annaulised	39.5%	-0.10
	Copper	0%		0.4%		20.5%	0.01
	Corn	11%		50.3%		23.1%	1.71
	Soybean	4%		49.0%		17.6%	2.54
	Silver	1%		-0.8%		42.5%	-0.03
	Gold	0%		-1.4%		18.0%	-0.08
	Wheat	9%		-4.1%		26.0%	-0.51
Real	Housing	3.3%	Mortgage and Insurance	2.9%	Rental Yield	5.1%	-0.08
Crypto	Ether	0.5%	LIBOR	-7%	Spot Front - Third Roll Yield, Annaulised	89.3%	-0.08
	Bitcoin	0.5%		-11%		57.6%	-0.20

Source: Bloomberg, Goldman Sachs GIR.

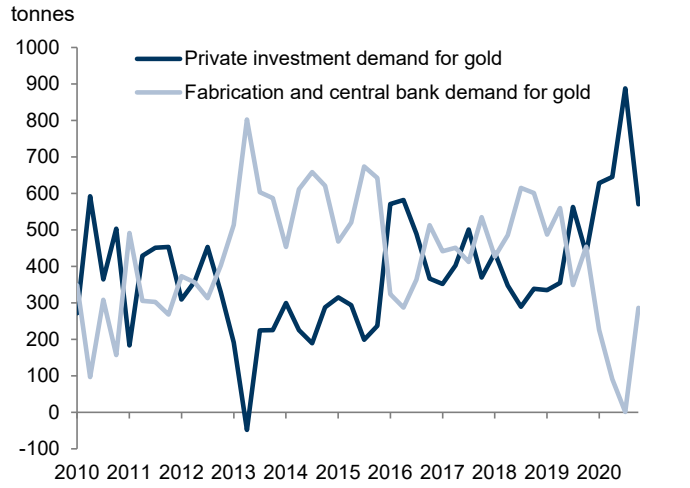
And when societies began to conquer each other and needed a means to standardize international trade, gold was the natural choice to solve this economic problem as most societies already owned gold and it was divisible. Real use is important for stores of value because consumption demand tends to be price-sensitive and therefore provides some offset to fluctuations in investment demand, tempering price volatility. For example, jewelry demand is the swing factor in the gold market, falling when investment demand for gold pushes prices higher, and vice versa.

Ether beats bitcoin as a store of value

Given the importance of real uses in determining store of value, ether has high chance of overtaking bitcoin as the dominant digital store of value. The Ethereum ecosystem supports smart contracts and provides developers a way to create new applications on its platform. Most decentralized finance (DeFi) applications are being built on the Ethereum network, and most non-fungible tokens (NFTs) issued today are purchased using ether. The greater number of transactions in ether versus bitcoin reflects this dominance. As cryptocurrency use in DeFi and NFTs becomes more widespread, ether will build its own first-mover advantage in applied crypto technology.

Ethereum can also be used to store almost any information securely and privately on a decentralized ledger. And this information can be tokenized and traded. This means that the Ethereum platform has the potential to become a large market for trusted information. We are seeing glimpses of that today with the sale of digital art and collectibles online through the use of NFTs. But this is a tiny peek at its actual practical uses. For example, individuals can store and sell their medical data through Ethereum to pharma research companies. A digital profile on Ethereum could contain personal data including asset ownership, medical history and even IP rights. Ethereum also has the benefit of running on a decentralized global server base rather than a centralized one like Amazon or Microsoft, possibly providing a solution to concerns about sharing personal data.

Real demand for gold is a powerful price stabilization tool



Source: World Gold Council, Goldman Sachs GIR.

A major argument in favor of bitcoin as a store of value is its limited supply. But demand, not scarcity, drives the success of stores of value. No other store of value has a fixed supply. Gold supply has grown nearly ~2% pa for centuries, and it has remained an accepted store of value. Plenty of scarce elements like osmium are not stores of value. In fact, a fixed and limited supply risks driving up price volatility by incentivizing hoarding and forcing new buyers to outbid existing holders, potentially creating financial bubbles. More important than having a limited supply to preserve value is having a low risk of dramatic and unpredictable increases in new supply. And ether, for which the total supply is not capped, but annual supply growth is, meets this criterion.

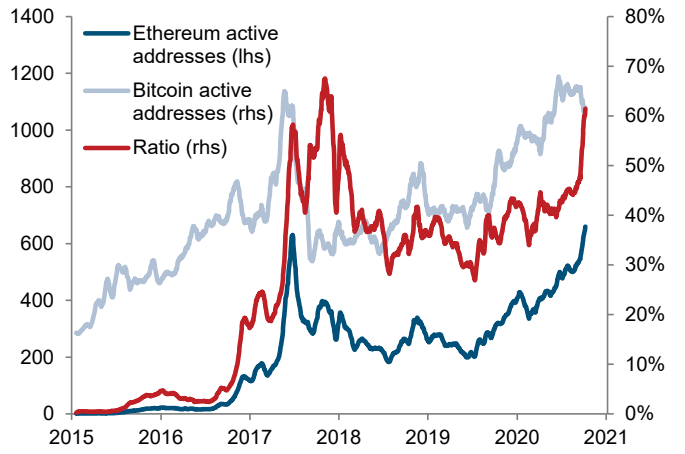
Fast-moving technologies break first-mover advantage

The most common argument in favor of bitcoin maintaining its dominance over other cryptocurrencies is its first-mover advantage and large user base. But history has shown that in an industry with fast-changing technology and growing demand, a first-mover advantage is difficult to maintain. If an incumbent fails to adjust to shifting consumer preferences or competitors' technological advances, they may lose their dominant position. Think of Myspace and Facebook, Netscape and Internet Explorer or Yahoo and Google.

For crypto networks themselves, active user numbers have been very volatile. During 2017/18, Ethereum was able to gain an active user base that was 80% the size of Bitcoin's within one year. Ethereum's governance structure, with a central developer team driving new proposals, may be best suited for today's dynamic environment in which crypto technology is changing rapidly and systems that fail to upgrade quickly can become obsolete.

Indeed, Ethereum is undergoing much more rapid upgrades to its protocol than Bitcoin. Namely, Ethereum is currently transitioning from a Proof of Work (PoW) to a Proof of Stake (PoS) verification method. Proof of Stake has the advantage of dramatically increasing the energy efficiency of the system as it rewards miners based on the amount of ether holdings they choose to stake rather than their processing capacity, which will end the electricity-burning race for miner rewards. Bitcoin's energy consumption is already the size of the Netherlands and could double if bitcoin prices rise to $100,000. This makes bitcoin investment challenging from an ESG perspective.

User base numbers remain highly volatile, meaning that leadership can change quickly



Source: Glassnode, Goldman Sachs GIR.

While PoS protocols raise security concerns due to the need for trusted supervisors in the verification process, Bitcoin is also not 100% secure. Four large Chinese mining pools control almost 60% of bitcoin supply and could in theory collude to verify a fake transaction. Ethereum too faces many risks and its ascendance to dominance is by no means guaranteed. For instance, if the Ethereum 2.0 upgrade is delayed, developers may choose to move to competing platforms. Equally, Bitcoin's usability can potentially be improved with the introduction of the Lightning Network, a change of protocol to support smart contracts and a shift to PoS. All cryptocurrencies remain in early days with fast-changing technology and volatile user bases.

High vol is here to stay until real use drives value

The key difference between the current rally in crypto and the crypto bull market of 2017/18 is the presence of institutional investors—a sign that financial markets are starting to embrace crypto assets. But bitcoin's volatility has remained persistently high, with prices falling 30% in one day in just this past week. Such volatility is unlikely to abate until bitcoin has an underlying real, economic use independent of price to smooth out periods of selling pressure. Indeed, more recently, institutional participation has slowed as reflected in lower inflows into crypto ETFs, while the outperformance of altcoins indicate that retail activity has once again taken center stage. This shift from institutional adoption to increasing retail speculation is creating a market that is increasingly comparable to that of 2017/18, increasing the risk of a material correction. Only real demand that solves an economic problem will end this volatility and usher in a new mature era for crypto—one based upon economics rather than upon speculation.

Mikhail Sprogis, Senior Commodities Strategist

Email: mikhail.sprogis@gs.com *Goldman Sachs and Co. LLC*
Tel: 44-20-7774-2535

Jeff Currie, Global Head of Commodities Research

Email: jeffrey.currie@gs.com *Goldman Sachs and Co. LLC*
Tel: 44-20-7552-7410

The role of crypto in balanced portfolios

Christian Mueller-Glissmann argues that the short and volatile history of bitcoin makes it difficult to assess how much of a beneficial role it could play in multi-asset portfolios

An important question both for asset allocators and for those assessing the prospect of further investor adoption of cryptocurrencies is how they fit into a multi-asset portfolio. In recent years, balanced portfolios have become imbalanced as low bond yields have provided less of a buffer against equity drawdowns and as the risk of rising inflation has grown. This has kicked off an intense search for alternative diversifiers that can help multi-asset portfolios buffer growth or rate shocks. But to add value from a portfolio perspective, an asset should offer an attractive risk/reward or low correlations with other assets, and preferably both. Over the last 35 years, bonds served this role as they delivered attractive risk-adjusted returns while being negatively correlated with equities.

With 20% ($14tn) of global debt offering negative yields, the hurdle rate for other assets to compete with bonds for the role of diversifier has declined. As a result, the lack of cash flow or yield from cryptocurrencies has become less of a concern, especially as the same is true for gold and most DM FX. And bitcoin, which was the first cryptocurrency and has the largest market cap today, has posted strong risk-adjusted returns mostly uncorrelated with traditional assets. But the history of bitcoin has been short and volatile—with a large proportion of that volatility idiosyncratic---making it difficult to assess how much of a beneficial role it could play in multi-asset portfolios. And institutional and other constraints remain headwinds for broader investor adoption.

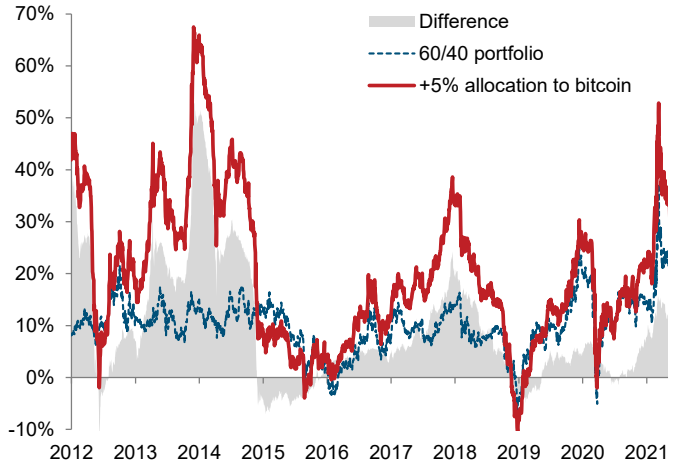
Small allocation, big impact

Just a small allocation to bitcoin in a standard US 60/40 portfolio would have enhanced risk-adjusted returns materially since 2014 (while bitcoin prices are available from mid-2010, we use prices since 2014 as bitcoin was not easily accessible to investors before then), even as balanced portfolios performed strongly on their own. Driving the enhanced performance was both higher risk-adjusted returns for bitcoin compared to the S&P 500 and US 10y bonds, despite much higher volatility, as well as diversification benefits from relatively low correlations between bitcoin and other assets.

However, bitcoin's strongest performance contribution to the portfolio resulted from isolated rallies in 2017, 2019 and last year, when it received a major boost from the COVID-19 crisis. Since 2014, bitcoin has actually often declined during equity drawdowns like in 2015, 2018 and 1Q20. These large drawdowns, combined with bitcoin's high volatility, have eventually outweighed the benefits of having it in a portfolio at higher allocations. Even with just a 5% allocation in a 60/40 portfolio, bitcoin drove roughly 20% of the portfolio's volatility, while US 10y bonds contributed only 2%. That is likely too much concentrated risk exposure for an institutional multi-asset portfolio, and such high volatility also limits the potential allocations from investors employing risk parity strategies or targeting a specific level of risk in the portfolio.

Strong performance during the rallies in 2017, 2019 and the COVID-19 crisis

One-year rolling return



Source: Bloomberg, Goldman Sachs GIR.

Untested correlations, high idiosyncratic risk

To assess the potential future diversification benefits of having bitcoin in their portfolios, investors need to understand the linkages between bitcoin and macro fundamentals, sentiment and other assets through the cycle. But bitcoin's history is too short to cover a full business cycle or a period of high inflationary pressures, so it is unclear how bitcoin would behave during a period of large growth and rate shocks. During the COVID-19 crisis, bitcoin became very correlated with other assets and turned out to be a highly levered bet on reflation.

A small allocation to bitcoin has enhanced a 60/40 portfolio in recent years

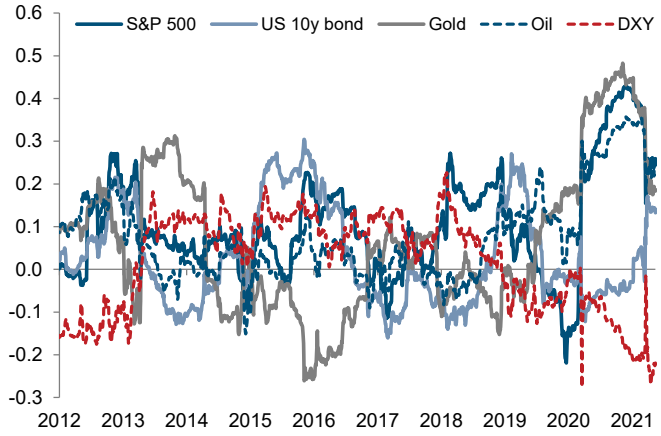
	S&P 500	US 10y bond	Bitcoin	60/40 portfolio	Allocation to bitcoin +2.5%	+5%	+10%	+20%
Since 2014								
Return p.a.	14%	4%	79%	10%	12%	14%	19%	27%
Volatility (daily)	18%	6%	73%	10%	10%	10%	12%	18%
Volatility (monthly)	15%	6%	87%	8%	9%	10%	13%	20%
Return/volatility	0.77	0.60	1.08	1.03	1.24	1.39	1.53	1.53
5% CVaR	-10%	-3%	-35%	-5%	-6%	-6%	-7%	-10%
Max drawdown	-34%	-11%	-83%	-18%	-19%	-19%	-20%	-29%
2014-2019								
Return p.a.	12%	4%	46%	9%	11%	12%	15%	21%
Volatility (daily)	13%	6%	74%	7%	7%	8%	10%	16%
Volatility (monthly)	11%	6%	87%	6%	7%	8%	11%	19%
Return/volatility	0.92	0.66	0.62	1.26	1.46	1.56	1.53	1.31
5% CVaR	-7%	-3%	-35%	-4%	-4%	-4%	-5%	-8%
Max drawdown	-19%	-11%	-83%	-11%	-11%	-12%	-18%	-29%

Source: Bloomberg, Goldman Sachs GIR.

Since the beginning of 2021, correlations with traditional assets have declined again, although bitcoin remains negatively correlated with the Dollar. While it's still too early to say for certain, this suggests that investors are treating bitcoin as a hedge against monetary debasement, similar to gold or real assets more broadly.

Low and unstable correlations between bitcoin and other assets, until recently

One-year rolling correlation, weekly changes

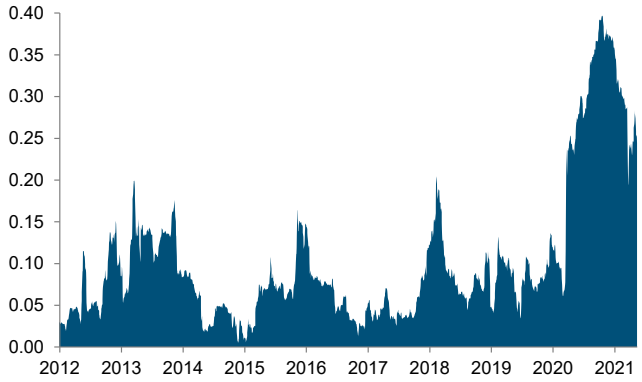


Source: Bloomberg, Goldman Sachs GIR.

Despite these correlations, most of the variation in bitcoin has been idiosyncratic. This could be good from a diversification perspective, but only if bitcoin were to have a positive expected return that is both predictable and attractive on a risk-adjusted basis. Given its limited and known supply, the price of bitcoin should primarily depend on investor demand and its perceived value. But investor demand so far seems to be linked to the asset itself rather than macro factors; adoption by retail investors—and recently some institutions—has boosted prices while regulatory and tax concerns—as well as positioning—have driven sharp setbacks. Without more clarity on these idiosyncratic drivers, assessing bitcoin's future risk/reward remains difficult.

Bitcoin has had high idiosyncratic risk since its inception

One-year rolling R-squared of a regression of bitcoin on S&P 500, US 10y bond, oil, gold, and DXY, weekly changes



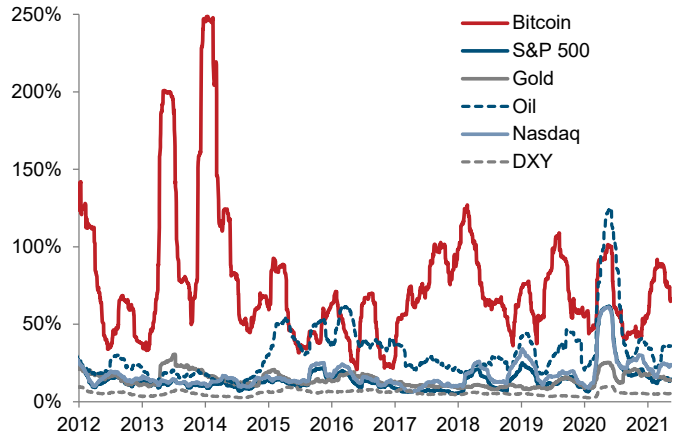
Source: Bloomberg, Goldman Sachs GIR.

High return, high risk during early adoption

Bitcoin's volatility has arguably been more stable than its correlations and returns, but at very high levels. While commodities in general tend to be more volatile than financial assets due to inelastic supply and oftentimes price-insensitive demand, bitcoin's price swings have been particularly extreme, with >50% drawdowns within a month and peak-to-trough declines of 80-90%. Just in 2021 alone, exceptionally large drawdowns have occurred in every month: -26% in January, -25% in February, -15% in March and -22% in April. But alongside that high risk, bitcoin delivered strong returns, with the price reaching all-time highs in April. Gold saw similarly high volatility and a sharp rally after the collapse of Bretton Woods in 1971. But once US private investors were allowed to get exposure to gold, first via certificates and then physically in the mid-1970s, volatility and returns eventually declined. The same might happen to cryptocurrencies if/when the market matures.

Bitcoin: not quite a safe haven

One-year rolling volatility, daily returns



Source: Bloomberg, Goldman Sachs GIR.

But, until then, the high and mostly idiosyncratic volatility of bitcoin can make it an unreliable macro hedge, especially over short time horizons, and increases the risk to balanced portfolios from market timing. In contrast to equities and bonds, bitcoin returns have also been more volatile on a monthly vs. daily basis, with both material and sustained drawdowns and rallies. With such volatile assets, more frequent rebalancing to return to target weights can increase drawdowns, as investors need to buy into a drawdown and sell during a rally. But less frequent rebalancing may introduce unintended market timing risks.

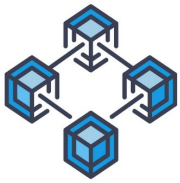
More headwinds from institutional constraints

Institutional asset allocators must also consider other factors when assessing potential bitcoin investments. First, the overall size and liquidity of cryptocurrencies is small; the market value of global financial assets (stocks and bonds) is roughly $200tn and the above-ground market value of gold is close to $11tn, while that of bitcoin is only $700bn. And with a multitude of other, smaller cryptocurrencies already in existence and many more that might be launched, picking the winning cryptocurrency is critical. Second, custody and counterparty risks can be difficult and costly to manage. And third, the potential for more regulation of the space, in part due to a lack of transparency and concerns over the carbon footprint of mining, creates significant uncertainty for investors. All of these factors may slow broad adoption from institutional investors.

Christian Mueller-Glissmann, Sr. Multi-Asset Strategist

Email: christian.mueller-glissmann@gs.com *Goldman Sachs and Co. LLC*
Tel: 44-20-7774-1714

Crypto's evolution in terms



Infrastructure layer

Distributed ledger

A database that is shared and synchronized across multiple sites and geographies by many participants. Each participant can access and own a copy of the ledger, and all changes to the ledger are visible to all participants. Distributed ledgers have no central authority; when a change is made to the ledger, a **consensus algorithm** is used to verify the change. Information on **blockchain**-based distributed ledgers is securely stored using cryptography and can be accessed using keys and signatures.

Blockchain

A blockchain is a type of **distributed ledger** that stores a list of records known as **blocks**. The Bitcoin blockchain was created by Satoshi Nakamoto in 2008 to solve the double-spend problem of decentralized systems—how to verify without a trusted central authority that the same coin was not spent twice—by using a "distributed timestamp server to generate computational proof of the chronological order of transactions."

Nodes

A computer that runs the blockchain software and transmits information across the blockchain network. Nodes are classified according to their roles: mining nodes add transactions to the blockchain through a **mining** process; full nodes hold and distribute copies of the ledger; super nodes connect full nodes to each other; light nodes are similar to full nodes but hold only a portion of the ledger.

Mining

The process of verifying and recording transactions on the blockchain via a consensus algorithm. Miners are rewarded in the form of a block reward. Bitcoin is a mineable **cryptocurrency**, but not all crypto currencies are mineable (see pg. 35 for more detail on bitcoin mining).

Forks

When blockchain nodes are not in agreement on a network's transaction history or rules around what makes a transaction valid, the blockchain may fork. Forks can happen by accident or intentionally. Soft forks are mostly accidental; there is still one blockchain as old nodes can continue to communicate with new nodes. Hard forks are intentional; the blockchain splits into two as old nodes cannot communicate with new nodes.

Protocol layer

Consensus algorithm

A mechanism by which all the nodes on a blockchain network reach a common agreement about the state of the distributed ledger. Various crypto networks use different consensus algorithms; the two most-recognized are **Proof of Work** and **Proof of Stake** (see pgs. 26-27 for more detail on which networks use which consensus algorithm).

Proof of Work (PoW)

Used by crypto networks like Bitcoin and Litecoin, PoW requires participant nodes to prove that a certain amount of computational effort has been expended. PoW requires a significant amount of computing resources.

Proof of Stake (PoS)

Currently used by crypto networks like Cardano and Polkadot, and planned for Ethereum in the future, PoS, unlike PoW, does not involve solving a mathematical puzzle to validate transactions. Instead, participant nodes must stake some amount of cryptocurrency if they want to validate. A random node is then selected as a validator based on how much cryptocurrency is staked, among other factors.

Services layer

Digital asset

An intangible asset created, traded, and stored digitally. Digital assets in the crypto ecosystem include **cryptocurrencies** and **crypto tokens**.

Crypto currencies

Native assets of a blockchain network that typically serve as mediums of exchange or stores of value. A cryptocurrency is issued directly by the blockchain protocol on which it runs.
They are typically decentralized, built on a blockchain, and secured using cryptography.
Cryptocurrencies include bitcoin and ether, the native asset of the Ethereum network, and **initial coin offerings**.

Crypto tokens

Unlike cryptocurrencies, which are native to a specific network, crypto tokens are created by platforms that build on top of other blockchains. For example, the tokens of Uniswap and Aave—UNI and AAVE—are built on the Ethereum network. Tokens can be used not only as mediums of exchange or stores of value, but also for governance decisions (e.g. voting on changes or upgrades to the protocol) or to access platform services.

The most widely used Ethereum tokens are ERC-20 for **fungible tokens** and ERC-721 for **non-fungible tokens.** They each specify how to build functional tokens for their respective uses.

Initial coin offering (ICO)

ICOs are a way for companies to raise capital. During an ICO, a company offers tokens to potential investors in exchange for fiat currency or established cryptocurrencies like bitcoin and ether to fund a project. The tokens are distributed via a blockchain network. One example of an ICO is Filecoin, launched in 2017 as a digital storage platform.

Tokens purchased in an ICO typically do not provide investors shares in the company, but rather grant access to the service or platform.

Smart contracts

Smart contracts are self-executing contracts with the terms of agreement between parties written directly into lines of code. Ethereum is the most popular blockchain for running smart contracts, which are typically written in the programming language **Solidity**.

Smart contracts are used by **decentralized applications** to connect to the blockchain.

Applications layer

Decentralized applications (dApps)

Digital applications that exist and run on decentralized blockchains rather than a centralized computer system. Most dApps are currently built on the Ethereum network.

dApps are used by a variety of industries, including finance as **decentralized finance** apps, gaming, and online gambling.

Decentralized finance (DeFi)

A blockchain-based form of finance that doesn't rely on centralized financial intermediaries like banks, brokerages, or exchanges. Instead, smart contracts are used to offer users traditional financial services like loans, derivatives, and insurance.

Similar to dApps, most DeFi applications are currently built on Ethereum.

Note: Not intended to provide an exhaustive list of terms for each layer.
Source: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", CoinDesk, Binance Academy, various news sources, Goldman Sachs GIR.

Interview with Mathew McDermott

Mathew McDermott is Global Head of Digital Assets at Goldman Sachs. Below, he discusses institutional interest in crypto assets, and Goldman Sachs' engagement in the space.

The interviewee is an employee of the Goldman Sachs Global Markets Division (GMD), not Goldman Sachs Research, and the views stated herein reflect those of the interviewee, not Goldman Sachs Research.

Allison Nathan: Goldman Sachs has had fits and starts in the crypto space. Why now for a new launch into the space?

Mathew McDermott: Client demand, pure and simple. When we originally explored creating our own digital custody offering and launching a crypto trading desk in 2017/2018, the price action was almost exclusively retail led. What's different today is the extent of institutional interest, coupled with very strong demand across the wealth management franchise. The product offering is broader as people are looking beyond bitcoin at the potential of the underlying blockchain infrastructure to transform the way markets behave. This has sparked interest in other kinds of cryptocurrencies—ether, dot, etc.—whose value proposition revolves more around what else can be done on blockchains. That, together with a more mature crypto market place with better risk management, execution, and digital custody, have all made it a bit easier for institutions to digest and access the market.

Allison Nathan: What's the nature of your conversations with institutional clients and their interest in the space?

Mathew McDermott: As a whole, discussions with institutional clients revolve around how they can learn more on the topic and get access to the space—as opposed to questions around what bitcoin or cryptocurrencies are—which was really the main topic just a few years ago. But beyond that, asset managers and macro funds are interested in whether or not crypto fits into their portfolios, and if it does, how to get access to either the physical—by trading the spot instrument on a blockchain—or exposure through other types of products, typically futures. Hedge funds, perhaps unsurprisingly, are more active in this space, and are particularly interested in profiting from the structural liquidity play inherent in the market—earning the basis between going long either the physical or an instrument that provides access on a spot basis to the underlying asset and shorting the future.

Corporate treasurers are interested in two slightly different questions. First, should they be investing in bitcoin on their balance sheets? Especially in places where firms face negative interest rates and fear asset devaluation amid the extraordinary amount of fiscal and monetary stimulus in the economy, having some portion of their balance sheet in bitcoin rather than paying to keep cash on deposit or holding negative yielding government bonds may make sense. And second, should bitcoin be considered a payment mechanism? I think that's a weaker argument given the inherent inefficiencies in the Bitcoin blockchain in terms of transaction speed. PayPal talks about allowing the use of bitcoin to pay for items, but behind the scenes a company called Paxos is actually converting bitcoin into fiat currency, which is then paid to merchants.

A portion of wealth management clients—high-net-worth individuals and family offices—are already very active in the space and in some sense are leading the way for other investors. They remain interested in bitcoin, but are also increasingly focused on the broader value that cryptocurrencies can bring. They're looking at ether in the context of the whole decentralized finance (DeFi) ecosystem and how that can really transform financial markets.

Allison Nathan: There seems to be a debate today about whether or not cryptocurrencies can be considered an asset class. Are clients are viewing it that way?

Mathew McDermott: Increasingly, yes. Bitcoin is now considered an investable asset. It has its own idiosyncratic risk, partly because it's still relatively new and going through an adoption phase. And it doesn't behave as one would intuitively expect relative to other assets given the analogy to digital gold; to date, it's tended to be more aligned with risk-on assets. But clients and beyond are largely treating it as a new asset class, which is notable—it's not often that we get to witness the emergence of a new asset class.

Allison Nathan: Are you observing FOMO-related pressure to invest given the extraordinary gains in crypto prices over the past year, and if so, are you concerned that price volatility will diminish client interest?

Mathew McDermott: There's no doubt that "fear of missing out" (FOMO) is playing a role given how much bitcoin and other crypto assets have appreciated and how many interested parties of all flavors have jumped into this space. If you're an asset manager or running a macro fund and your closest rivals are all investing and seeing material returns, your investors will naturally wonder why you are not investing. But I see investor interest in crypto enduring; we've crossed the Rubicon in terms of institutional buy-in, and there is much greater value in the space than there was three or four years ago.

Allison Nathan: Roughly what percentage of clients that you engage with are interested in the space versus actually active in the space?

Mathew McDermott: That is a good question. Last year we definitely saw many clients exploring rather than executing. From what we see and anecdotally hear that seems to be changing. A survey from our Digital Asset team conducted in early March found that of the 280 clients that responded, 40% have exposure in some form to cryptocurrencies, with 61% expecting their holdings to increase over the next 12 months, and I suspect that would be more now. Another indicator of increased activity is the almost 900% yoy increase in CME bitcoin future daily activity in April.

Allison Nathan: Goldman Sachs itself is only engaging in the space in a relatively limited way. Why is that?

Mathew McDermott: It's true that we are in early days of our engagement and the regulatory landscape remains in flux, so we're only just starting to offer our clients access to the crypto space. We're currently transacting non-deliverable forwards, which we cash settle, and CME futures on bitcoin and ether, the latter on an agency basis for now. To help facilitate client transactions, we expect to trade the bitcoin CME future and certain pre-agreed upon bitcoin-linked securities on a principal basis in the near future. From a prime brokerage perspective, we plan to offer clients the ability to go synthetically long/short bitcoin-linked securities and exchange-traded notes (ETNs) in Europe. We're also looking into offering lending structures in and around the crypto space to corporate clients as well as structured notes. And from a wealth management perspective, we are gearing up to offer access to cryptocurrencies, specifically bitcoin, via fund or structured note-like products.

Allison Nathan: How would you rate the liquidity of the products that we trade today?

Mathew McDermott: Liquidity has increased dramatically over the past year. Between April 2020 and April 2021, daily bitcoin dollar spot volume increased from ~$300mn to ~$1.5bn, and daily CME bitcoin futures volume grew from ~$200mn to close to ~$2bn. That's a very clear indication of the inflow of institutional demand into this market, which has only just begun. But even though liquidity has increased, it's still difficult for institutions to gain access to the market, which remains quite fragmented. That fragmentation is driving the basis that I mentioned between going long the physical and shorting the future that hedge funds are picking up. And that basis has fluctuated considerably over the last three to six months.

Allison Nathan: Beyond ease of access considerations, what are some of the custodial/security challenges institutions face when transacting in the crypto space today, and how have these evolved?

Mathew McDermott: Digital custody is very different from traditional custody in terms of the risks associated with cryptography, public and private keys, etc. But institutions have gotten more comfortable with these risks over the last several years, for two reasons. One, market participants within the crypto space are more institutional-grade today as entities and in terms of their offerings—custodial offerings are a lot more secure and execution and risk management have improved considerably. Many of these entities are now raising capital in the public markets, both to further institutionalize their offerings and credentialize their activities. And two, the quality of custody both in terms of the technology itself as well as the products around it have evolved with the market. Security around cold storage—where the preponderance of institutional assets sits—has fundamentally improved; multi-signature options are available, the private key can be sharded, etc. And insurance offerings associated with hot storage, which is more vulnerable to theft, have also grown, reflecting the greater confidence from an insurers' perspective. All of that has helped institutions feel more comfortable participating in the crypto market.

Allison Nathan: What are you hearing from clients are their biggest constraints to increased involvement in crypto?

Mathew McDermott: There are three key constraints. The first is mandate limitations. For corporates, increased involvement often depends on whether their board feels such involvement makes sense given the nature of the company and its objectives. And some investment funds and asset managers don't have the authority to invest a portion of their portfolios in crypto. The second constraint is the ease of access that I mentioned: how easily can clients gain exposure to the market, is the liquidity sufficient to meet their needs, and are they comfortable enough with the custody and security aspects of managing these assets? And the third constraint, perhaps more philosophical, is whether having crypto exposure is the right thing to do and makes sense for their portfolios, balance sheets, etc. But as evidenced by the increased inflows, more and more entities are becoming comfortable with having some exposure to the crypto space.

Allison Nathan: Do you hear concerns from investors about the environmental footprint of proof of work crypto assets like bitcoin, especially given increased investor focus on ESG today?

Mathew McDermott: A number of potential investors have voiced concerns and understandably want to delve more into that aspect of crypto assets and really understand it. Generally, the environmental concerns have not caused investors to fully close the door, but they are looking at improved sustainability options. Investors are intrigued to hear about miners leveraging renewable energy sources to mine crypto assets. And carbon neutral funds are emerging, that, for example, calculate the carbon cost of crypto mining, and buy credits to offset their environmental impact.

Allison Nathan: What risks worry you the most as we and our clients increase engagement in the space?

Mathew McDermott: A key concern is inconsistent regulatory actions around the globe that impede the further development of the crypto space, or the ability of more regulated entities to engage within it. It feels like the regulatory tone has turned more constructive, but I certainly wouldn't want to be complacent. And the other major concern is fraud, both in terms of storage and nefarious activity on the blockchain. Particularly as it relates to hot storage, we're only one big fraud away from a very negative impact on the market. But it's reassuring to watch large crypto companies with significant increases in assets under management actually manage that growth without any noticeable increase in fraudulent activity.

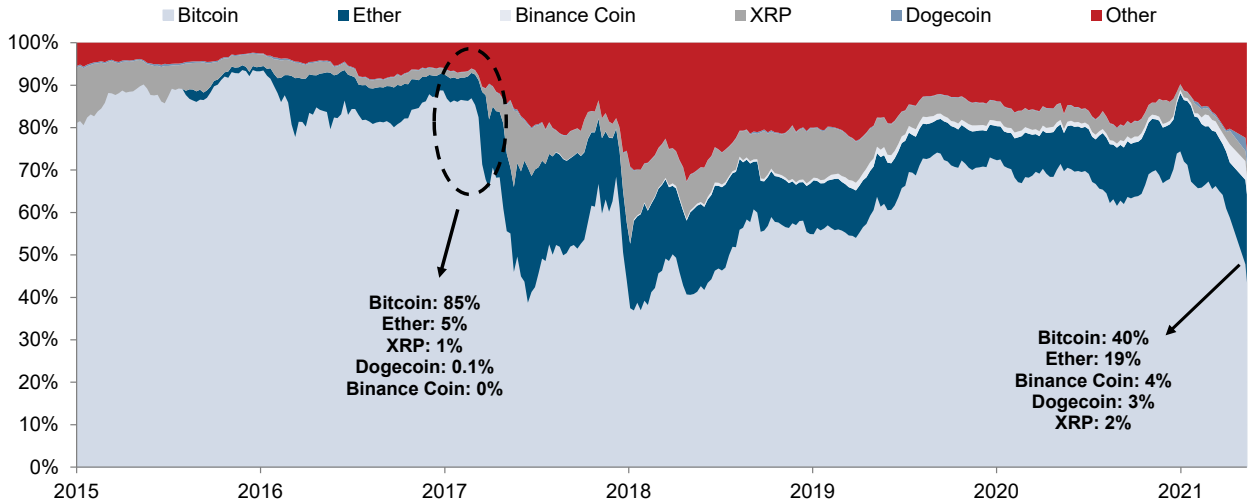
Top coins and tokens

Name/ Market cap	Function	Established	Background/Objectives	Current/ Maximum supply	Consensus mechanism
Bitcoin (BTC) **$700bn**	Currency	2009	The first cryptocurrency, established to allow peer-to-peer transactions without the need for a trusted third party. Transactions are verified by network nodes and recorded on the blockchain.	18.7mn/ 21mn	Proof of work (one party proves to the other that a certain amount of computational effort has been expended)
Ethereum (ETH) **$285bn**	Smart contract application platform	2015	The most actively used blockchain, established to enable the creation and use of smart contracts and decentralized applications. Ether is Ethereum's native cryptocurrency.	115.9mn/ unlimited	Currently proof of work, but moving to proof of stake
Tether (USDT) **$58bn**	Stablecoin	2014	Originally designed as a stablecoin—aiming to be fully backed by a fiat currency—it was later found that each tether was not fully backed by US Dollars at all times.	58bn/ unlimited	N/A; USDT tokens run on the Algorand, BCH, EOS, Ethereum, Liquid Network, Omni, Solana, Tron blockchains
Binance Coin (BNB) **$52bn**	Currency/ application/ utility	2017	Issued by the Binance cryptocurrency exchange, Binance Coin is used to pay for fees on the exchange. While it originally operated on the Ethereum blockchain, BNB had its own mainnet[1] launch in 2019.	153.4mn/ 170.5mn	Proof of stake (randomly assigns the node that will mine/validate, partially according to the number of coins a node stakes)
Cardano (ADA) **$47bn**	Smart contract application platform	2017	Cardano is a public blockchain established to enable the creation and use of smart contracts while focusing on scalability and interoperability. Ada is Cardano's internal cryptocurrency.	31.9bn/ 45bn	Proof of stake
Dogecoin (DOGE) **$43bn**	Currency	2013	Named after the Shiba Inu meme and created as a "fun" alternative to bitcoin, dogecoin is a peer-to-peer, open-source cryptocurrency. Dogecoin is a fork of the luckycoin blockchain.	130bn/ unlimited	Proof of work
XRP **$38bn**	Currency	2012	XRP is a real-time settlement system, exchange, and remittance network that facilitates cross-border payments for financial institutions.	46bn/ 100bn	A network of servers validates transactions through a custom consensus algorithm
Polkadot (DOT) **$24bn**	Smart contract application platform	2017	Polkadot is designed to provide interoperability between other blockchains. Polkadot features "shared security"—developers can create their own blockchains on the system while still having access to Polkadot's security.	939mn/ unlimited	Proof of stake
Internet Computer (ICP) **$15bn**	Smart contract/data platform	2021	Internet Computer is a public blockchain that extends the functionality of the public internet to allow it to host back-end software. This enables developers to create websites, enterprise IT systems and internet services by installing code directly onto the public internet, bypassing server computers and commercial cloud services. ICP is Internet Computer's utility and governance token.	124mn/ unlimited	Independent data centers operate standardized computer nodes, and are rewarded for the time that they correctly operate these nodes (currently 48 data centers run 1,300 nodes)

[1] A testnet is used by developers to test and troubleshoot all the features of a blockchain network. After a successful testnet, a mainnet version of the blockchain is launched, and all transactions are broadcast, verified, and recorded. The mainnet phase also sees the deployment of a native token rather than the previously issued Ethereum-based token, which is swapped for the new token during a process known as the mainnet swap.

Name/ Market cap	Function	Established	Background/Objectives	Current/ Maximum supply	Consensus mechanism
USD Coin (USDC) **$14bn**	Stablecoin	2018	USDC is a stablecoin running on the Ethereum, Stellar, Algorand and Solana blockchains. USDC is fully backed by the US Dollar, with Centre—the consortium that mints USDC—holding $1 for every coin in reserves.	14.4bn/ unlimited	N/A; USDC tokens run on the Ethereum, Stellar, Algorand, and Solana blockchains
Bitcoin Cash (BCH) **$13bn**	Currency	2017	Another fork of Bitcoin, bitcoin cash was created to facilitate the use of BTC as a medium of exchange rather than the original store of value purpose. BCH does this by increasing the speed at which transactions are processed via larger blocks.	18.7mn/ 21mn	Proof of work
Uniswap (UNI) **$13bn**	Governance token	2018	Uniswap is a decentralized finance (DeFi) platform running on the Ethereum blockchain on which users trade cryptocurrencies and tokens. UNI is the platform's governance token, giving users the right to vote on new developments and platform changes.	565mn/ 1bn	N/A; UNI tokens run on the Ethereum blockchain
Litecoin (LTC) **$13bn**	Currency	2011	A fork of Bitcoin, Litecoin was created with the goal of speeding up transaction times, which it achieves by utilizing a different cryptographic algorithm than BTC.	67mn/ 84mn	Proof of work
Aave (AAVE) **$5bn**	Governance token	2017	Aave is a decentralized non-custodial money market platform that allows users to lend and borrow crypto assets. AAVE is the Ethereum-based, native governance token of the platform.	12.8mn/ 16mn	N/A; AAVE tokens run on the Ethereum blockchain
Monero (XMR) **$4bn**	Privacy currency	2014	A privacy-focused cryptocurrency, Monero aims to make transactions untraceable and unlinkable through the use of ring signatures and stealth addresses.	17.9mn/ 18.4mn	Proof of work
Algorand (ALGO) **$3bn**	Smart contract application platform	2017	Algorand is a blockchain built by MIT professor Silvio Micali that supports DeFi applications and smart contracts, built on scalability as its most important principle, but also on open participation, security, and transaction finality.	3bn/ 10bn	Proof of stake

Bitcoin's market cap has fallen over time as new coins have gained market share



Note: Table does not constitute an exhaustive list of all cryptocurrencies/altcoins/tokens; data as of May 19, 2021.
Source: Underlying whitepapers, Coinbase, CoinDesk, CoinMarketCap, various news sources, Goldman Sachs GIR.

Interview with Alan Cohen

Alan Cohen served as Senior Policy Advisor to former SEC Chairman Jay Clayton from 2017 to 2021, and was the Global Head of Compliance at Goldman Sachs from 2004 to 2017. Below, he discusses the current state of cryptocurrency regulation in the US.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: How do regulators treat crypto assets today—as securities, commodities, currencies, or something else?

Alan Cohen: No single US regulator oversees all aspects of crypto assets. Different regulators are focused on different applications and functions of blockchain technology. For example, if the financial institution that is acting as a custodian of a cryptocurrency is a bank, then the relevant banking regulator—the Office of the Comptroller of the Currency (OCC), the Fed, or the FDIC—will issue rules or guidance on how that custody function should be performed. The OCC did just that in late 2020, authorizing regulated banks to participate in certain blockchain nodes, to custody client cryptocurrency assets and to facilitate cryptocurrency payments. It makes sense that banking regulators would prescribe how regulated banks under their supervision should address this class of assets.

Allison Nathan: How focused are regulators on cryptocurrencies today, and what areas are they most focused on?

Alan Cohen: The SEC and other US financial regulators are increasingly focused on cryptocurrencies and blockchain technology as the space continues to evolve. Regulatory activity will almost certainly focus on three main areas in which crypto assets have the potential for greatest market penetration and disruption—application of distributed ledger technology (DLT) to facilitate financial transactions, the use of crypto assets and the blockchain to make payments, and investing in crypto assets as a store of value. Many companies have sought to deploy DLT that allows parties to record, track, verify and store transactions of value, e.g., financial and real estate transactions, without the need for a trusted intermediary to verify the transaction, and in a way in which the stored information is impervious to tampering or destruction.

The application of DLT to highly regulated activities in financial transactions is still in its infancy, with both large and small players developing solutions and applications. For example, in the area of securities transactions, firms are undertaking the digitization or tokenization of shares or other securities of companies, the trading of those digital securities, the clearing and settlement of those transactions, and the recording of those transactions and the ownership of assets—to name just a few applications. Insofar as these innovations will perform highly regulated market functions, the regulators in those areas—such as the SEC in the previous examples—will need to consider whether existing regulations are sufficient to cover these new applications or whether new rules are required. An example of this type of review was the recent SEC guidance on how broker-dealers could custody digital assets, which has enabled greater custody of digital assets by registered broker-dealers.

A second major area of regulatory focus is the application of blockchain technology to fiat currency and the global payments system, which appears to be heading toward a new digital era. On the global stage, the Financial Stability Board (FSB)—comprised of G20 Finance Ministers, central banks, the Bank for International Settlements (BIS) and other international organizations and global standard-setting bodies—is hard at work on an overhaul of the global payments system that will likely embrace crypto assets in the form of fiat digital currency. That new system will replace or supplement the existing SWIFT system that has been the backbone of the global bank-to-bank payments system for decades. These digital currencies are likely to be in the form of sovereign fiat currencies, e.g., a digital dollar, euro or yuan. Of course, China has already begun to implement a digital yuan domestically, which will give its government more control of and transparency into the use of its currency in China. This has set off a global race to adopt fiat currency in digital form. Various European countries have begun to investigate their own digital currencies and the US Treasury and the Fed have announced that they are studying the possibility of a digital dollar.

The implication of fiat digital currencies for existing cryptocurrencies is unclear. But let's not forget the old adage, "Don't bet against the Fed." You might modify that to say: "Don't bet against the central banks of the world" to relinquish control over their money supply and currency. The evolving regulation of stablecoins—digital assets designed to track an underlying fiat currency or basket of such currencies—provides some insight into the future of cryptocurrency regulation in the US and elsewhere. In an October 2020 FSB Report, the first recommendation tells you all you need to know: "Authorities should have and utilize the necessary powers and tools… to comprehensively regulate, supervise and oversee a [global stablecoins] arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively." That was followed in December 2020 by a statement released in the US by the President's Working Group on Financial Markets, which is composed of the leading federal financial regulators, encouraging innovation. But the statement went on to make clear that (1) stablecoins must comply with applicable US legal, regulatory and oversight requirements; and (2) stablecoin participants and arrangements must meet all applicable anti-money laundering (AML) and counter-terrorist financing and sanctions obligations before bringing them to market.

A proposed set of regulations was also issued by FinCEN in December 2020, which the Biden administration will need to finalize. The proposed regulations are designed to ensure that transactions in cryptocurrency are broadly subject to the same AML and related controls as other forms of payment. Those regulations are entirely consistent with the Financial Action Task Force (FATF) standards applied broadly across the globe to prevent AML and terrorist financing. It's difficult to imagine that cryptocurrencies in whatever form will not be subject to those

same requirements. Financial regulators spent decades doing away with bearer bonds because of the AML, fraud and tax evasion risks posed by the instrument, and it's unlikely that global regulators will permit cryptocurrencies to take their place in the global financial system. The bottom line is that the anonymity promised by some crypto assets will inevitably meet intense regulatory opposition. The third main area of regulatory focus is cryptocurrencies as a store of value, as an increasing number of institutional and retail investors are focused on investing in cryptocurrencies as an asset class with growth potential. Regulators and investors want markets that are transparent, fair and well regulated. But a very significant percentage of trades—some claim in excess of 90% of all trades—in these assets takes place on markets that are not transparent or regulated in a manner consistent with global market regulatory standards. The notorious instances of clients losing their money when brokers were hacked, custodians disappeared, or market prices were allegedly manipulated partly reflect this lack of regulation. This dearth of regulation will likely remain a key challenge for the cryptocurrency ecosystem.

Allison Nathan: Given these different areas of regulatory focus, which crypto assets is the SEC focused on?

Alan Cohen: The SEC is focused on crypto assets that are, in effect, securities. In the period between 2017 and 2020, the SEC was very active in pursuing securities fraud and other types of cases against Initial Coin Offerings (ICOs) that were securities masquerading as currencies or commodities. If an offering is a security, then the offering must be done pursuant to the Securities Act of 1933 and trading must occur in a manner permitted under the Securities Exchange Act of 1934, or under exemption to the requirements under those Acts.

Allison Nathan: How does the SEC decide if a crypto asset is a security?

Alan Cohen: The SEC's Decentralized Autonomous Organization (DAO) Report discusses the elements that the SEC considers in deciding whether a digital offering is a security. As outlined in that report and in subsequent SEC cases, the SEC applies a test set forth in a Supreme Court case, the so-called Howey test, to determine if the offering is a security. Among other factors, Howey test elements include (1) investment of money, (2) in a common enterprise, and (3) with a reasonable expectation of profits derived from the efforts of others. With this in mind, we can distinguish between three types of crypto assets: asset or equity tokens, which represent a claim on an issuer, tokens that are meant as a means of payment or exchange, such as bitcoin, and utility tokens that represent a right to have access to some digital application or service. The first group is considered a security, while the second and third groups generally are not viewed as securities. SEC officials have publicly stated that Bitcoin and Ethereum are sufficiently decentralized networks that neither bitcoin nor ether are securities. And the SEC established the Strategic Hub for Innovation and Financial Technology to foster innovation in DLT, including by providing clear guidance that utility tokens are not securities.

Allison Nathan: What if the SEC finds that an ICO should have been registered as a security and was not?

Alan Cohen: Under US securities laws, a sale of a security confers certain rights to the buyer—including the right to get their money back, a so-called "right of rescission"—in the event that a securities offering should have been registered and was not—as was the case with some ICOs—or if there was fraud in connection with that offering. Two recent cases illustrate that the sale of unregistered securities to investors can have serious consequences for issuers. The SEC successfully sued Telegram, alleging that Grams were unregistered securities. The court agreed, and Telegram had to return the money from the sale of Grams to its investors. In another case, the SEC sued Kik Interactive over its offering of a "Kin" token, which the court preliminarily agreed was a security. There is also a pending case brought by the SEC against Ripple Labs, Inc. and others over its sale of XRP on the same theory. That's a case worth watching.

Allison Nathan: What will it take for the SEC to approve a cryptocurrency ETF?

Alan Cohen: A number of firms have announced their intention to offer such a product. The SEC's mission to protect investors, maintain fair, orderly and efficient markets, and to facilitate capital formation will be sharply in focus as regulators assess whether a cryptocurrency ETF should be approved. Indeed, a prerequisite, among other things, for a cryptocurrency ETF will be that regulators and investors are satisfied that underlying market prices are fair, accurate, and transparent. And the recent bout of volatility doesn't provide much comfort in this regard.

Allison Nathan: If bitcoin and ether are not securities, does that mean that the CFTC regulates trading in them?

Alan Cohen: Not exactly. The mission of the CFTC is "to promote the integrity, resilience, and vibrancy of the US derivatives markets through sound regulation." That means that the CFTC regulates the derivatives market, but does not directly regulate the underlying market. The CFTC regulates trading in the CME-listed bitcoin and ether futures contracts. In certain instances, it will look through to trading in the underlying market insofar as it impacts the futures market. But it does not regulate that underlying market.

Allison Nathan: Do states regulate the underlying market?

Alan Cohen: New York has been one of the most active states in this space. In 2015, the New York State Department of Financial Services issued regulation for a "BitLicense," which allows firms to create, issue, transact, and custody virtual currencies. The purpose of the license is to regulate what it calls "Virtual Currency Business Activity". New York and other states, including Utah, have also amended their banking or trust laws in an effort to foster innovation and capture a share of the future revenue stream associated with this activity.

Allison Nathan: Shouldn't there be a single federal agency responsible for the regulation of cryptocurrencies?

Alan Cohen: Not necessarily. What is required is close coordination with and on the federal level and among international standard-setting bodies—the FSB, BIS, International Organization of Securities Commissions (IOSCO) and others. Because of the multitude of applications of blockchain technology across the spectrum of financial transactions—from banking to securities markets to payments to investing—the relevant federal authorities that oversee those markets are best able to assess the benefits and the risks of this technology in those regulated areas.

Interview with Dan Guido

Dan Guido is Co-Founder and CEO of Trail of Bits, a software security research and development firm specializing in blockchain software and cryptography. Below, he discusses security risks inherent in cryptocurrency blockchains, as well as in smart contracts.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: How secure is the blockchain that underlies bitcoin and other cryptocurrencies?

Dan Guido: There are two main facets of blockchain security: the security of the software and the security of how the distributed network is run. Nobody would expect that software written in C++ with its own custom network protocol running on globally distributed machines that provides millions—if not billions—of dollars for a successful hack would be secure, but most of the software running cryptocurrency networks is generally fairly safe. And we know that because, at least for Bitcoin, the software is relatively mature, so a lot of eyes have been prying into it for a long time, and we have actually done source code audits on much of it. But we also know that because there's a massive reward for not being secure, which no one has reaped. That being said, I would not be surprised if a high severity vulnerability in Bitcoin software was revealed tomorrow. But relative to other blockchain software, it is relatively safe.

Beyond the software itself is the fact that the blockchains that underlie Bitcoin, Ethereum and other crypto networks have no central authority that controls them. Volunteers run nodes—entities that come to a distributed consensus—that accept transactions and attempt to get them incorporated into the blockchain. And then miners compete against each other to construct new blocks on the blockchain. The incentives in that distributed protocol are interesting and sensitive.

People commonly discount the risk of an adversarial network attack on a cryptocurrency blockchain, believing that everyone on a blockchain has an economic incentive to keep it going—that there's more money in a network that's running than in a network that's not. But there have been attacks on blockchains, and it's possible that certain chain forks attributed to bugs in a consensus protocol were actually deliberately triggered by attackers. We need to remember that some bad actors just want to see the world burn. And current state-level efforts in China and other countries to implement a nationally anointed cryptocurrency make me wonder if public blockchains may become persona non grata in those countries, opening the floodgates for adversarial network attacks by foreign nation-states with the resources to pull them off.

Allison Nathan: What form would such an attack take, and how difficult would it be for a bad actor to execute one?

Dan Guido: An oft-discussed threat is the so-called 51% attack in which a single entity gains control over 51% or more of the mining power in the world, allowing it to invalidate the immutability properties of the blockchain to rewrite history or cause what's called a double-spend: Suppose Alice tries to give Bob and Eve one bitcoin each, but Alice has only one bitcoin. If those two transactions are submitted to the blockchain at the same time, it's almost arbitrary which one will be executed first, but the one executed second will fail. Someone with 51% control of the network can make them both succeed. It's almost impossible to know for certain where miners are located geographically, but there's evidence that a significant portion of them are concentrated in China, likely due to energy resource availability; several weeks ago, a gas explosion and flood in a coal mine in the Xinjiang region led the Chinese government to shut down all the neighboring cryptocurrency mining farms to conduct fire safety inspections. That was the morning of April 16, and by the end of the day, Bitcoin's global hash rate had dropped by 50%.

But even with less than 51% of the mining power, bad actors with control over a majority of a blockchain's nodes can still conduct nefarious activities like denying service to specific users. For example, a nation-state could use their nationwide firewall to block all traffic for a specific Bitcoin address. Importantly, if someone were to manipulate the network in such a way, it could be done so subtly that detecting it would be almost impossible.

Allison Nathan: Have any bad state actors tried to engage in that type of activity?

Dan Guido: To my knowledge, there is no evidence that any state actor has directly targeted the stability of the network, although significant nation-state activity has occurred on cryptocurrencies themselves. Russia has heavily used cryptocurrencies over the last few years. North Korea has mostly focused on attacking endpoints like exchanges and digital wallets. But non-nation-state bad actors have attempted to financially manipulate the network to gain an edge on specific epochs of time to sneak a transaction in and somehow benefit. That's occurring particularly on the Ethereum network, where many decentralized finance (DeFi) and other activities amenable to exploitation are located.

Allison Nathan: So how can institutional investors getting involved in the space safely engage in it?

Dan Guido: Two important ways: through safe exchanges and safe interactions with an exchange. There's a mantra in some parts of the blockchain industry, "not my keys, not my bitcoin", which essentially advocates taking your private keys—and, thus, your bitcoin—shoving them under your mattress, and hoping they don't get stolen. That's a bad idea. Institutions and people more broadly should be storing their cryptocurrencies on a reputable exchange. But the security of an exchange is not obvious from the outside. Exchanges exist today that have no business being exchanges, operating in unregulated markets or as pure crypto exchanges without any exposure to fiat currency to avoid regulation. Just last month, the CEO of a Turkish cryptocurrency exchange allegedly stole $2 billion from the exchange's users. And riff-raff in the space just flying by the seat of their pants and getting hacked is prevalent. But the top 10% of centralized exchanges probably have enough resources

and maturity to have invested in their own security well enough to protect users' investments. They generally also have ways to architect their internal systems through a segregation of resources, key management, and fund movement processes such that a potential compromise of the exchange wouldn't be catastrophic. And some of them have built checks into their user interfaces to ensure money isn't being sent to a null address—which would prevent the funds from ever being accessed again—due to something like a fat-finger mistake.

But the other point of vulnerability is the device used to interact with the exchange. Setting up a high-risk machine like an iPad or Chromebook that is used only to interact with an exchange instead of a general-purpose machine is generally the safest route to take. As long as you're doing that, the likelihood of your computer being infected with surreptitious malware or ransomware that will steal your cryptocurrency is pretty low. And that's important because once those funds are gone, they're unrecoverable.

Allison Nathan: Why are they unrecoverable if all the activity on public blockchains is transparent?

Dan Guido: It's true that you can see exactly where the cryptocurrency went, but it's difficult to map that to the point at which a human connects to the blockchain. Funds can also be laundered through different blockchains, and services like tumblers and those that use zero-knowledge proofs can help obfuscate where the cryptocurrency came from. And even if you know exactly who perpetrated the crime, if they're in a different jurisdiction you may have no legal recourse.

Allison Nathan: How much of a risk does quantum computing—which could make current encryption obsolete—pose to blockchains?

Dan Guido: I'm not currently worried about that risk, both because there are more significant use cases for quantum computing than breaking Bitcoin's cryptography and because technologically, we're not there yet. In order to break crypto with a quantum computer, you would need a computer much larger than what exists today. And even though quantum computers have been demonstrated to work on a small scale, as the number of qubits scales up, more noise is introduced into these systems, which prohibits them from running computations. So quantum computers have significant fundamental problems to overcome before they can reach the scale and size capable of impacting crypto in any meaningful way.

By the time that quantum computers do become usable for real work, we'll likely have a really solid, well-reviewed suite of cryptography algorithms to rely on. Some quantum-resistant algorithms have already been submitted to the National Institutes of Standards and Technology (NIST) as potentially the next big standard, although one of them was broken by high schoolers on the back of a napkin. So they've not yet been proven to work, and their trade-offs and weaknesses are unclear. But we will likely have reliable quantum-resistant algorithms within the next five years, and as an industry we'll have a 10, 15, or 20-year head start on implementing those algorithms. Quantum computing is the slowest-moving problem in computer security today; we're going to see it coming from a thousand yards away.

Allison Nathan: How secure are today's smart contracts?

Dan Guido: We frequently find vulnerabilities in the smart contracts we review. A few months ago we ran Slither—a tool we developed to detect vulnerabilities in smart contracts—on 2,000 new contracts posted to the Ethereum blockchain over a nine-day period. About half of them had known vulnerabilities. Of those, on average, each contract had ten known vulnerable patterns and at least one high severity vulnerability. That's the consequence of having tools that are really difficult to build secure software with. It's a wild west out there for developers building applications on the blockchain. Solidity—the language being used—has dozens of different foot guns and opportunities for failure. Developers are generally on their own using stone tools to cobble together houses built of balsa wood and cardboard and trying to scale them up to 20 stories high in a neighborhood that constantly gets lit on fire.

That said, a few firms made early investments in software testing tools that allow them to apply techniques like symbolic execution, abstract interpretation, and security property testing, and have produced highly reliable software capable of managing billions of dollars. But a huge amount of churn exists at the bottom of the market where companies have no access to expertise and no experience of their own, and many end up deploying software that explodes in their faces almost immediately. And even systems that pass formal security evaluations aren't necessarily secure. Only about half the bugs we find in our security reviews are amenable to being formally proven. Proving the other half requires a human brain, because they're logical in nature, deal with interactions between the system and the world at large, or just can't be modeled with a machine. So a tremendous amount of risk remains, even when everything is done right on the code security level.

Allison Nathan: So what worries you most about the underlying technology and infrastructure of the crypto space?

Dan Guido: Smart contracts concern me because the potential for one incident to affect the entire industry is really large. It's akin to being an insurance provider in a world where every house is built on the beach in Florida. And it's also important to recognize that very few DeFi systems are truly decentralized; almost all of them have a centralized backdoor or a set of private keys that allow the owner to manipulate account balances or the functionality or state of the system. So the systems are not trustless, even though they're advertised that way, making it necessary to have trust in the company that deploys the smart contract and the security assessments it utilizes. It's not enough that an external security firm produced a report; a company may have hired the firm only to do a week-long assessment when the project's size requires an eight-week assessment. As a result, the security firm will likely have missed something.

And even when secure code is deployed, if the functionality of the underlying blockchain has changed—which, for example, happens every few months on the Ethereum blockchain as it forks—that may inadvertently make existing contracts insecure. So a preponderance of evidence is needed to assess security. That means having an educated team with industry experience, security standards, authentication systems, key management, and regular external security reviews. A single data point isn't enough; security needs to be thought about holistically.

Interview with Michael Gronager

Michael Gronager is Co-Founder and CEO of Chainalysis, a leading blockchain data, investigations, and compliance company, and was a co-founder of the cryptocurrency exchange Kraken. Below, he discusses the extent to which bitcoin and other cryptocurrencies facilitate illicit activity.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: Cryptocurrency transactions are commonly perceived to be associated with illicit activity. What does your analysis suggest?

Michael Gronager: Cryptocurrencies are by design permissionless value transfer networks that enable anyone in the world to access and transfer funds. In the early days of cryptocurrencies, this ease of access created a perception that they were an anonymous global money system everyone could use, which attracted interest from criminals. But the interesting thing about blockchain is that every single transaction is public, immutable and never disappears. This visibility has enabled us to create a map of the entire crypto network based on every transaction on the blockchain which, combined with intelligence from the public and private sectors, provides a fairly comprehensive view of the entire crypto ecosystem. By using this map, and looking at different patterns of behavior and the entities involved in transactions, we can track the amount of funds that are being used for various purposes, including legitimate investment and illicit activity. Our analysis shows that in 2020 total illicit activity accounted for around 0.34% of all crypto transactions. That's down from around 2% of all transactions in 2019, much of which was dominated by a single large Ponzi scheme. Scams are a major use case among criminals that abuse crypto. So a very small share of all crypto transactions today are illicit, which is quite different from the general perception that cryptocurrency activity is dominated by criminals.

Allison Nathan: How certain can you be of the accuracy of these figures?

Michael Gronager: We are very confident in what we know, as we have a very rigorous, high bar for attributing services to blockchain activity. While it's true that we don't necessarily know every entity on the blockchain—especially the smaller ones—the combination of our machine learning and collaboration with customers and partners gives me confidence that we have accurate estimates.

Allison Nathan: How do you identify an illicit transaction?

Michael Gronager: The map that we've created is basically a map of every entity that transacts on the blockchain, including exchanges such as Binance in Asia and Bitstamp in Europe, blockchain service providers like BlockFi, gaming sites, payment providers, and even Tesla, which accepts bitcoin for vehicle purchases. By identifying certain entities that provide illicit services, it's possible to track all of the activity that touches those entities via the blockchain. Further, most legitimate entities typically check the identity of their customers. For example, when a customer opens an account with a regulated bitcoin exchange in the US, they have to identify themselves in the same way as when opening a bank account. This usually includes a thorough "know your customer" (KYC) process. What KYC entails is not always standardized, and it could involve everything from requiring a customer to upload their passport to jumping on a video call to confirm their identity. For smaller transactions, KYC rules might only involve confirming a person's phone number and location via a third party. And even though we can't see the identities of private wallet owners, if a law enforcement agency sees criminal activity associated with a wallet, they can subpoena the crypto exchange where the individual bought their cryptocurrencies for the personal information associated with the wallet, which allows them to identify the owner and investigate further.

Allison Nathan: But don't the majority of cryptocurrency transactions take place on exchanges that aren't regulated and don't comply with KYC and anti-money laundering (AML) protocols?

Michael Gronager: The extent of non-compliance has likely been overstated. When I was running Kraken in 2012/13, we logged into all of the major exchanges to see what information they asked users for, and every one required some level of KYC information. Many exchanges that are not formally regulated still comply with standard KYC protocols in practice. Up until last year, for example, there was no regulatory framework for public crypto exchanges in Europe; while some countries had individually rolled out requirements, theoretically many exchanges in the EU could onboard customers without asking for any identification. But most exchanges still collected information on their clients. And there are many other digital breadcrumbs that can enable the identification of a user and facilitate an investigation of criminal activity.

Allison Nathan: So what share of transactions do you think take place on exchanges that don't comply with KYC?

Michael Gronager: I wouldn't attempt to cite a specific number, but I am confident in saying that a majority of crypto exchanges are collecting some level of identification from users. Some that don't are peer-to-peer (P2P) exchanges that facilitate people meeting on the street with only a username. In this situation, the transaction is an exchange of cash for crypto, which can be completely anonymous. But many P2P exchanges collect KYC information now too. Another example is some online sites operating out of Eastern Europe where the lack of identification is almost a feature. But people may be afraid to use such sites given the lack of protection. And even in cases where a transaction is associated with an exchange that isn't KYC complaint, the wallet will likely have transacted with someone that has been identified. So it usually only takes a few steps to identify individuals on the blockchain.

Allison Nathan: What about darknets? Aren't they difficult to identify?

Michael Gronager: It's true that darknet markets that facilitate the purchase of weapons, drugs, and other illegal products and services online operate on the "dark web"—parts of the internet that are encrypted or otherwise difficult to access. They also often provide instructions for how users can try to obfuscate their transactions. But despite such efforts, we can generally map out these markets and see their traffic. Once an operation is identified as involving criminal activity, the size and scope of that activity can be tracked because it happens on the blockchain.

Allison Nathan: But isn't it possible that there are darknet markets out there that you haven't uncovered?

Michael Gronager: Yes, but the whole idea of a market—whether it's on the darknet, clearnet, or in person—is to attract customers. To get a customer base, they tend to market their products or services via darknet forums, or some can even be found through a Google search. So, some darknet markets may be really bad at marketing and therefore remain undetected, but that would also probably mean that they don't have many users and only account for a small share of illicit activity. Even if we can't identify a darknet market, we can oftentimes identify an entity that looks like a criminal service simply because of its patterns and activities.

Allison Nathan: What patterns do you look at to identify illicit activity?

Michael Gronager: Entities or wallets engaged in illicit activity will try to obfuscate their transactions by enlisting services such as mixers or coinswaps, where someone can swap bitcoin for privacy coins that better preserve their anonymity. An entity interacting with a service like this would be flagged. And as in the case of darknet markets, the mixers on the blockchain are public in the sense that they need a website in order to acquire a customer base, making them easy to identify. The harder part is identifying the users sending funds to these services. But they don't provide 100% obfuscation from blockchain analysis.

Allison Nathan: Is illicit activity involving fiat-to-crypto exchanges, such as money laundering, captured in what you track?

Michael Gronager: To some extent. Activities like money laundering typically start with criminal funds, which can be identified. A transaction that wouldn't be captured is a drug lord that buys $10 million of bitcoin on the street and then places it on a P2P exchange. We would not have identified that because it's basically the job of traditional investigations to flag that the money had a criminal tie before it ended up on the exchange. These transactions aren't well captured because we have no way of knowing from the onset that they're criminal.

Allison Nathan: But doesn't that mean that your methodology likely misses a lot of illicit activity?

Michael Gronager: That's true in principle. But it's hard to say why someone looking to hide this type of illicit activity would move into crypto. If you already have cash, crypto is not the best instrument for money laundering. It would make more sense, for example, to build a house and pay the workers in cash and then sell the house than to send funds via crypto where they leave a trace. So it could be done, but I doubt it accounts for a large amount of activity. Crypto transactions only really make sense in facilitating illicit activity that happens online, where using cash isn't possible, such as buying drugs or a weapon that are mailed to you. As soon as you transact in person, cash is a better anonymity-preserving instrument than crypto, because it leaves no trace. For anything that happens physically, cash is king.

Allison Nathan: What about financial crimes such as tax evasion? Is that captured in your numbers?

Michael Gronager: Someone recently asked me whether the recent rise of crypto prices has been driven by a rise in tax evasion. But that seems unlikely because taxes are typically filed around the end of the year, so that wouldn't account for the rise in prices since the start of the year. There probably is quite a lot of evasion in the sense of people not paying taxes owed on crypto gains, though. Guidance on these tax liabilities remains unclear, but those taxes will likely have to be paid at some point. But the main point is that blockchain and crypto aren't simply online enablers of all bad activity and dark money. What they help with is the ability to move money earned through illegal activity abroad more easily and possibly evade recourse so long as they're in a jurisdiction that's unlikely to punish them. But that arguably happens already with wire transfers and a lot of other schemes where financial proceeds end up in another jurisdiction where there's no reach in terms of the law and no willingness to investigate. Crypto gains made in some foreign jurisdictions are also relatively untouchable.

Allison Nathan: Have illicit actors using cryptocurrencies gotten smarter, and how do you keep up?

Michael Gronager: Criminal actors are always looking for areas that offer the least friction and the best opportunities for obfuscation. In the early days of cryptocurrencies, criminal activity was predominately tied to smaller transactions involving relatively normal people buying drugs online. But there's now a greater concentration of illicit activity tied to larger transactions. As the size of transactions has increased, so too has the desire of criminals to feel safe in their transactions, which has led to greater guidance online about how to try and avoid being tracked.

But the danger of using the blockchain for anything criminal is that transaction records are stored forever. While an obfuscation scheme may work well today, it's always possible that technology will eventually make it trivial to investigate. And that's what we've seen consistently over time; anything that seemed like a really good obfuscation scheme yesterday has often vanished completely after a year or two and become simple to investigate as we study the activity and figure out how it works. At some point, we understand it well enough to be able to assist the public sector in keeping citizens safe.

Bitcoin: beyond the basics

Step 1: Joining the Network and Buying Bitcoin

- Bitcoin is a peer-to-peer electronic payment system that transfers value between digital ***wallets***. Wallets don't store currency, but rather interact with the blockchain by generating the necessary information to receive and send money via blockchain transactions.
- Wallets are a combination of a ***public key*** and a ***private key***, and based on these keys, an alphanumeric identifier called a ***public address*** is generated. Similar to an email address, the public address specifies the location to which coins can be sent to the blockchain, and is shared among users. The private key is used to access funds, and like a password, should not be shared with anyone.
- Security issues present important risks for bitcoin users—bitcoin is a bearer instrument, and knowing the private key to a wallet would effectively put the user in possession of all bitcoin directed towards that address. The best security practice for crypto custody is to keep everything in ***cold storage***—offline—until you need to make a transaction, move the wallet to ***hot storage***—online—for the transaction, and then move the wallet back into cold storage. Today, a number of solutions exist to move wallets in and out of cold storage.
- The most popular way to obtain Bitcoin is through an exchange. Currently, the most commonly used type of exchange is not decentralized, and users need to provide personal identification documents per Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. Bitcoin ATMs and P2P exchanges are alternative ways of obtaining bitcoin.

What do public and private keys actually look like?

Cryptographic keys—which underpin BTC wallets—are strings of numbers and letters:

Public key: Account number, similar to an e-mail address.

```
0450863aD64A87ae8A2fE83c1aF1a8403cB53f53e486D8511
DaD8A04887e5B23522cD470243453a299fa9E77237716103A
bc11A1dF38855eD6F2eE187E9c581bA6
```

Address: Shortened version of the public key, unique to each transaction.

```
1FfGkGsfn3DoDzwJTDmizXVVGBQKbVSwuo
```

Private key: Password granting access to a wallet's funds

```
Kx3uWwctbQRj3dDhMynqamfLApV6wiX7JUY7cgN1YQgijhRY7PQe
```

What does a typical wallet look like?

Wallets contain digital records of past transactions, which are used to calculate a total balance.

Example: Web/Mobile Wallet	
.0061BTC *$300*	
Send BTC	*Request BTC*
Transaction History	
Received Bitcoin (4/23/2021)	0.002BTC (+$100)
Sent Bitcoin (4/23/2021)	-0.004BTC (-$200)
Purchased Bitcoin (4/23/2021)	0.0081BTC (+$400)

Step 2: Transacting in Bitcoin

- Bitcoin can be transferred between wallets in exchange for other currencies or goods/services. There are three key variables in a bitcoin transaction: an ***amount***, an ***input***—the address from which the bitcoin is sent—and an ***output***—the address that receives the funds. To make a transaction, users need to enter their private key, the amount of bitcoins they want to send, and the output address. A ***digital signature*** is then generated from the private key, and the transaction is announced to the network.
- The transaction is included in a ***block***, which is attached to the previous block to be added to the network's public ledger, the ***blockchain***. The blockchain does not track account balances. Rather, it keeps a record of where the bitcoin comes from and which address it is sent to. Therefore, the transaction input must match a past transaction, not the value being transferred.
- If a user makes a transaction worth less than the total amount of bitcoin they have, ***change*** is returned to the user. For example, assume User A has a total balance of 10BTC, received through two previous transactions of 6BTC and 4BTC. User A wants to send 2BTC to User B. To do so, User A sends 4BTC to User B and sends the change back to himself. This change is less any transaction fees that User A incurs, which are based on the size of the transaction (bytes). And the change does not go back to the original output—it will go to a new address under the user's control.
- The transaction is not immediately processed. Instead, it enters a pool of pending transactions and goes through the verification process (see Step 3: Verifying Bitcoin Transactions).

How are bitcoin transactions recorded?

Example: User A Sends 2BTC to User B		
Sender	**Address**	**Input (BTC)**
User A	14Q7x8pWz	4.0
Receiver	**Address**	**Output (BTC)**
User B	12rgbuMEv	2.0
User A	1EmDcxbnu	2.0-fees
Receiver	**Address**	**Fee (BTC)**

Value sent must have been received in a past transaction—think of it like using a gift card with 4BTC.

The transaction's "change" goes back to User A; the address is different, but the funds will likely return to the same wallet.

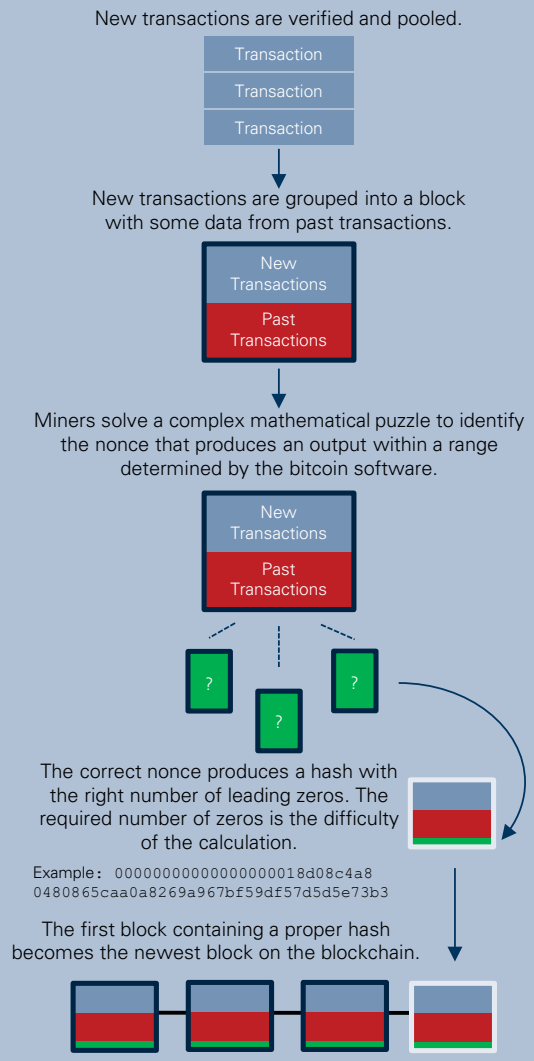
Every transaction in the blockchain is tied to a unique identifier known as a transaction hash, which is a 64-character random string of letters and numbers. Transactions can be tracked using this identifier.

Example ID: `0818d8a2f694077370cedf571c246d9cb3c4bd49 0bec66960df684fae618c68`

Step 3: Verifying Bitcoin Transactions

- In order for transactions to be recorded on the blockchain, they must be verified by ***miners***. Miners can be individuals or ***pools*** of people. Most mining today is conducted by pools of miners.
- First, miners identify whether a transaction is valid. Bitcoin senders must have both the proper authority to send funds and the necessary funds to back the transaction. Once the transaction is validated, it is packaged into a block with other valid transactions. Blocks have a maximum size of 1MB.
- Miners then compete against each other to be the first to add their block to the blockchain by solving a complex mathematical puzzle and including the answer in the block. The puzzle is to find a number that, when combined with the data in the block and passed through a ***hash function***—which converts input data of any size into output data of a fixed length—produces a result within a certain range. The result is called a ***nonce***, which is an integer between 0 and 4,294,967,296.
- Miners find the nonce effectively by guessing what it is. The more computing power a miner has, the more guessing calculations he can perform. The hash function is applied to the combination of a guessed number and the data in the block, and the resulting hash will begin with a certain number of zeros—which determines the difficulty of the calculation. This difficulty is frequently adjusted to ensure that it takes an average of 10 minutes to process a block.
- The first miner to get a resulting hash within the proper range alerts the network, and all other miners stop working on the block at that point. As a reward, the winning miner gets compensated with some new bitcoin. The amount of the reward decreases over time, halving around every four years.
- Importantly, the hashing process puts a timestamp on all transactions contained within each block. It also links the data from new transactions to information from past blocks. Therefore, transactions can't be undone or tampered with, because that would require redoing all the blocks that came after the original block.

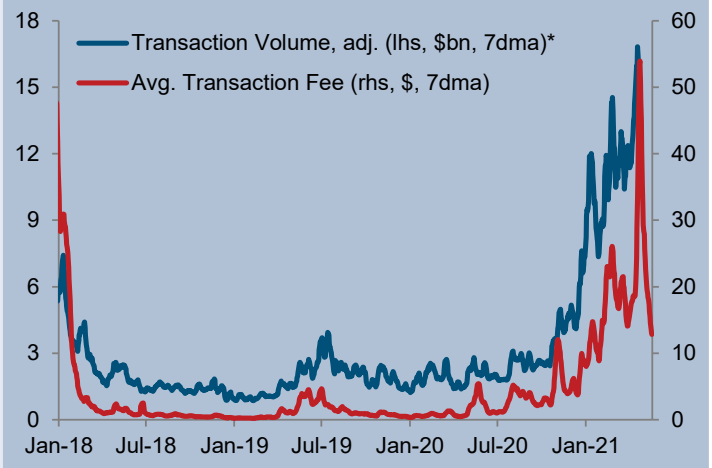
How do miners add blocks to the blockchain?



Step 4: Creating New Bitcoins

- In addition to receiving rewards for verifying transactions and maintaining the blockchain, miners also receive transaction fees. These are payments by bitcoin users to ensure that their transactions go through quickly given the limited throughput of the bitcoin network (approx. **4.6** transactions per second). Therefore, increases in transaction volume have led to an increase in transaction fees paid to miners.
- Bitcoin's founder set a limit for the maximum supply of bitcoin that will ever be in circulation at **21**mn. Today, there are approx. **18.7**mn in circulation, although some coins have likely been lost. Given the current halving rate, the final bitcoin is expected to be mined in 2140.
- While its technically feasible to change the 21mn limit if the community chooses to do so, the bitcoin community has long stood in favor of the limit.
- Once the 21mn limit is reached, transaction costs may need to significantly increase to incentivize miners to continue maintaining the blockchain, since there will not be any more rewards received from mining a new block.

What's keeping the network running?



*Adjusted transaction volume is calculated by Coinmetrics as the dollar value of the sum of all native units transferred that day, removing noise and certain artifacts.
Source: *Coinmetrics, Goldman Sachs GIR.*

Source: Princeton University, Cambridge University, Blockchain Council, Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Blockchain.com, CoinDesk, Coinmetrics, various news sources, Goldman Sachs GIR.

Top of Mind archive: click to access

Issue 97
Reflation Risk
April 1, 2021

Issue 96
The Short and Long of Recent Volatility
February 25, 2021

Issue 95
The IPO SPAC-tacle
January 28, 2021

Special Issue
2020 Update, and a Peek at 2021
December 17, 2020

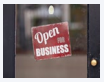
Issue 94
What's In Store For the Dollar
October 29, 2020

Issue 93
Beyond 2020: Post-Election Policies
October 1, 2020

Issue 92
COVID-19: Where We Go From Here
August 13, 2020

Issue 91
Investing in Racial Economic Equality
July 16, 2020

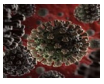
Issue 90
Daunting Debt Dynamics
May 28, 2020



Issue 89
Reopening the Economy
April 28, 2020

Issue 88
Oil's Seismic Shock
March 31, 2020

Issue 87
Roaring into Recession
March 24, 2020



Issue 86
2020's Black swan: COVID-19
February 28, 2020

Issue 85
Investing in Climate Change
January 30, 2020

Special Issue
2019 Update, and a Peek at 2020
December 17, 2019

Issue 84
Fiscal Focus
November 26, 2019

Issue 83
Growth and Geopolitical Risk
October 10, 2019

Issue 82
Currency Wars
September 12, 2019

Issue 81
Central Bank Independence
August 8, 2019

Issue 80
Dissecting the Market Disconnect
July 11, 2019

Issue 79
Trade Wars 3.0
June 6, 2019

Issue 78
EU Elections: What's at Stake?
May 9, 2019

Issue 77
Buyback Realities
April 11, 2019

Issue 76
The Fed's Dovish Pivot
March 5, 2019

Issue 75
Where Are We in the Market Cycle?
February 4, 2019

Issue 74
What's Next for China?
December 7, 2018

Issue 73
Making Sense of Midterms
October 29, 2018

Issue 72
Recession Risk
October 16, 2018

Issue 71
Fiscal Folly
September 13, 2018

Issue 70
Deal or No Deal: Brexit and the Future of Europe
August 13, 2018

Issue 69
Emerging Markets: Invest or Avoid?
July 10, 2018

Issue 68
Liquidity, Volatility, Fragility
June 12, 2018

Issue 67
Regulating Big Tech
April 26, 2018

Issue 66
Trade Wars 2.0
March 28, 2018

Source of photos: www.istockphoto.com, www.shutterstock.com, US Department of State/Wikimedia Commons/Public Domain.

開示事項

レギュレーションAC

私達、アリソン・ネーザン、ジェニー・グリムバーグ、ガベ・リプトン　ガルブレイス、ジェフリー・カリー、クリスチャン・ミュラーグラスマン、ザック・パンドル、ミクハイル・スポロジスはここに本リポートで表明された全ての見解が、私個人の見解を正確に反映したものであり、当社の業務や顧客との関係への配慮により影響を受けていないことを証明します。

特に断りのない限り、本リポートの表紙に掲載されている個人はゴールドマン・サックスのグローバル投資調査部のアナリストです。

開示事項

規制に基づく開示事項

米国法ならびに米国の規制に基づく開示事項

本資料に記載された企業に要求される以下の開示事項に関しては、上記の各会社に関する規制に基づく開示事項をご参照ください：主幹事会社または 共同主幹事会社の役割；1%またはその他の持分；特定の業務に係る報酬の受領；顧客関係の種類；過去の証券公募における主幹事会社または共同主 幹事会社の役割；役員の兼務；株式については、マーケット・メーカーおよび/またはスペシャリストの任務。ゴールドマン・サックスは本資料に記載 された発行体の債券(あるいは関連する派生商品)の自己勘定売買を行います、あるいは行う場合があります。

追加の開示事項： **証券の保有ならびに実質的な利害の対立**：ゴールドマン・サックスの方針では、アナリスト、アナリストの下で業務を行うプロフェッショナル、およびその同居家族が、アナリストが調査対象としている企業の証券を保有することを禁止しています。 **アナリストの報酬**：アナリストの報酬は、投資銀行部門の収益を含むゴールドマン・サックス全体の収益も考慮した上で決定されています。 **アナリストによる役員の兼務**：ゴールドマン・サックスの方針では通常、アナリスト、アナリストの下で業務を行う者、またはその同居家族が、アナリストが調査対象としている企業 の役員、取締役または顧問を兼務することを禁止しています。 **米国以外のアナリスト**：米国以外のアナリストは必ずしもゴールドマン・サックス・アンド・カンパニーの外務員ではなく、したがって調査対象企業とのコミュニケーション、公の場への登場、保有証券の売買を規制するFINRAの規則2241あるいは規則2242の適用対象とならない場合があります。

米国以外の管轄地域の法律や規制に基づく追加の開示事項

以下の開示事項は、米国法ならびに規制に基づきすでに記載された項目以外に、各管轄地域で開示が求められているものです。 **オーストラリア**：ゴールドマン・サックス・オーストラリアPty Ltdおよびその関連会社はBanking Act 1959 (Cth)で定義されるオーストラリアの公認預金受入機関ではなく、オーストラリアにおいて銀行サービスを提供することも銀行業務を営むこともありません。本資料および本資料の入手や利用は、ゴールドマン・ サックスが別段に合意した場合を除き、Australian Corporations Actで定義されている”wholesale clients”のみを対象としています。調査資料の作成にあたり、ゴールドマン・サックス・オーストラリア投資調査部の社員が、調査資料で言及する企業およびその他の事業体が主催する会社訪問や工 場見学、その他会合に出席することがあります。ゴールドマン・サックス・オーストラリアがかかる訪問や会合に関する状況に照らして適切かつ妥当と 判断した場合には、その訪問や会合の費用の一部または全額を当該発行体が負担することがあります。本資料において金融商品に関してなんらかの意 見が含まれる場合は一般的な見解であり、個々のお客様の投資目的、財務状況、もしくは必要性を考慮することなくゴールドマン・サックスが作成し たものです。お客様は、これらの意見に基づき投資行動をとる場合、当該意見が自身の投資目的、財務状況、必要性に鑑み適切であるかを事前にご考 慮ください。 オーストラリアおよびニュージーランドのゴールドマン・サックスにおける利益相反に関する開示事項並びにゴールドマン・サックスにおけるオーストラリアセルサイドリサーチの独立性に関するポリシーはhttps://www.goldmansachs.com/disclosures/australia-new-zealand/index.html をご覧ください。 **ブラジル**：ブラジル証券取引委員会(CVM) Instruction 598に関係する開示情報については、https://www.gs.com/worldwide/brazil/area/gir/index.html をご覧ください。CVM Instruction598第20項が適用される場合、本文の最後に特に明記のない限り、本資料の初めに記載された最初のアナリストが、同項が定義する、本資料の内容に 主たる責任を負う、ブラジルで資格登録されたアナリストとなります。 **カナダ**：ゴールドマン・サックス・カナダ・インクはゴールドマン・サックス・グループ・インクの関連会社であり、したがってゴールドマン・サックス(上記定義)に関する会社に関する規制に基づく開示の対象に含まれます。ゴール ドマン・サックス・カナダ・インクは、本資料を顧客に広範に配布する場合、その範囲において本資料を承認するものとし、またその内容に責任を負う ことに同意しているものとします。 **香港**：本資料に記載された、当社アナリストが調査対象としている企業の有価証券に関し、さらに詳しい情報がご入用の際には、ゴールドマン・サックス(アジア)L.L.C.にお問い合わせください。 **インド**：本資料に記載された企業に関しさらに詳しい情報がご入用の際には、ゴールドマン・サックス(インド)セキュリティーズ・プライベート・リミテッド、SEBIにおけるリサーチアナリスト登録番号INH000001493、951-A, Rational House, Appasaheb Marathe Marg, Prabhadevi, Mumbai 400 025, India、法人登記番号U74140MH2006FTC160634、電話番号+91 22 6616 9000、Fax +91 22 6616 9001までお問い合わせください。ゴールドマン・サックスは本資料に記載された企業の(Indian Securities Contracts (Regulation) Act 1956第2項(h)で定義される)証券を1%以上実質保有している場合があります。 **日本**：金融商品取引法第37条に定める事項の表示をご参照ください。 **韓国**：本資料及びそのアクセスは、ゴールドマン・サックスとの別段の同意がない限り、韓国金融投資サービスおよび資本市場法の「プロフェッショナル投資家」に向けたものです。 本資料に記載された企業に関しさらに詳しい情報がご入用の際には、ゴールドマン・サックス(アジア)L.L.C.ソウル支店までお問い合わせください。 **ニュージーランド**：ゴールドマン・サックス・ニュージーランド・リミテッドおよびその関連会社は(Reserve Bank of New Zealand Act 1989で定義される)「登録銀行」でも「預金受入機関」でもありません。本資料および本資料の入手や利用は、ゴールドマン・サックスが別段に合意した場合を除き、Financial Advisors Act 2008で定義されている”wholesale clients”のみを対象としています。 オーストラリアおよびニュージーランドのゴールドマン・サックスにおける利益相反に関する開示事項は https://www.goldmansachs.com/disclosures/australia-new-zealand/index.html をご覧ください。 **ロシア**：ロシア連邦で配布される調査リポートは、ロシア法で定義される広告ではなく、商品の宣伝を主目的としない情報・分析に該当するものであり、ロシアの資産評価に関する法の意義の範囲 内における評価を提供するものではありません。 調査リポートは、ロシア法ならびに規制に基づく個人向けの推奨を構成するものではありません。また、特定のお客様に向けたものではなく、お客様の財務状況、投資プロファイルまたはリスクプロファイルを分析することなく作成したものです。 本資料に基づくお客様やその他の投資行動について、ゴールドマン・サックスは一切の責任を負いかねます。 **シンガポール**：本資料に関するあらゆる事柄については、シンガポール金融管理局の規制を受け、本資料の法的責任を負っているゴールドマン・サックス(シンガポール)Pte.(Company Number: 198602165W)までお問合せください。 **台湾**：本資料は情報提供のみを目的としたものであり、当社の承諾なしに転載することはできません。投資に際しましては、各自の投資リスクを慎重にご検討ください。投資の結果につきましては個々の投資家が責任を負うものとします。 **英国**：英国金融行動監視機構の規則において個人投資家の定義に該当するお客様は、本資料を本資料で取り上げた、当社アナリストが調査対象としている企業に 関する過去のゴールドマン・サックス・リポートと関連してお読みいただき、ゴールドマン・サックス・インターナショナルから送られたリスク警告を参 照して下さい。これらのリスク警告の写しや本資料で使用した金融用語の用語解説をご希望の方は、ゴールドマン・サックス・インターナショナルまで お問い合わせ下さい。

欧州連合ならびに英国：投資推奨または投資戦略を推奨、提案するその他の情報の客観的な提示、および個人の利益の開示または利益相反の表明の技 術的な手続きに関する規制技術基準についての欧州議会および理事会規則(EU) No 596/2014を補足する欧州委員会委任規則(EU)(2016/958)の第6条2項(英国の欧州連合および欧州経済領域からの離脱後に英国の国内法や規制に組み込まれる委任規則も含む)に関連する開示情報は、欧州での投資調査に 関する利益相反管理方針を記載したhttps://www.gs.com/disclosures/europeanpolicy.htmlでご覧いただけます。

グローバル調査資料：配布機関

ゴールドマン・サックスのグローバル・インベストメント・リサーチ部門は、全世界でゴールドマン・サックスのお客様向けに調査資料の発行と配布を行 っています。世界各地のゴールドマン・サックスのオフィスに勤務するアナリストは、業界および企業、マクロ経済、為替、市況商品、ポートフォリオ戦略

に関する調査資料を発行しています。本資料の配布については、オーストラリアではゴールドマン・サックス・オーストラリアPtyリミテッド(ABN 21 006 797 897)が、ブラジルではゴールドマン・サックス・ドゥ・ブラジル・コレトラ・デ・ティツロス・エ・ヴァロレス・モビリアリオスS.A.が、オンブスマン・ゴールドマン・サックス・ブラジル： 0800 727 5764 および/または ouvidoriagoldmansachs@gs.com (平日の午前9時から午後6時にお問い合わせください)。Ouvidoria Goldman Sachs Brasil: 0800 727 5764 e/ou ouvidoriagoldmansachs@gs.com. Horário de funcionamento: segunda-feira à sexta-feira (exceto feriados), das 9h às 18h、カナダではゴールドマン・サックス・カナダ・インクまたはゴールドマン・サックス・アンド・カンパニーが、香港ではゴールドマン・サックス(アジア)LLC が、インドではゴールドマン・サックス(インド)セキュリティーズ・プライベート・リミテッドが、日本ではゴールドマン・サックス証券株式会社が、韓国ではゴールドマン・サックス(アジア)LLC ソウル支社が、ニュージーランドではゴールドマン・サックス・ニュージーランド・リミテッドが、ロシアではOOOゴールドマン・サックスが、シンガポールではゴールドマン・サックス(シンガポール)Pte(Company Number: 198602165W)が、米国ではゴールドマン・サックス・アンド・カンパニーが、これを行います。ゴールドマン・サックス・インターナショナルは英国および欧州連合内での本資料の配布を承認しています。

欧州委員会：英国プルーデンス規制機構により認可され、英国金融行動監視機構ならびに英国プルーデンス規制機構の監督を受けるゴールドマン・サックス・インターナショナルは、欧州連合域内および英国国内における本資料の配布を承認しております。

英国が欧州連合ならびに欧州経済領域を離脱した日(「離脱日」)からは、配布機関に関する以下の情報が適用されます。

英国プルーデンス規制機構(「PRA」)により認可され、英国金融行動監視機構(「FCA」)ならびにPRAの監督を受けるゴールドマン・サックス・インターナショナル(「GSI」)は、英国国内における本資料の配布を承認しております。

欧州経済領域：PRAにより認可され、FCAならびにPRAの監督を受けるGSIは欧州経済領域内の以下の管轄地域で調査資料を配布します：ルクセンブルク 大公国、イタリア、ベルギー王国、デンマーク王国、ノルウェー王国、フィンランド共和国、アイルランド共和国；フランスでは、離脱日よりフラン ス健全性監督破綻処理機構(「ACPR」)が認可し、ACPRとフランス金融市場庁(「AMF」)が監督することになるGS -Succursale de Paris(パリ支店)が調査資料を配布します；スペイン王国では、スペイン証券取引委員会に認可されたGSI - Sucursal en España(マドリード支店)が調査資料を配布します； GSI - Sweden Bankfilial(ストックホルム支店)はSwedish Securities and Market Act (Sw. lag (2007:528) om värdepappersmarknaden)第4章4項に基づきSFSAより「第三国支店」として認可されており、スウェーデン王国内で調査資料の配布を行います。ドイツで法人化された金融機関であり、単一 監督メカニズム内で欧州中央銀行の直接のプルーデンシャル規制の対象となり、その他の点ではドイツ連邦金融監督庁(Bundesanstalt für Finanzdienstleistungsaufsicht、BaFin)およびドイツ連邦銀行の監督を受けるゴールドマン・サックス・バンク・ヨーロッパSE (「GSBE」)が、ドイツ連邦共和国内および欧州経済領域内でGSIが認可されていない管轄地域で調査資料を配布します；また、デンマーク王国では、デンマーク金融監督庁の 監督を受けるGSBEコペンハーゲン支店(filial af GSBE、Tyksland)が調査資料を配布します；スペイン王国では、(限られた範囲で)スペイン銀行の国内での監督対象となるGSBE - Sucursal en España(マドリード支店)が調査資料を配布します；イタリアでは、関係する適切な範囲内でイタリア銀行(Banca d'Italia)およびイタリア証券取引委員会(Commissione Nazionale per le Società e la Borsa "Consob")の国内での監督対象となるGSBE - Succursale Italia(ミラノ支店)が調査資料を配布します；フランスでは、AMFとACPRの監督対象となるGSBE - Succursale de Paris(パリ支店)が調査資料を配布します；スウェーデン王国では、限られた範囲でSwedish Financial Supervisory Authority (Finansinpektionen)の国内での監督対象となるGSBE - Sweden Bankfilial(ストックホルム支店)が調査資料を配布します。

一般的な開示事項

本資料はお客様への情報提供のみを目的としています。ゴールドマン・サックスに関する開示事項を除き、本資料は信頼できると思われる現在の公開 情報に基づいて作成されていますが、当社はその正確性、完全性に関する責任を負いません。本資料に記載された情報、意見、推定、予想等は全て本 資料発行時点のものであり、事前の通知なしに変更される場合があります。当社は本資料中の情報を合理的な範囲で更新するようにしていますが、法 令上の理由などにより、これができない場合があります。定期的に発行される一部の業界リポートを除いて、大部分のリポートはアナリストの判断に より変則的な間隔を置いて発行されます。

ゴールドマン・サックスは、投資銀行業務、投資顧問業務および証券業務を全世界で提供する総合金融会社です。当社はグローバル・インベストメン ト・リサーチ部門が調査対象としている企業の大部分と投資銀行その他の業務上の関係を持っています。米国のブローカー・ディーラーであるゴールド マン・サックス・アンド・カンパニーは証券投資家保護公社(SIPC)(https://www.sipc.org)に加盟しています。

当社のセールス担当者、トレーダーその他の従業員は、口頭または書面で、本資料で述べられた意見と異なる内容の市場に関するコメントや投資戦略 を、当社の顧客およびプリンシパル取引部門に提供することがあります。当社の資産運用部門、プリンシパル取引部門、投資部門は、本資料で示され た投資見解や意見と整合しない投資決定を下すことがあります。

当社および当社の関連会社、役員、社員は、法令あるいはゴールドマン・サックスのポリシーで禁じられていない限り、本資料に記載された証券また は派生商品(もしあれば)の買い持ちや売り持ち、および売買を時として行うことがあります。

当社主催のコンファレンスで、当社の他の部門の従業員を含む、サードパーティのスピーカーが示す見解は、必ずしもグローバル投資調査部の見解を 反映したものではなく、また当社の公式見解でもありません。

ここで述べるサードパーティは、セールス担当者、トレーダー、その他プロフェッショナル、およびその同居家族を含み、本資料で言及された金融商 品について、本資料を執筆したアナリストの見解と相反するポジションをとることがあります。

本資料は市場や業種、セクターを越えた投資テーマに重点を置いています。本資料は当社が言及する業種またはセクター内の個別企業の見通しやパフ ォーマンスを識別しようとするものではなく、個別企業の分析を提供しようとするものでもありません。

本資料における、ある業種またはセクター内の一つもしくは複数のエクイティまたはクレジット証券に関する取引推奨は、いずれも本資料で論じた投 資テーマを反映するものであり、テーマから切り離して当該証券を推奨するものではありません。

本資料は売却・購入が違法となるような法域での有価証券の売却もしくは購入を勧めるものではありません。本資料は個人向けの推奨を構成するもの ではなく、また個々のお客様の特定の投資目的、財務状況、もしくは要望を考慮したものでもありません。お客様は、本資料のいかなる意見または推 奨に基づき投資行動をとる場合でも、その前にそれらがお客様の特定の状況に当てはまるか否かを考慮に入れるべきであり、必要とあれば税務アドバ イスも含めて専門家に助言を求めて下さい。本資料に記載されている投資対象の価格と価値、およびそれらがもたらす収益は変動することがありま す。過去の実績は将来のパフォーマンスを約束するものではありません。将来の収益は保証されているわけではなく、投資元本割れが生じることはあ り得ます。為替変動は特定の投資の価格と価値、およびそれがもたらす収益にマイナスの影響を与えることがあります。

先物、オプション、およびその他派生商品に関係する取引は大きなリスクを生むことがあり、すべての投資家に適切な取引ではありません。投資の際 にはゴールドマン・サックスの担当者もしくはウェブサイトhttps://www.theocc.com/about/publications/character-risks.jspおよびhttps://www.fiadocumentation.org/fia/regulatory-disclosures_1/fia-uniform-futures-and-options-on-futures-risk-disclosures-booklet-pdf-version-2018を通じて入手可能なオプションおよび先物に関する最新の開示資料をよくお読みください。オプションの買いと売りを組み合わせるスプ レッドなどのオプション戦略では取引コストがかなり高くなることがあります。関連資料をご希望の方はお申しつけください。

グローバル投資調査部が提供する異なるレベルのサービス：当社グローバル投資調査部が提供するサービスのレベルならびに種類は、コミュニケーシ ョンを受け取る頻度や手段に関するお客様のご要望、お客様のリスク特性や投資の重点分野ならびに大局的な投資観(市場全体、セクター固有、長期、短期等)、当社との顧客関係全体の規模や範囲、法律や規制による制約といった様々な要因により、当社の社内顧客および社外の他の顧客に提供 されるサービスと異なる場合があります。一つの例として、特定の有価証券に関する調査資料の発行時に通知を依頼されるお客様もいれば、当社顧客 向け内部ウェブサイトで入手可能なアナリストのファンダメンタル分析の基礎となる特定のデータの、データフィードその他手段による電子配信を依 頼されるお客様もいます。アナリストの根本的な調査見解の変更(株式の場合はレーティングや目標株価、業績予想の大幅な変更など)については、かかる情報を含む調査リポートが作成され、当社顧客向け内部ウェブサイトへの掲載という電子的発行または必要に応じてその他手段により、当該リポ ートがそれを受け取る資格のあるすべての顧客に広範に配布されるまでは、いかなる顧客にも伝達されることはありません。

すべての調査資料は電子的発行手段により当社の顧客向け内部ウェブサイトですべての顧客に一斉に配布され、閲覧可能となります。調査資料のすべ て

の内容が当社顧客向けに再配布されたり、第三者のアグリゲーターに提供されたりするわけではなく、ゴールドマン・サックスは第三者のアグリゲ ーター に

よる当社の調査資料の再配布に責任を負っているわけでもありません。一つ以上の有価証券や市場、資産クラス(関連サービス含む)に関して ご利用可能な調査資料やモデル、その他データについては、当社の営業担当者にお問い合わせいただくか、https://research.gs.comをご覧ください。

その他の開示事項については、https://www.gs.com/research/hedge.htmlをご参照いただくか、200 West Street, New York, NY 10282のリサーチ・コンプライアンスから入手することができます。

金融商品取引法第37 条に定める事項の表示

本資料とともに、金融商品取引をご案内させていただく場合は、各金融商品取引の資料をよくお読みください。金融商品取引を行われる場合は、各商 品等に所定の手数料等(たとえば、株式のお取引の場合には、約定代金に対し、事前にお客様と合意した手数料率の委託手数料および消費税、投資信 託のお取引の場合には、銘柄ごとに設定された販売手数料および信託報酬等の諸経費、等)をご負担いただく場合があります。また、すべての金融商 品には、関連する特殊リスクがあり、国内外の政治・経済・金融情勢、為替相場、株式相場、商品相場、金利水準等の市場情勢、発行体等の信用力、 その他指標とされた原資産の変動により、多額の損失または支払い義務が生じるおそれがあります。さらに、デリバティブのお取引の場合には、弊社 との合意により具体的な額が定まる保証金等をお客様に差し入れていただくこと、加えて、追加保証金等を差し入れていただく可能性もあり、こうし た取引についてはお取引の額が保証金等の額を上回る可能性があります(お取引の額の保証金等の額に対する比率は、現時点では具体的条件が定まっ ていないため算出できません)。また、上記の指標とされた原資産の変動により、保証金等の額を上回る損失または支払い義務が生じるおそれがあり ます。さらに、取引の種類によっては、金融商品取引法施行令第16条第1項第6号が定める売付けの価格と買付けの価格に相当するものに差がある場合 があります。なお、商品毎に手数料等およびリスクは異なりますので、当該商品等の契約締結前交付書面や目論見書またはお客様向け資料をよくお読 みください。

権利行使期間がある場合は権利を行使できる期間に制限がありますので留意が必要です。

期限前解約条項、自動消滅条項等の早期終了条項が付されている場合は、予定された終了日の前に取引が終了する可能性があります。

商号等：ゴールドマン・サックス証券株式会社 金融商品取引業者 関東財務局長(金商)第69号

加入協会：日本証券業協会、一般社団法人金融先物取引業協会、一般社団法人第二種金融商品取引業協会