Twitter Thread by Alex Krüger

Alex Krüger
@krugermacro

Crypto, a new asset class - quite a comprehensive report by Goldman.

Crypto: a new asset class?

With cryptocurrency prices remaining extremely volatile on news about regulatory crackdowns, environmental concerns and heightened tax scrutiny even as interest in crypto assets from credible investors has been rising and legacy financial institutions—including ourselves—have been launching new crypto offerings, crypto is undoubtedly Top of Mind. We first wrote about bitcoin in 2014 and cryptos more broadly in 2018, exploring the potential and risks of the crypto ecosystem. Amid the recent volatility, here we focus on whether crypto assets can be considered an institutional asset class.

We start by speaking with Michael Novogratz, Co-founder and CEO of Galaxy Digital Holdings, which is active in crypto investing and trading, asset management, and venture financing. He argues that the mere fact that a critical mass of credible investors and institutions is now engaging with crypto assets has cemented their position as an official asset class. And, despite the price volatility, he doesn't see the institutional interest in bitcoin, which he primarily views as a convenient store of value, waning as long as the current macro and political backdrop—in which the government has no imperative to stop spending on social issues that the Fed is largely financing—continues, and crypto remains in the adoption cycle.

Michael Sonnenshein, CEO of Grayscale Investments, the world's largest digital asset manager, agrees that institutional investors now generally appreciate that digital assets are here to stay, with investors increasingly attracted to the finite quality of assets like bitcoin—which is verifiably scarce—as a way to hedge against inflation and currency debasement, and to diversify their portfolios in the pursuit of higher risk-adjusted returns. Even though crypto assets have behaved as anything but a diversifier over the past year—selling off more than traditional assets as the COVID-19 pandemic set in—he says that their faster and stronger rebound in 2020 only reassured investors about their resiliency as an asset class.

But what makes a crypto like bitcoin—which has no income, no practical uses and high volatility—a good store of value? Novogratz's answer: because "the world has voted that they believe" it is. Zach Pandl, GS Co-Head of Global FX, Rates, and EM Strategy, largely agrees, arguing that bitcoin's potential for widespread social adoption given its strong brand on top of its other properties, such as its security, privacy, transferability and the fact that it's digital makes it a plausible store of value for future generations. And he believes that institutional investors today should treat bitcoin as a macro asset, akin to gold.

GS commodity analyst Mikhail Sprogis and Jeff Currie, Global Head of Commodities Research, for their part, argue that cryptos can act as stores of value, but only if they have other real world uses that create value and temper price volatility. This, they say, best positions cryptos whose blockchains offer the greatest potential for such uses, like ether, to become the dominant digital store of value. More broadly, Currie contends 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 that legal challenges to their future growth loom large due to their decentralized and anonymous nature.

And Nouriel Roubini, professor of economics at NYU's Stern School of Business, entirely disagrees with the idea that something with no income, utility or relationship with economic fundamentals can be considered a store of value, or an asset at all. Despite the recent crypto mania, he doubts the willingness of most institutions to expose themselves to cryptos' volatility and risks, which the volatile price action in recent days has served as a stark reminder of.

Christian Mueller-Glissmann, GS Senior Multi-Asset Strategist, then makes the case that for an asset to add value to a portfolio, it has to offer either an attractive risk/reward or low correlations with other macro assets, and preferably both. He finds that a small allocation to bitcoin in a standard US 60/40 portfolio since 2014 would've led to strong outperformance, owing both to higher risk-adjusted returns for bitcoin compared to the S&P 500 and US 10y bonds, as well as diversification benefits from relatively low correlations between bitcoin and other assets. But with this outperformance largely owing to only a handful of idiosyncratic bitcoin rallies, he concludes that bitcoin's short and volatile history makes it too soon to conclude how much value it adds to a balanced portfolio.

But beyond the debatable role of cryptos as a store of value and investible asset, does the broader crypto ecosystem provide promise for investors? Novogratz and Sonnenshein strongly believe that the answer is yes, given a myriad of potential use cases for crypto assets. In particular, Novogratz sees the three biggest developments in the crypto ecosystem—payments, Decentralized Finance (DeFi), and non-fungible tokens (NFTs)—mostly being built on the Ethereum network, which suggests substantial upside for it and various DeFi applications. But Roubini contends that few successful applications of blockchain technology exist today. And he sees many potential corporate uses of it as "BINO"—Blockchain In Name Only. In short, he's skeptical that blockchain technology will prove revolutionary because "the idea that technology can resolve the question of trust is delusional."

Mathew McDermott, GS Global Head of Digital Assets, then explains why GS has (re)engaged in the space—in two words: client demand—and how interest in cryptos differs between client types—from asset managers who are seeking portfolio diversification, to high-net-worth clients who are increasingly looking for exposure to broader crypto use cases, to hedge funds that are largely aiming to profit from the basis between going long the physical and short the future—an arbitrage that reflects the difficulties that still persist in accessing the market today.

Beyond this issue of market fragmentation, we conclude with a look at some of the other main obstacles to further institutional adoption of crypto assets. Alan Cohen, previous senior policy advisor to former SEC Chairman Jay Clayton and former GS Global Head of Compliance, explains how regulators are looking at crypto assets today. Michael Gronager, Co-founder and CEO of blockchain investigations firm Chainalysis, explains what is—and isn't—included in their analysis that finds that less than 1% of all cryptocurrency activity is illicit. And Dan Guido, Co-founder and CEO of software security firm Trail of Bits, discusses the black swan technological and security scenarios that all investors in the crypto ecosystem should be aware of.

Allison Nathan, Editor

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

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.

Bitcoin

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)**

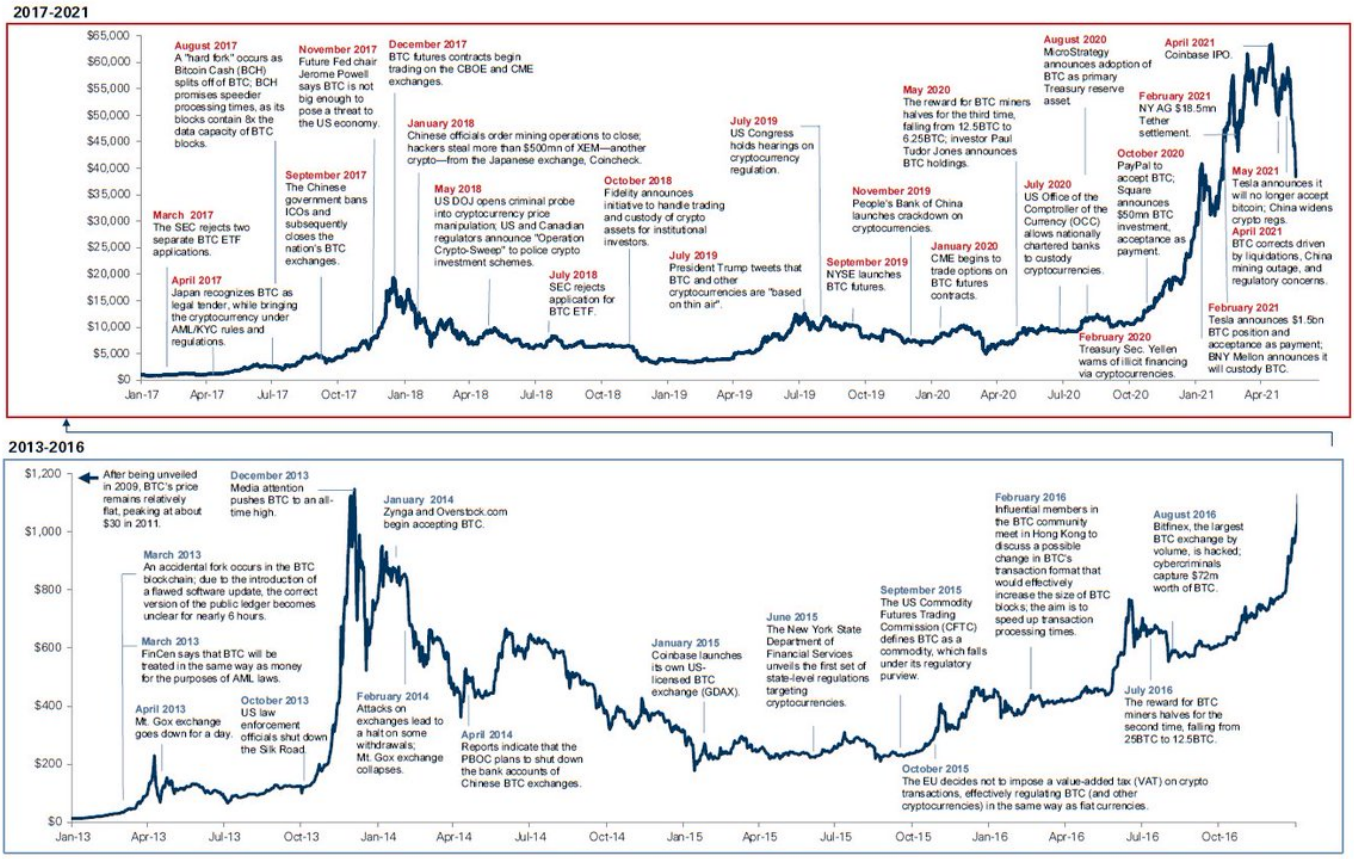
Value sent must have been received in a past transaction—think of it like using a gift card with 4BTC.

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`

2013-2016 sv 2017-2021



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

If I read that report and were a nocoiner, I'd go look at the charts, recognize this as a great entry point, and go shopping. Granted, I'm not a dinosaur.