



Opalesque Crypto Asset Pricing & Valuation Roundtable

Opalesque Roundtable Sponsor:



Editor's Note

Most insiders agree that the future growth of cryptocurrencies and digital assets largely depends on institutional adoption, and, of course, those type of investors must rely on fair value measurement of their assets. However, when it comes to cryptocurrencies and digital assets, most people would not think that valuation – defining their worth in an audit-able form – would be such a challenge. Just ask the American Institute of Certified Public Accountants' (AICPA) Digital Asset Working Group of approximately 30 subject-matter experts who over the past 10 months have been working to develop nonauthoritative guidance for professionals related to the accounting and auditing of these assets.

We're just getting started: Get a grasp on the emerging paradigm now

Technology and Data specialist Lukka has already over 3,000 digital assets in their database they actively keep track of, noting that *"this is not an exhaustive list by any stretch of imagination. Plenty of things are still in the SAFT (simple agreement for future tokens) or SAFE (simple agreement for future equity) form and so while these are not the actual tokens, they may still actually trade. And if we would include some of the very illiquid things, the number would be a lot more than that.*

"When you look at US stocks that are reasonably liquid, we may be looking at a number of around 8,000 to 10,000. So, to put in perspective, with digital assets we are looking at the same order of magnitude as equities already, and here, we just started."

Given that **experts expect that in 10-15 years traditional and other assets will be trading the way Bitcoin is traded now** (page 8) implies that all types of investors are advised to develop a deep understanding of the new paradigm:

- **Why taxonomy is important:** Cryptocurrencies, digitized assets, digital securities, stablecoins, and four types of tokens (page 6-11, 20)
- **How do you price these assets and establish consistency across the industry when they trade 24/7 and there's no principal market?** What is the closing price of assets on exchanges that never close? Is taking 11:59 pm UTC as a standard pricing measurement for the more liquid instruments trading 24/7/365 a good idea? (page 11-19)
- **Are cryptocurrencies / digital assets Level 1, 2 or 3** in the fair value hierarchy, and why has this question such a significant practical impact? (page 15-20)
- **Why is "nearly all" data from the 200+ exchanges (better: marketplaces) wrong?** How do practitioners work with data that is "95% fake"? Which processes are used to get to the real transaction data ? (page 16-19)
- **The role of fees in valuation procedures & the Bifinex phenomenon. Risk considerations in valuation. Shor's algorithm, quantum computing and the perspective of professional code breakers** (page 21-24)
- **Auditing investment funds that hold digital assets: Why public block explorers won't give you assurance but running your own nodes.** Implications of the Wyoming custody rules. SOC 1, SOC 2 / Type 1, Type 2: How to properly audit a crypto asset custodian (page 24-29).

The Opalesque Crypto Asset Pricing & Valuation Roundtable, sponsored by Lukka, took place in New York with:

1. Diana (Di) Krupica, **Lead Manager for Emerging Assurance Technologies, American Institute of Certified Public Accountants (AICPA)**
2. Jay Biancamano, **Managing Director, Digital Assets and Blockchain Innovation, State Street**
3. Jeremy Drane, **Chief Commercial Officer, Lukka, Inc.**
4. Joshua Lefcowitz, **Partner-in-Charge, Valuation Services, Cohen & Company**
5. Martin Schmidt, **Partner, Valuation Services, KPMG**
6. Nick Ogurtsov, **Chief Operating Officer and Chief Risk Officer, Lukka, Inc.**
7. Teddy Fusaro, **Chief Operating Officer, Bitwise Asset Management**

Enjoy!

Matthias Knab

Participant Profiles



(LEFT TO RIGHT):

Jeremy Drane (Lukka, Inc.), Di Krupica (AICPA), Teddy Fusaro (Bitwise Asset Management), Jay Biancamano (State Street), Joshua Lefcowitz (Cohen & Company), Martin Schmidt (KPMG), Nick Ogurtsov (Lukka, Inc.), Matthias Knab

CRYPTO?

Lukka Crypto Office.

Lukka Reference Data.

Lukka Pricing & Valuation.



The most advanced technology & data services
for middle & back office crypto asset processing.

www.lukka.tech | sales@lukka.tech



Introduction

Di Krupica

American Institute of Certified Public Accountants (AICPA)

My name is Di Krupica. I am an Emerging Assurance Technology Lead Manager at the AICPA. I have been at the AICPA for almost 10 years. I am involved with the development of all types of content relating to blockchain, cryptocurrencies, digital assets, robotic process automation, and artificial intelligence. I have experience developing many blockchain related CPE courses, including the Blockchain Fundamentals for Accounting and Finance Professionals certificate course, Blockchain for Supply Chain, Blockchain Implications for Audit and Assurance Services, and Blockchain for Financial Services. My main role is to take highly technical content and transform it into information that can be understood by those in the profession that may not have the specific expertise or background. Currently, one of my major projects is working with the Digital Asset Working Group, which is comprised of approximately 30 subject-matter experts from all size firms, who over the past 10 months have been working to develop nonauthoritative guidance for professionals related to the accounting and auditing for digital assets, including cryptocurrencies.

Martin Schmidt

KPMG

My name is Martin Schmidt. I am a partner of KPMG where I work in the firm's Valuation Practice. I have been doing business valuations and tangible asset valuations for over 30 years have a background in financial analysis and engineering. Currently, I serve as the risk management partner for the valuation practice with additional responsibilities related to blockchain, digital ledger, and cryptocurrency clients. At the moment, we are developing our risk framework and methodologies around a wide range of aspects on the accounting, tax, and consulting sides in this niche.

Nick Ogurtsov

Lukka, Inc.

My name is Nick Ogurtsov. I'm the Chief Operating Officer here at Lukka. I have been with Lukka for well over a year now, and prior to Lukka, I was the Chief Operating Officer and Chief Risk Officer for a publicly traded company called KCG, a Wall Street trading firm which was trading about 15% of US daily volume in equities. We were also one of the largest traders of treasuries and many other global liquid assets. A couple of years ago, we sold the company and that was also when I got very interested in the blockchain space and actually came to Lukka first as an investor before joining Lukka full time.

During my time at KCG, I was also a board member of the DTCC, so I'm very familiar with the traditional Wall Street structures and details of how markets operate. Prior to KCG, I spent most of my career at very large banks, UBS and others focusing primarily on equities, but was also involved in other interesting things like the first high-frequency trading businesses on Wall Street. As to my educational background, I'm trained in computer science and physics.

Joshua Lefcowitz

Cohen & Company

Joshua Lefcowitz from Cohen & Company. I started with Cohen & Company about 18 months ago to build out and lead the firm's valuations practice.

Prior to Cohen, I was at BDO for about four years in a similar role where I was leading the practice regionally, and prior to that, I was with a regional firm, which joined BDO in 2013. Nearly all of my career has been in valuation, similar to Martin doing business valuation and intangible asset valuation. Now at Cohen, I focus on a wide array of asset classes including digital assets. Currently, Cohen & Company audits around 100 cryptocurrency funds from all over the world, and all of the fair value measurement issues related to those cryptocurrency funds pretty much flow through my team.

In the world of auditing investment funds holding digital assets, there are many procedures outside of valuation for liquid digital assets and valuation is relatively straight forward, although not as simple as typical equities. However, when it comes to the illiquid digital assets, that sort of

flips upside down, right? It's all about valuation and some of the other audit procedures become a little bit easier to do. So, my team has been involved, predominantly on the valuation side working through just about everything you can think of on the illiquid side relative to cryptocurrencies and digital assets.

Teddy Fusaro
Bitwise Asset Management

My name is Teddy, I am the Chief Operating Officer at Bitwise Asset Management. Bitwise is a leading provider of private cryptocurrency index and beta funds which are offered to accredited investors. We focus on distribution to financial advisors, high net worth individuals, pensions, foundations, and endowments. Our flagship fund is an index fund that's based on the top 10 cryptocurrencies, as measured and published in the Bitwise 10 Large Cap Crypto Index. As a separate part of our business, we also create and publish cryptocurrency indexes. As you can imagine, creating indexes in the cryptocurrency world is full of complications that are much different than what we see in traditional asset classes. Bitwise is also one of the leading applicants for a Bitcoin Exchange Traded Fund, having a live application before the Securities and Exchange Commission that is currently under review now.

My background is primarily in exchange-traded funds where I spent about a decade and I also spent a few years at Goldman Sachs in equity derivatives prior to that. In the ETF sector I was primarily running portfolio management, trading, capital markets, and operations of early stage ETF issuers, most recently as an executive with an alternative strategy ETF issuer called IndexIQ, which we sold to New York Life about three and half years ago. At IndexIQ we managed hedge fund replication strategies packaged into ETFs. We were also one of the first issuers to do self-indexing, so there's a lot of crossover experience there related to what we're working on at Bitwise. Prior to that, my first ETF experience was with one of the early leveraged and inverse ETF issuing firm, a firm called DirexionShares where we pioneered the use of leverage and swaps inside daily leveraged ETF portfolios.

Jeremy Drane
Lukka, Inc.

My name is Jeremy Drane, I am the Chief Commercial Officer here at Lukka and have been here for three years. Prior to that, I spent 13 years at PricewaterhouseCoopers in a variety of roles and in my last role was in the firm's US Blockchain practice.

I left PwC because I was confronted with the question, "What happens if you have a use case where you are pulling data from multiple blockchains, and the blockchains you're pulling from don't have all the data needed to execute a downstream process?" I realized you would have to supplement blockchain data with additional data elements in order to get the job done. So I became very interested in what Lukka was doing, which was essentially solving for these questions by providing institutional grade data collection, standardization, and reconciliation services for blockchain data.

Jay Biancamano
State Street

Jay Biancamano, State Street Bank and Trust which as you probably know is one of the largest global custodians. I joined State Street in 2017 to head the US Digital Assets design and innovation team. My background is 20 years in mostly designing and building equity market structure products. I joined ITG in 1996 to when they began building their algorithmic suite and their TCA business as well as one of the first registered Alternative Trading Systems, I was also involved with the regulatory end of that. After ITG I joined their biggest Liquidnet, where as the Global Head of Marketplace I built their H2O product, My background is really in taking technology and building products around that.

Officially at State Street, we are not in the crypto asset business. One of the reasons for that is our clients are not in the crypto asset space. However, we do know they are looking at it very closely. We are mentioned frequently due to our position as a global custodian, when people theorize when Institutions will enter crypto, such as "Oh, if a big a global custodian got into the business institution, we'll follow." So, we're very aware of that and it is still something we're investigating. We are also on my team focused on the artificial intelligence business, and building products there.

Let me add that at State Street we are using the term “Digital Assets” rather than crypto because not everyone is really interested in trading Bitcoin, so we need to change the conversation to digital assets. People sometimes ask, “if digital assets were a baseball game, what inning are we in?” I’ll tell them that we are not even at the bat yet. There’s a lot that still has to happen, but I think that game can start very quickly.”

This material reflects the analysis and opinions of the speakers and may differ from the opinions of Opalesque and/or the Roundtable sponsors. It is intended to be of general interest only and should not be construed as investment, legal, tax or accounting advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. This material also does not constitute an offer to sell or a solicitation of an offer to purchase any interest in any fund or investment vehicle.

The views expressed are those of the speakers and the comments, opinions and analyses are rendered as of 19th July 2019 and may change without notice. The speakers make no representation or warranty as to the accuracy of any views or information contained herein and expressly disclaim any obligation to revised or update such views or information. The information provided is not intended as a complete analysis of any subject discussed herein. Statements of fact are from sources considered to be reliable, but no representation or warranty is made as to their completeness or accuracy. Furthermore, any assumptions, assessments, estimates, projections or the like (collectively, “Statements”) regarding future events or which are forward-looking in nature constitute only subjective views, outlooks or estimations, are based upon the speaker’s expectations or beliefs, and involve inherent risks and uncertainties, many of which cannot be predicted or quantified. In light of these risks and uncertainties, there can be no assurance and no representation or warranty is given that these Statements are now or will prove in the future to be accurate or complete in any way.

Matthias Knab

It's interesting that Jay already brought up the question of the distinction between crypto or cryptocurrencies and digital assets, so this is something we should elaborate a bit on as well. But first, I am curious about your thoughts what are crypto or digital assets and why are they important? Why should people make an effort to understand them and this technology?

Jay Biancamano: I teach a course on Blockchain for Business at the College of New Jersey and I can say that most of the students I've spoken to tend to know more than I do because they are already knee-deep into bitcoin, and they are well ahead of many capital markets professionals. My high-level definition is that a crypto asset is a digital asset, and digital assets are irrefutable, non-replicable records of a value.

*Now, why is it important? When we look back, we can identify a number of waves or changes in the fundamental technology in this industry. **The biggest wave was in the late '80s or early '90s where we moved from material assets via dematerialization to electronic, registered assets.** This transformation allowed a number of things to happen. It allowed the regulators to more look more closely at who owns particular assets at a single point in time, and much of that came directly from regulators who saw the value of electronic ledgers. When you look back at the late '80s or early '90s, trading financial instruments was a very manual process. We were trading 60 million to 100 million shares a day in equities, for example. After moving that to an electronic process, we went from 60 million to 100 million shares to two to three to five to 10 billion shares on some days, right? That changed the whole system.*

***When FIX protocol came out, this allowed for a number of new products, from dark pools to algorithmic trading to, of course, high-frequency trading.** Why? Because in an electronic market you now had a source and pool of data that had insight which we couldn't capture before.*

***With digital assets, we will be able to capture more intelligence and thus create products even more profound.** We are now talking about something that has asset intelligence built into it. I think it is really exciting to think about what we can now build around that and what type of analytics can we now use?*

I mentioned that now we also have digital asset records that are irrefutable. This means we can also see a history of these assets and to some, that is a kind of scary aspect. As an aside, you know the history of bitcoin is a very interesting one and it has been associated with some nefarious activities.

Getting back to my point, I said that electronic trading allows to take manual processes and automate them, allowing the system to do more and operate at high efficiency. What is interesting is that with digital assets, some of those processes go away entirely, making the system then even more efficient. Transfer agents, for example, is one. So processes that we scaled with electronification may go away, creating greater efficiencies and saving costs while possibly freeing up the ability to move between asset classes.

There are a lot of things we can do with digital assets that we can't do with traditional assets. This is why I believe we are in a profoundly revolutionary time.

Digitalization is democratizing assets. Just for this discussion's sake, let's look at an average portfolio, and it will probably look like 60% equity, 35% bonds, and 5% cash, or something like that. Now, think about the portfolios in the future which can be open to digitized assets like intellectual property, real estate and other hard illiquid assets like real estate tokens, or CryptoKitties. OK, maybe not CryptoKitties.



Democratizing assets will also result in a completely new portfolio management. It's not the 60-35-5, but maybe 10-15-10, we could have any type of model, and also, these models could actually change very actively as now people and markets can operate in a 24/7 type of model. So, many things will change and are already changing.

Sometimes when I talk to people about these things, they look at me and say, "Okay, you're dreaming." I'm like, "No, this is reality, it's happening now. You can now take a \$30-million penthouse in Manhattan and tokenize it. I couldn't buy a piece of the \$30-million dollar penthouse before, but now I can."

Nick Ogurtsov: You mentioned digital versus crypto and I'm just curious, do you think there is a genuine distinction or is it just like a different terminology depending on who you talk to?



Jay Biancamano: I'll clarify that we're talking the same language.

Crypto seems a little nefarious, a bit like the dark pools in the equity world where some people preferred them rather than the correct term: alternative trading systems. Bitcoin is what most people think of when they hear cryptocurrency, however, I prefer to say "Digital Assets", referring to all of them.

Here is another point I explain to people: **The way Bitcoin is traded now is the same way you will be trading traditional and other assets 10-15 years from now.**

Nick Ogurtsov: At Lukka we often have this debate of crypto asset versus digital asset, and we believe that there is an actual difference there. When we say "crypto" we do mean Bitcoin and cryptocurrencies as opposed to things that are more packaged.

Stablecoins are also somewhere in the frame – it could be crypto, but probably not – but certainly, we would not call tokenized real estate, for example, crypto but we would call it a digital asset, as it's simply not a cryptocurrency. In other words, we tend to use crypto as a shortcut for cryptocurrency as opposed to something more.





Jay Biancamano: When we talk about things on my team at State Street we tend to demarcate between what is native and non-native.

Non-native would have a tangible asset that's attached to it, and native being something like a cryptocurrency. We do try and steer everything into the digital assets space because the term crypto is related to something that some people may not believe in, but they are open to digital assets.

The other thing is that we don't talk about material assets and electronic assets anymore – they are all assets. So, eventually, the digital piece will go away as well, in my view.

Nick Ogurtsov:

Did you know that the DTCC still has plenty of paper assets to process? I'm old enough to remember having to send people in a taxi cab just to settle transactions. As a matter of fact, the longest-dated paper bond still in the DTCC vault is a bearer bond that they still physically clip the coupons with scissors every six months until 2032 when that bond matures. It's a hundred-year bond issued by, I think, a utility company or an old railroad company or something like that. So, we are not actually going to get rid of physical paper at least until 2032 at the DTCC.

Di Krupica: Through the work with our Digital Assets Working Group, a lot of progress has been made and the AICPA plans to release a series of interactive accounting and auditing whitepapers. It is planned that the accounting whitepapers will include a collection of questions and answers. As part of our working group discussions, we spent time talking about the basic question, "What is a digital asset?"

Broadly defined, a digital asset or crypto is a digital unit of account in which cryptography is used to verify and secure transactions on a digital, decentralized ledger, referred to as a blockchain that keeps a record of all transactions that take place across the blockchain network.

Because the working group believes there are professionals that may not be familiar with these terms, or they may simply be confused, the working group is developing an answer to the question, "What is the difference between a cryptocurrency and other digital assets?" It is being discussed that for our specific scope, we will define cryptocurrency and stablecoins.

As far as tokens are concerned, we will define four types of tokens: **security tokens, utility tokens, asset tokens, and hybrid tokens**, which may have multiple characteristics of some of the other types of tokens.

We feel that it is important that people understand these differences. When someone says "token" professionals need to understand that it is not all the same thing. Because professionals may generalize, it is important that professionals are clear that they need to gain an understanding of the underlying aspect of tokens as a first step.



Teddy Fusaro: What you are pointing out is important because we still need to work out a lot of things when it comes to pricing, valuation, audit, and assurance of crypto or digital assets. *The lack of clear standards around all of these things has been part of the challenge for companies because market participants, auditors, and regulators have historically spoken about these issues in slightly different ways. I am looking forward to a time where we all talk about these things the same way, and I think that time is fast-approaching.*

Industry participants are starting to draw distinctions, at least in their own records, between cryptocurrencies, digitized assets, utility tokens, and digital securities. Perhaps as Jay mentioned, we can bucket all of these things under one roof as “Digital Assets” or “Cryptoassets.”

Cryptocurrencies are things like Bitcoin, Litecoin, Ethereum, and a handful of others, which can be properly categorized as a store of value or a medium of exchange.

Digitized assets are assets that are tied to something else, like the portion of the penthouse that Jay mentioned, or any other traditional or offline asset, like a car or a stock certificate. That’s a digitized asset because the token is pointing to something that’s off the chain, and in that way, the asset has been made digital.

Utility tokens are coins or tokens that are intended to be used specifically within their own network or ecosystem. Think of Chuck-E-Cheese tokens or batting cage tokens. They are valuable as long as you’re in the ball pit or in the batting cage – but not usable elsewhere.

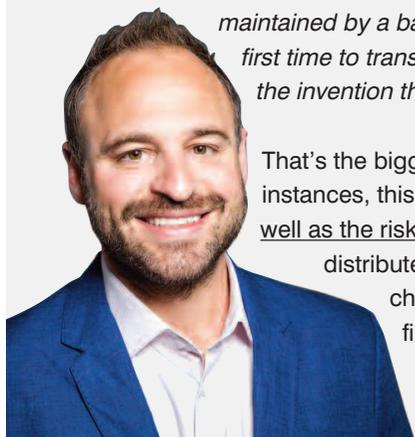
Then there are **digital securities**, those digital assets that could be ICO tokens or other equity or security representations where the token itself is the asset. With those, there’s nothing off chain, the token itself is the asset. The token could be equity in an ICO, or the actual representation of ownership in the common enterprise, or equity in a company that is merely issued through an offering using a blockchain.

Stablecoins – a category that deserves their own consideration – maybe need their own bucket.

Again, there are questions that aren’t settled yet, and so when we are speaking with people who haven’t started to really grapple with these differences and distinctions, they may look at you as if you have six heads – like, “What do you mean? You’re telling me there are five different buckets that I need to not think about? I don’t even know what Bitcoin is yet.” So, it is complicated.

Going back to the second part of Matthias’ question – **why digital assets are important**, I think we really need to point to the public blockchain as the invention. This is the new thing that really wasn’t possibly implementable before Bitcoin.

What’s new here is that it is decentralized, that there’s no central counter-party to it, there’s no central ledger that’s maintained by a bank or government or an entity, and that anyone can interact with it. This allows you for the first time to transact value over the internet without a central counter-party. I think that is really the aspect or the invention that matters.



That’s the biggest breakthrough, and a lot of other things are then developing from that. In many instances, this mechanism then also allows us to squeeze out the fees associated with the middleman as well as the risk associated with the middleman, or the need to trust the middleman. The way this distributed ledger works has also spawned a number of additional inventions – things that will change the way we think about capital raising, settlement, and the transfer of ownership – and firms are now working on ways to implement these solutions.

Jeremy Drane: I agree, once we have the ability to transfer value between two people without having a central counterparty, we now have all of these fantastic use cases. How I see this technology is that it's, in essence, **business process improvement software**. For a long time now, corporations have focused on improving efficiencies within their own organizations with blockchain they can now focus on building efficiencies between organizations.



Di Krupica: One aspect we have not mentioned is that with these new technologies and solutions, so many people that do not even have access to bank accounts can now be given the ability to transfer and receive cryptocurrencies and become more integrated and included into the economy. Anybody with access to the internet can join, and I think that is fantastic.



Martin Schmidt: We talk a lot about the taxonomy of cryptocurrency: “Is it equity? Is it currency? Is it pre-paid services?” But from a valuation point of view, we need to get past that.

When we are trying to come up with the value of an asset, we always look at the fundamental element of what we call the **Bundle of Rights**. What do I have by owning it? So, in the valuation world, we like to go back to first principles and look at what's the Bundle of Rights represented by that asset? This is important how we are going to value it, how we are going to account for it, or how they are going to tax it.

Matthias Knab

With the point of valuation that Martin brought up, we have now arrived at the center of the discussion we want to have today, namely looking at the challenges and potential solutions when it comes to the pricing, valuation, and audit of crypto and digital assets.

Can we start by elaborating a bit what is the challenge here and how do you go about it?

Joshua Lefcowitz: There are a variety of challenges, starting with the fact that at least to my knowledge this is the first time we are dealing with an asset class that trades 24/7/365.

If we are talking about fair value measurements for audited financial statements, how do you price these actively traded or liquid assets and establish consistency across the industry when they trade 24/7 and oftentimes may not have a clear principal market?

In traditional assets, the principal market is well defined and generally pretty evident, but in this asset class, it is not as well-defined and not as clear. The principal market is defined as the market with the greatest level of activity. The most

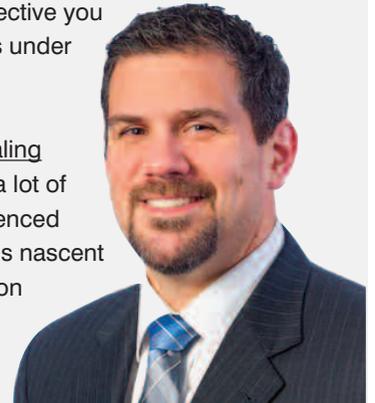
advantageous market is also relevant and would generally be considered the market with the highest price for the asset. Under fair value, market participants also have to be able to enter into a transaction, so access issues exist. Therefore, when determining fair value we could be looking at one of many markets.

I'm making up an example, but there could be 20 active markets for an asset, but the holder of that asset only has access to say 10 of those markets. So, from the perspective of determining fair value, we would exclude half of the markets that exist that are trading that asset, under US GAAP. That said, fair value is from a market perspective. Therefore, if market participants generally have access to the market with the highest price and greatest activity, that may be deemed to be the principal and most advantageous market, even if our specific client does not have access to it.

I'm sure Teddy will have a lot to say about this as well, but we all know that there are from time to time **pricing inconsistencies** across these markets. A lot of our clients are investment funds. Some may follow an arbitrage strategy where the principal market is whichever market has the highest price in which it has access. If it's more a long-term hold strategy the manager may not be as focused on what is necessarily the highest price. There are also data aggregators out there that are collecting prices that can be used as the most appropriate price to establish value.

My point here is that there can be a lot of room from the valuation perspective, whether we are dealing with liquid assets or illiquid assets. Let me clarify here that when I mention illiquid asset, I'm talking about pre-ICO type instruments, generally a SAFT (simple agreement for future tokens) or SAFE, a simple agreement for future equity. These could also be in essence, IOUs, a futures contract, or a variety of non-traded assets where from a liquidity perspective you can't convert that asset to a fiat currency. This is important because audited financial statements under US GAAP are being stated in US dollars.

So, if you cannot convert the asset into US dollars in a matter of 24 to 72 hours, then we are dealing with some form of illiquidity and valuation issues get far more complex. Summing up, there are a lot of issues in this new digital asset class that from the valuation perspective we really haven't experienced before. And then – we mentioned the four or five buckets before – when there are nuances to this nascent asset class that are not typical from a trading perspective, that is then causing additional valuation issues.



Nick Ogurtsov: Just to add a few numbers to some of the things Josh was mentioning, as we see the same things.

With our Lukka Reference Data product, we keep track of all the exchanges, all digital assets and all the players and takers around the world. To put it in some context for the purpose of this question of why is this a complicated thing to track: in our database, we have over 200 crypto or digital exchanges. Not all of them are liquid, obviously, and not all of them are made the same. A bunch of them already went out of business, but we still have to keep track of it because if a client had an account there three years ago, that might still be relevant to a tax authority for instance. But, of course, out of the 200 exchanges, not one has over 5% market share, so none of them are close to being the primary exchange for Bitcoin.



We also have **over 3,000 digital assets** in our database that we actively keep track of, and this is not an exhaustive list by any stretch of imagination. Plenty of things are still in the SAFE and SAFT form and so while these are not the actual tokens, they may still actually trade. And if we would include some of the very illiquid things, the number would be a lot more than that.

When you look at US stocks that are reasonably liquid, we may be looking at a number of around 8,000 to 10,000. So, again, to put in perspective, with digital assets we are looking at the same order of magnitude as equities already, and here, we just started.

I completely agree with Jay's earlier comment, we are not even in the first inning and so we're absolutely just getting started and already have reached a very high complexity.

And then, Josh mentioned it, dealing with exchanges that never close and that subsequently have no closing price is a hard problem. There is no primary exchange which leads to massive complexity given the thousands of assets and hundreds of exchanges. And here we are not even talking about distributed exchanges, OTC trading or derivatives, and all these things, but just around the raw assets themselves. Lukka's Reference Data product simplifies and streamlines this complexity.

Jay Biancamano:

I think 60% of all Bitcoin business by volume is OTC right now, that's the last I heard. But the other thing I'd like to add is that there are really no crypto exchanges because exchanges are regulated, what we have instead is 190 marketplaces or markets, and this fact of having unregulated markets contributes of course to the conundrum of pricing.

Di Krupica: Josh mentioned some of the challenges regarding determining the principal market for digital assets, which includes the challenge to determine the greatest volume and level of activity when it may fluctuate daily. He also mentioned the issues or questions on the reliability or the potential inconsistency of reporting of these numbers – you probably remember that the Wall Street Journal came out with an article regarding the inflated trading volumes at some exchanges. A professional may make a determination that a market is a principal market, but it is not, because the data used to make that determination is wrong or has been manipulated.

Because it may not be possible to convert a cryptocurrency straight to a fiat currency in one transaction, is there an additional challenge when potentially two principal markets may exist that need to be evaluated for a digital asset which only trades on a crypto-to-crypto exchange? Two markets may be involved, for example, one to convert crypto-to-crypto and then another to convert crypto-to-fiat.



Joshua Lefcowitz:

We have had that issue with our clients, but generally there is a liquid asset used as the medium of exchange (e.g., Bitcoin, Ethereum). As a result, it has not caused issues in our work.



Jeremy Drane: We can see a couple of issues here. There are crypto-to-fiat trades as well as crypto-to-crypto with a fee in crypto – essentially three capital assets all going off against each other – and then some exchanges don't provide a fiat price which means that now you have to go figure out where you will be getting your pricing from.

We see a lot of these data processing complexities, which has caused some issues around the ability for traditional software systems to process crypto transactions.

Teddy Fusaro: Just to add a practical dimension here – our fund invests in 10 coins. Acquiring Bitcoin, acquiring Ethereum, acquiring XRP, these are easy things to do, relatively speaking, once you understand how to operate in the cryptocurrency ecosystem and you've organized the right relationships.

But once you get down to the eighth or ninth coin, it can require a little bit more work – you may not be able to acquire it from the wholesale OTC desks given size constraints, or you may not be able to trade it in exchange for fiat currency (e.g., USD). This means you have to go and buy Bitcoin, transfer that to an exchange, and trade that Bitcoin into the other asset.

Those are now the transactions that the Fund has in its books and records related to how we're trading with the purpose of just acquiring one last coin. So it is a multiple step process that does create complexity, particularly from a tax, valuation, and accounting perspective, particularly since verified and professional tools haven't always existed to properly value each step of the transaction.



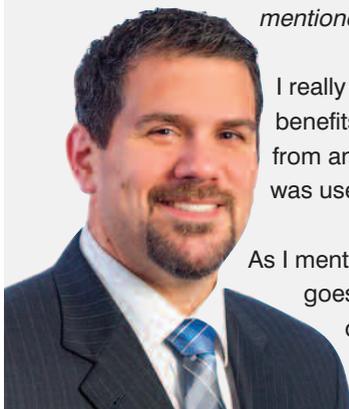
Joshua Lefcowitz: So Matthias asked about challenges in valuation, here is another one – kind of the same issue, but slightly different from a fair value or audited financial statement context.

We have clients investing in a SAFT, and then the project might go sideways or maybe slower than expected. And from a fair value perspective, the client might think, "Okay, we made this investment six months ago, eight months ago, a year and a half ago, whatever it is. The liquid markets are very volatile and it's difficult to value this illiquid instrument. Let's make a worst-case scenario – there's been no additional fundraising and our transaction was a while ago. We and most of the investors made the investment in Ethereum and so, we think if this project completely dies, and we get sort of a refund of our capital in Ethereum, right? We transacted 100 Ethereum and so we think we'll get 100 Ethereum back. What was the price when we invested? What's the price now?" And so here we may be trying to couple what was invested into this illiquid instrument.

*And then we have other client saying, "No, that has nothing to do with one the other, it was just a medium of exchange!" – you know what I mean? So, we have clients with different views and perspectives, so there are very significant challenges right now from a valuation perspective on the illiquid side. That said, we have been trying to take a practical approach by **getting things very well documented as much as we can**. The clients need to be in constant communication with us and other service providers about those new technologies that are coming on board in these five buckets that we mentioned.*

I really resonated with Martin's point about what is that Bundle of Rights? What are those economic benefits associated with the asset, and how will that translate into a number on your balance sheet? And, from an illiquid perspective, should it be tied to an index? Should it be tied to a currency or the asset that was used to acquire this asset? Should it be tethered to a fiat currency, a Stablecoin whatever?

As I mentioned, we have clients that are sort of all over the map right now and we are hoping that as time goes on we get much more consistency when it comes to issuing financial statements that have to deal with such issues.



Di Krupica: As we know, assets carried at fair value should be classified and disclosed in one of three levels (1, 2 or 3) in the fair value hierarchy table. The digital asset markets are 24/7 with no closing prices. Would this fact influence the level at which the digital asset is classified?

Martin Schmidt: Correct, the differences are that in Level 1 there's an active market in that exact asset. In Level 2 there's an active market in a similar enough asset that you can draw an analogy. While in Level 3 there are no observable markets and so you are relying on analysis and models to determine the value.

Di Krupica: Right, and while for digital assets we may have an active market for the same asset because the market is not closing but is 24/7, would that bump the asset into level 2 or would it be still at a level 1?

Would the use of one price modified by another price still be considered a level 1 classification or is the combination of prices considered an adjustment resulting in a level 2 classification?



Martin Schmidt: That's a good question.

The significance is that you have to disclose on the financial statements how something was valued. The auditing procedures that have to be done depends on the Level of the asset and can be quite different. These definitions and distinctions do have a significant practical impact in the accounting world because they also define what the accounting rules are going to be around this asset. And, of course, at the moment there is no general agreement on a lot of those fundamental questions.



Di Krupica: That is right, although we have not finalized any content as of yet the Digital Asset Working Group is working hard trying to figure out what we can provide to professionals. We have made a lot of progress and plan to release a series of comprehensive whitepapers covering both accounting and auditing topics. When each topic is finalized and has gone through AICPA's formal review process, we will publish the whitepapers as soon as possible. Based on the evolving nature of the digital asset ecosystem, we plan to post the whitepapers to our website and will have the ability to modify the content, if needed, as information changes.

Matthias Knab

What makes the most sense from your perspective?

Joshua Lefcowitz: When we work with a client, obviously we can give them our thoughts and observations about their financial statements, but they need to make their own decision.

That said, we generally recommend, from a pricing perspective, first and foremost, a consistent approach. For example, don't use one time for one asset and another time to price another asset. Generally, we are recommending 11:59 pm UTC as a standard pricing measurement for the more liquid instruments that are trading 24/7/365. In terms of the level of value hierarchy, we are generally advising clients that they should be categorizing these investments as Level 2 and Level 3 investments, and this goes back to that principal market condition we spoke about.

If a client, however, can define the principal market as one singular active market and that exact asset is trading on that one specific market, then that could be pushed into a Level 1 asset class or value characterization.

Generally, most of our clients are using some sort of data aggregator and a Volume Weighted Average Price (VWAP), which we believe instantaneously pushes you into Level 2 because it's not the exact price of that exact asset on one exchange or one principal market. And then the pre-ICO SAFT and those kinds of things are clearly Level 3.



Teddy Fusaro: As a Fund manager and practitioner, and based on consultation with our audit partners at Cohen & Company, we categorize as Level 2 all of the crypto assets that we hold in our portfolios. We opened our first fund in 2017 and the conversation we are having now was impossible to have then – pricing was more disparate, data availability was low, and tools like Lukka didn't exist. The marketplace for data has matured enormously since then, but we are still in this evolutionary phase of the process.

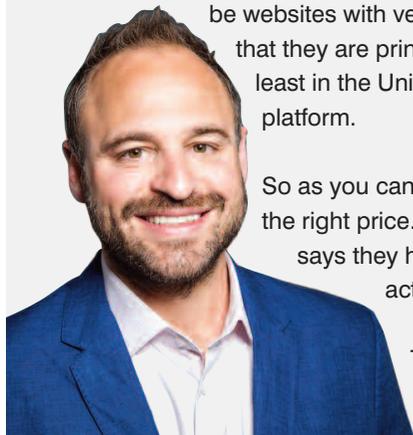
In deciding how to strike the Fund's NAV and choosing which price to use to mark our assets to market, we first attempted to find the exchanges that actually have volume traded on them. And as was mentioned, this is not an easy task, which led to Bitwise doing a deep dive on this particular topic. What we landed on, from a practical perspective, is first to determine the exchanges that actually have volume – an active market – and then use a price that is derived from that combination to value the asset. We consider that Level 2.

*But then, the question exists: how do you know that the data you are using is good? And what we found – and we presented this research to the SEC as part of the Bitwise Bitcoin ETF application – is that **most of the data, nearly all of the data is bad!** Nearly all of the data is garbage and wrong.*

Why? Because there has been this incentive along the way for marketplace operators - which can effectively just be websites with very little infrastructure - to claim that they are liquid exchanges. They just inflate the number that they are printing as a way to entice ICOs to come list on their platform which is likely illegal anyhow, at least in the United States. The ICOs would then pay the exchange listing fees for putting their token on the platform.

So as you can see, there are very practical and relevant concerns about audit standards and determining the right price. And, again, say you are just picking up a data stream from some random exchange which says they have half a billion dollars worth of Bitcoin volume every day. How do you know that they actually do?

This is where we spend a lot of time looking at these things as we try to identify where and



what the real market is. At this point it is not even about a principal market, I don't have the answer to that, but to find out where there are real transactions and volume.

The good news is that the pricing itself is actually very efficient. While it sounds like bad news to say that 95% of the volume and reported data is fake, when you look closer, it's actually good news because once you know what the garbage is, take it out and look at the data that's left behind, the market is actually very robust, very efficient, very well-functioning. Prices are integrated, they are tightly knitted together, and arbitrage is working well across all these market centers.

Matthias Knab

How do you determine what a marketplace is reporting is garbage? Do you look at their trade logs and how do you check them?

Teddy Fusaro: Right, this is very difficult and involves the effort of a dedicated research team and sophisticated engineering execution. You could start by looking at their trade logs, which you would typically do by accessing an API.

But as the group at this table knows, the information on the public website for one of these operators may look like there's trade activity going on there, but if you open up an API with them where you actually pull the historical record of activities they are reporting or have claimed in real time, often there's just nothing there. You find gaps or the data isn't actually there to download.

*So you need to **build a crawler** that looks at their screen that's actually displayed to the public – what we built looks at it four times a second - look at the bids and offers that they are posting, and pulls that down. You look at the prints that they're posting as actual trades, pull that down. Compare those prints to the rest of the market, look at the global order book. And once you start to do that, cutting out a lot of it is actually quite easy, because if they are faking it, this data makes it very obvious.*

Certain exchanges just print the same trade size every five seconds or they'll have a bell curve shape of volume sizes where all of the trades that ever printed on their exchange were perfectly distributed. Or they have really weird patterns, where no trades ever happened on their exchange in sizes from 0.1 Bitcoin to 0.9 Bitcoin, but all the time, they have trades that are exactly 6.0 Bitcoins. Of course, that is just not happening in the real world, this is not how markets behave. Markets are both logical and illogical in certain particular ways. On real exchanges, you see many very small trades without any obvious pattern in size, you see spikes of trades that occur at certain psychological levels – for example, one whole bitcoin will be a trade size that occurs more regularly than 0.94 bitcoin – and you also see synchronous spikes in volume across multiple exchanges in response to events or price action. So, those are the type things we are dealing with.

There are also some qualitative measures you can look at, real-world footprints. Take Coinbase: I've personally been to their offices multiple times; they have over 800 employees; they have raised hundreds of millions of dollars from well-known venture capital firms; have millions of web-page views; 26 million Google search results; a million followers on Twitter. All of these things point to real-world users and real-world activity. If you look at an exchange like CoinBene you see something like 42 part-time employees on LinkedIn, no record of raising venture capital, nobody knows where their offices are. They have few webpage visitors and a few thousand Twitter followers, no research commentary, et cetera. So, you can build a world view of what you think is happening in the exchange



ecosystem by putting together the rigorous research with the real world footprints, and we've taken the time to do that as well.

But I should say, we have only done that for Bitcoin. Nick said they have 3,000 digital assets? So, although, we have drawn some conclusions, there's still a lot of work that needs to be done.

Nick Ogurtsov: We have done exactly the same thing, maybe not as deep as you but broader: for several hundred assets at this point. We see the same things, except way worse as you go down the list.

But even for something as liquid as Bitcoin, there are other major technical issues. So, let's take UTC midnight as you suggested, 11:59:59 or whatever. One of the tactical things you actually see in this place is that some exchanges report prices sometimes by tens of minutes. This means you actually take a snapshot and then come back five minutes later and they get a totally different price. And that's even for Bitcoin, let alone for some other coins no one has ever heard of.

*These technical issues may not even be nefarious, but possibly just bad or slow technology. Who knows what it is, maybe it's nefarious, but the point is that stuff like this happens all the time. **So what exactly is a 11:59:59 price?** Is it 11:59:59 or whatever is reported as of 11:59:59 within 30 minutes? It could be very different. And then, as Teddy mentioned, they do have gaps. So, if you are pretty sure this is a liquid exchange, what do you do with the gaps in the data? That data may or may not be backfilled, who knows, right? All these are very practical challenges.*



I also agree that one can recognize some manipulative activities very clearly, like a trade entry for 500 or some very peculiar size every three minutes, these things happen, and a lot of it is very obvious and so discrepancies in reported and actual volume do happen everywhere.

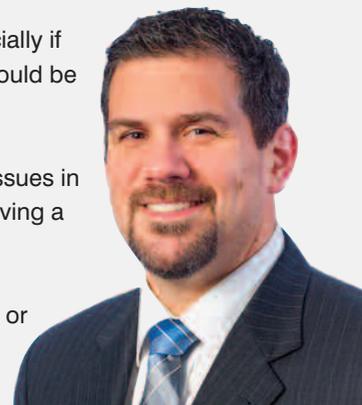
Joshua Lefcowitz: I don't have a perfect answer for that. To put some additional framework around it, from a valuation perspective, the notion or the standard that we use is information that's known or knowable as of that measurement date or in this case, that measurement time.

Now, even here people have different opinions as to what is known or knowable. Some groups take a very restrictive perspective of 11:59:59 which would be limited to what did you know exactly at that point? Other groups may encourage us to take a bit more of a liberal approach to that when asking what is the knowable piece. If we had an infinite amount of data transferability capabilities, then the numbers should be what it actually was.

So, if there are lags in the system, try to work those out and then deal with the good data, especially if we are talking about half an hour, an hour, whatever the timeframe is under the premise that it would be knowable in a perfect data stream environment, right?

But again, there is not a right or wrong answer, and so we as a CPA firm dealing with valuation issues in the audit context, we try to be as much within the technical guidance that's out there but also having a little bit of a practical perspective.

Personally, I don't necessarily have an opinion or don't know that I care too much if it's a perfect or



maybe not-so-perfect data stream, as long as we are being consistent and as long as it's not cherry picking. I mean, in these markets a coin could be up by 3% or 5% in a very short time, and if you are now taking advantage of that and charging fees associated with that by messing up your reporting process, then, as a practitioner, I would have a problem with that type of cherry picking. **Consistency in approach is key.**



Nick Ogurtsov: We built a product to solve some of these issues, and I agree that some of the parameters can be totally arbitrary, and so if other folks have a different view, we can adjust to that.

But what we have been doing for Ethereum and Bitcoin is to define 10 minutes after as the cutoff for the valuation. For those two coins we then seem to capture more than 99% of the data, and then for everything else, it's 30 minutes. The value doesn't change after that.

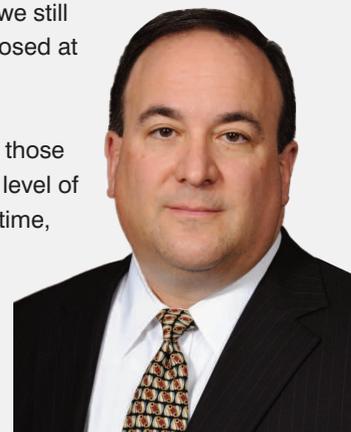
Teddy Fusaro:

I have a question for the experts in the room – Martin and Josh - on Level 1 classification of digital assets.

I explained the research we have done, and at the moment, let's say we think that we have good prices on 10 exchanges, and those look to me as observable prices in active markets. What's the specific guidance on why that is Level 2 instead of Level 1?

Martin Schmidt: I think you answered the question yourself when you said 10 markets because we still have to satisfy the principal market issue. So, a conventional asset is traded in New York and it closed at 4:00: one market, one day, one price. It's one data point and we didn't have to do any analysis.

In your example, it's Level 2 because you're looking at 10 markets and there's arbitrage amongst those markets, it might be significant. But more, in order to come to those 10 exchanges you did some level of analysis, you cut it down to 10 markets, and then from there you get 10 data points for the same time, and then you do even something else with this information. Maybe a simple average, maybe something more sophisticated, but *the point is that you didn't just observe it, you observed and then analyzed.*





Joshua Lefcowitz: I completely agree with Martin. The only thing I'm going to add is that the accounting guidance that we are working with wasn't written for this asset class, and so we are not only facing these issues of Level 1, 2 or 3 but there are other issues in terms of operating entities that own digital assets and how they are accounted for as intangible assets and things like that.

The accounting guidance around this entire asset class is square peg and round hole, and so Diane is working on that, but give her some time...

Martin Schmidt: I definitely agree with that and so the definitional conversation that we had earlier is important in the accounting world. *Is it a currency? Is it a commodity? Is it equity? Is it a derivative, or an intangible asset?*

In the accounting world, how you define it can very much drive how you value it, and so you define what is it first, then you look to the accounting guidance and that tells you how to value it for accounting purposes. So, the **taxonomy** is important before you get to the valuation for accounting.



Di Krupica:

Of course, Josh, we at the AICPA are responsible for the auditing standards for nonpublic entities, but not the accounting standards, which is developed and updated by FASB. Hopefully, by the end of the year, the Digital Assets Working Group will be able to start rolling out content for those professionals who need it.

Teddy Fusaro:

What would the guidance standards call for us needing to see in order, let's use Bitcoin as the example, to see Bitcoin become a Level 1 categorization? Do we need to evolve in the digital assets ecosystem to have that one exchange or primary market to pick the price from?



Joshua Lefcowitz: If you go to the guidance, and this is just more of a definitional discussion, not an opinion, we would need an active market that is trading the exact asset. So your example with Bitcoin, you would have to define the principal market as singular active market trading that exact asset for it to be qualified as Level 1. These are things we generally see with a regulated exchange.

Now, getting back to the real world, I don't know what the answer would be even if we had 10 good real markets and they all were trading at the exact same price, at the exact time, it was a perfectly efficient market, would that be Level 1? I don't know the answer to that.

Nick Ogurtsov: There are a number of exchanges that are relatively efficient in terms of lack of arbitrage, but then we also have phenomenons like **Bitfinex** where for a while there had been a several point spread versus the other liquid exchanges. And this is not a rounding error but can see 1% to 2% difference, and there are good reasons for this that we all know.

So when you take a closer look, the assumption that the crypto marketplaces are fully arbitrageable or in line is not true at all by several percentage points. And this is for Bitcoin, let alone all the other alt coins, right? What about the very illiquid digital assets, we know the pricing differentials can be very large there as well.

And that also brings up the issue that when you create an average price across exchanges, and one or more have their pricing off for any reason, you may, in fact, end up with a price that you couldn't possibly trade at all at that point, right? Is your averaged price then still fair value?



Joshua Lefcowitz:

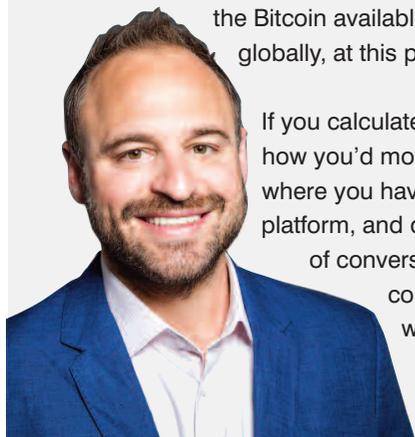
That goes that notion of being Level 2 where you could do that analysis and say that market is an outlier. It is not a principal market and should not be included in the data.

Nick Ogurtsov:

But it might be for a specific client. I am just highlighting the difficulties, and that, again, there aren't many answers on this.

Teddy Fusaro: I want to point out at this point of conversation that Bitfinex has a number of other issues it is dealing with, including a court order from the New York Attorney General enjoining iFinex Inc., the operator of the Bitfinex trading platform, from further violations of New York Law. That case is ongoing.

I'd also like to add that the reason the price of a Bitcoin on Bitfinex was different from other exchanges is because the Bitcoin available on that platform is priced in USD on Finex that trades at a premium or discount to USD globally, at this particular time due to USD withdrawal issues.



If you calculate the USD-Bitfinex to USD-global cross rate, then convert that rate to USDT to account for how you'd move it off-exchange, then the price snaps into line with the global bitcoin price. This is clearly where you have Level 2 analysis. Bitwise did also find that Bitfinex has real actual trading volume on its platform, and did include Bitfinex as part of our pricing component, which included that additional analysis of conversion. But our pricing methodology calls for us to remove platforms that are not in compliance with local regulations or are subject to extraordinary legal or regulatory action – so we removed it immediately after the NYAG instituted the order.

Nick Ogurtsov: We also need to look at the **fees** which are quite large, especially for high-frequency arbitrage. The way their fee structure is set up is that if you do more than a relatively few number of transactions per unit of time, the fees go up.

There's a very specific structure to discourage active high-frequency style arbitrage on that particular exchange, it is on purpose set up not to be very arbitrage-able, but still, prices will actually fluctuate quite a bit. Quite large like, I forgot the numbers, but they are on the order of 1% sort of large.

Joshua Lefcowitz: Generally for fair value measurement, transaction fees are ignored. This is current accounting standards, fair value context. Fair value for financial reporting according to US GAAP – those transaction expenses are not a component of value. So, Nick, back to your point on fees – when you do that analysis, fees wouldn't be taken into consideration.

Nick Ogurtsov: Take a look at this chart where we plotted a couple of exchanges to showcase where Bitfinex particularly diverged. This is where they were having severe regulatory issues with New York State Attorney General. My point is that this is a significant difference for that period, this is several percentage points even for Bitcoin, so this is not a minor or negligible anomaly.

Teddy Fusaro: I think that that is 3% probably difference there, right? At this time what the chart is showing is that in order to trade Bitcoin on Bitfinex, your dollar on that platform and a dollar elsewhere is about 3% different, which is feeding through to the Bitcoin price on Bitfinex.

Nick Ogurtsov: Plus, fees.

Teddy Fusaro: Right, agreed, and those fees or withdrawal complications both drive the pricing dynamic.

Nick Ogurtsov: Which is also due to the credit risk of both.

Teddy Fusaro: Yes, and we see how the chart is roughly back in line as the value of USD on Bitfinex and the USDT/USD pair has normalized since then. Or not completely in line, but on this scale, it appears as such.

Martin Schmidt: Changing gears a bit, one of the main things that we look at in any valuation is the risk. So far, we talked about the risk of bad data and the risk of fraudulent data.

We also have regulatory risk. But, I think, at some point, we also have to think about the idea of the risk from the cryptography itself. All cryptocurrencies and digital assets are based on the assumption that the underlying cryptography is sound and will always be sound.

*We have the advantage of having two physics majors in the room, Nick and me. How do you see the exchanges and the industry facing these risks? **Will quantum computing at some point break the cryptography?** And, will we know when it does and is it going to be a regulator that figures that out or is it going to be a fraudulent actor that figures that out? How should we think about that risk?*



Nick Ogurtsov: Martin, may I turn the question back to you asking if you take that risk into account when conducting an audit?

Martin Schmidt: At the moment, as far as I know, we do not take the cryptography risk into account as it is still such an open question and nobody knows how to handle that one.

Which other risks are we looking at then? Well, in the valuation world, we put ourselves in the shoes of the potential buyer of this asset. What would he or she need to know as of that date? What would he or she consider?



Joshua Lefcowitz: I am borrowing the following comment from a colleague who says that when we reach the point where quantum computing can break the cryptography, we will be facing much bigger problems than valuing blockchain assets because this will cause instability in the entire economic system.

There are major security risks like nuclear warheads being taken over. Such things then become a legitimate concern, and so there are way bigger issues to worry about when quantum computing breaks that cryptography.

Nick Ogurtsov: At this point, it could be helpful to explain the background of cryptography when we discuss quantum computing. In 1994, a mathematician called Peter Shor developed what became known as **Shor's algorithm**, a quantum computer algorithm for integer factorization. Informally, it solves the following problem: Given an integer N , find its prime factors. This basically showed that a quantum computer can factor very large prime numbers, which is the fundamental basis of most public key cryptography or at least the basic public key cryptography.

You cannot compute this using traditional computers in reasonable time, but if viable commercial quantum computers were to be built, and there are plenty of prototypes that are heading in that direction but not quite fully operational yet, the question is, could a similar algorithm be applied to the algorithms that are actually used as cryptography in blockchain?



Matthias Knab What we discussed at a Cryptocurrency Roundtables we produced earlier this year in Dubai is that the current cryptography will probably break if those quantum computers come online. However, some then also say that at that time we will, maybe with the help of those very same quantum computers, create a new form or a new level of cryptography. What do you think?

Nick Ogurtsov: I have two majors, in computer science and physics, and my computer science research was on computer security where my adviser was actually a cryptographer, and he shared some background with me.

When you talk to professional code breakers who work for government agencies, they sort of shrug their shoulders and say, “All codes are broken sooner or later. So, what’s the difference?”, which is, of course, a slightly different perspective from how most crypto traders approach cryptography like Bitcoin, but that is how professional cryptographers who had been breaking codes for decades sort of approach this.

Their perspective is, “Well, so what if today’s cryptography is broken, we’ll just put in a new algorithm that is not broken yet.” Perhaps it might involve something derived from quantum computing as far as the algorithm or it might be just a mathematical problem that is harder to solve by quantum computing. It’s not the quantum in nature, this could be a problem where quantum computing does not lend itself as readily as factoring in large prime numbers, for example. It could be some other class of problem. So, that perspective is that we’ll just place a hard fork and substitute a different type of cryptography and life will go on.



We don’t know what will actually happen. I suspect it will be somewhere between real calamity and nothing happens. There’s probably going to be some disruption, but it’s not necessarily a black and white thing and I don’t think the world will end.

Martin Schmidt: I don’t have much experience in auditing blockchain, right now I am more involved in consulting and the tax side.

We’ll give a commercial message for another firm that there was information that came out recently that PWC had added a blockchain auditing module to their audit software that in certain situations can match the public and private keys. So, one of the big four may have a way to audit who actual owns the cryptocurrency. This is a relatively basic step and a good indication of how far we have to go.



Joshua Lefcowitz: We are auditing investment funds that hold digital assets. Some of the procedures we are performing can be considered traditional audit techniques like sending confirmations.

In that procedure, there is an independent individual or entity, whatever the case may be, that states, “Yes, we received funds from this entity and we gave them X in exchange for that.”



To gain comfort over transactions and balances on the public blockchain, we apply a multi-tiered approach that involves using a variety of sources or methods to obtain the blockchain data and gain comfort over reliability. The approach involves taking into account certain factors like whether the blockchain is public or private, the significance of the balances reported by the client, as well as, client controls surrounding access to funds and record keeping.

As a way to **show control over the private key** to move those assets, there are a few options available that include the use of digital signatures, movement of a specified amount of tokens at a prescribed time, generation of view keys, etc. However, it varies depending on the blockchain and wallet providers being used.

Teddy Fusaro: I expect the Nick and Jeremy may have something to add on this related to one of Lukka's products, but in terms of auditing the blockchain, what gets Bitwise and a lot of other folks excited is the fact that the blockchain has this immutable record that anybody can look at.

So, audit step one would then involve exploring the blockchain, the immutable record, to see if what the client is claiming is true. The sort of everyman's way to look at the blockchain would be to use a web browser and navigate to a block explorer that queries the blockchain and returns results for you.

Remember, think about a blockchain as a big database, or a large spreadsheet. In order to confirm something, you need to look in the record and make sure it's there, and that's where the idea of a block explorer comes in. Once you determine, from 'exploring' the chain that something is where you say it is, you can go a level deeper and do something like Josh mentioned: ask the person or entity who owns the asset to send a small amount, move the entire amount, or just sign a message using the private key to prove that they have ownership over the private key associated with the asset in the address that had just been verified. Then use the explorer to again review that second action and check if that has happened on the chain.

So that's a process, but the next level of questions that auditors are now solving is: how do you trust the block explorer tool that is used to actually check blockchain? The ultimate answer will be that it's not good enough to do that.

What you need to do, in order to prove that you can determine something exists, is have your own controlled environment where you run a node yourself to download the entire transaction history of the chain in question. Then you can check that data with the nodes that you have inside your controlled environment. You don't need to use a public block explorer that itself could have risks.

Of course, there are implications about what a controlled environment means when it comes to things like SOC 1, SOC 2, so how you actually run this platform that verifies the transaction history.

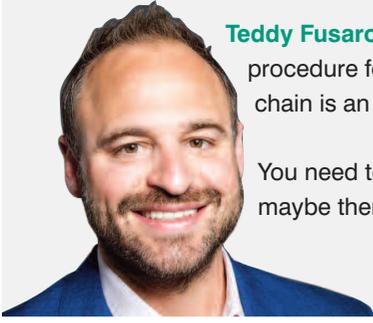
But this is where we are going as an industry. The audit firms themselves need to have their own – or have access to – a controlled environment for checking the historical record of blockchain, and I know that at least a number of the big four firms are building out this capability and functionality now.

In that way, when their client says, "I have this asset that's on this blockchain and I can transfer it here, or this is my proof of ownership of it," the auditor can actually verify that themselves using those fully controlled nodes to access the historical transaction record.



Matthias Knab

As there are many blockchains this would mean for the audit firms running nodes for each of them, right?



Teddy Fusaro: Yes, the implication is: if you want to do audit work related to blockchains, you need to have procedure for accessing the data on each specific chain, and so I would think that having nodes for each chain is an answer for that, or at least having access to nodes that are in a controlled environment.

You need to have a way of checking things in a manner that is consistent with what your mandate is. Now, maybe there could be a service that could provide this to auditors.

Jeremy Drane: Teddy is spot on. Let me add, first, there's a big difference between auditing a blockchain and auditing a transaction that occurred on blockchain. I think those two aspects get interchanged but they are really two completely different concepts. Auditing a blockchain is asking the question, "Is the blockchain working as engineered?" There are a whole set of system audit efforts that go into this which includes accounting firms and many different players.

The other point Teddy mentioned is, "I have this transaction, and now I want to make sure that that transaction is valid." This is exactly one of the things that Lukka does. We run our own blockchain nodes, and so when an exchange sends us a transfer notification, we will then ping our nodes, which are within a SOC 1 Type 2 environment, to independently verify, on our node, the information that came from the exchange.

In this context, I'd also like to point out that anybody who uses a public block explorer has to be very, very careful. All you have to do is to read the disclosures at the bottom of those webpages which basically say, "You cannot rely on the information on this website as being true." They have bug bounties which also tells you that there are issues. We have run tests across multiple block explorers and you get different answers for lots of different reasons. Usually, the folks that use those public explorers end up using multiples of them and try to figure out where the outliers are. Our perspective, and I think the perspective of an accounting firm, is that you should use them only as your last line of defense and run your own nodes as best practice.



Jay Biancamano: I'd like to bring up the anti-money laundering and the KYC issues that represent another critical issue that needs to be solved to make a custody solution certainly comfortable and enable audits. When we think about the history of an asset such as cash and many others we find that it typically is very finite, whereas, with Bitcoin or any other digital asset, we find that their history is written into the actual asset – so, if it that history shows it went through somewhere such as Silkroad, you can't erase it.



One of the things that I think institutions have to understand is that the history of the asset shouldn't be a roadblock for them to invest in these assets. If we look at cash, there was a study done about 10 years ago that stated 90% of bills in the U.S. in circulation probably has a trace of cocaine on it, yet no one ever accuses somebody of being a cocaine dealer because they have a \$20 bill. The same is true with digital assets where the auditability and being able to trace that history shouldn't be a reason to pause and we have to solve what is ownership and when does ownership occur.

Martin Schmidt: Jay, do you think the new custody rule in Wyoming is a breakthrough? Are you familiar with it?

Jay Biancamano: Yes, I'm reading up on it. I think it's a step in the right direction but like everything else, it's just a start. There are a number of regulators proposing rules that I think will clarify things.

Di Krupica: Who owns the cryptocurrency? In the world of digital assets, the person who holds the private key owns the cryptocurrency. If we give the private key to a custodian, at that point the question becomes, does the custodian own the cryptocurrency?

*There potentially will be **new laws in Wyoming** that discuss this topic related to a custodian holding a private key but the individual account holder retaining ownership of that cryptocurrency. This is an important step forward because this continues to be a major challenge.* The Digital Assets Working Group has had many discussions related to the challenges surrounding the determination of ownership in the digital asset space.

I also have a question: Is there any risk to an individual or an entity if they download a node?



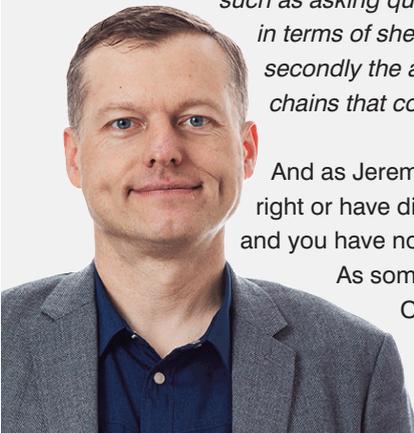
Nick Ogurtsov: I'll answer in a couple of different ways. As far as risk for an individual of running a node, it's not that it's a risk, but it's surprisingly difficult, at least if you want to run in a way that it's useful for audit, valuation, accounting, taxes, etc. For those let's call them professional purposes, it's surprisingly difficult. If you just want to run a node for other purposes like mining, for example, it's a lot easier, because you don't care about history, you don't care about operating databases, you don't care about figuring out details or smart contract detail, so it's much easier.

If you just want to mine a bit of Bitcoin using a laptop, that is not particularly hard or risky. But to run nodes for other purposes such as asking quality questions and get an answer that actually means something, it's surprisingly hard both in terms of sheer volume of data – these chains can get very large, gigabytes and terabytes of data, and secondly the aspect of complexity, especially if you look at Ethereum or other types of smart contract chains that could have a lot of nuances.

And as Jeremy was saying, when you look at a bunch of different public explorers, many just don't get it right or have different interpretations of something and then you can end up with very different answers and you have no idea which one is right. Therefore, to get to a real audit quality of work is seriously difficult.

As some of you are aware, this is one of the things we do at Lukka, specifically because it's hard.

Our clients come to us to not have to do all of that themselves. That's part of the answer.



Teddy Fusaro: The process which Nick was describing is hard and it requires a lot of engineering and computational resources. That's the challenge with it, particularly when you want to do things like download all of the potential transaction records in the Ethereum blockchain, for example. Keep in mind that some of the firms that we have doing these audits have now full staffs of blockchain engineers building these controlled environments, nodes and databases that then can interpret all of the data in a searchable and useful way.

The other end of the spectrum is, if you want to get started with Bitcoin, you can buy nodes now that come preloaded with all of the transactional records on a hard drive up to a certain point in time. You can plug that into the internet and it will get updated from production date when the manufacturer would have loaded the entire historical record up to that date. And then you can begin running your own node at home – it does take some computational power, it needs to be connected to the internet, but doing that is not that hard.

I also wanted to circle back to what Diana brought up, which is **auditing of crypto asset custodians** -- meaning auditing of exclusive ownership and exclusive control of a private key, and the processes and controls of those service organizations that act as safekeepers of those private keys.

This is an area where we are starting to attain clarity because certain of the institutional type of crypto-custodians that exist in the marketplace are in the process of completing their SOC audits. Many have actually obtained SOC 2 reports already, which is a report on controls within a service organization. What we haven't seen yet amongst these custodians is a SOC 1, and I think 2019 is the year that we will likely see at least one of those firms complete their SOC 1 audit.



The SOC 1 is a report on internal controls at an organization and specifically evaluates the impact of those controls on the firm's financial statements. With a SOC 1 audit completed, this will give a higher level of comfort to the institutional community around what it means to have exclusive ownership, exclusive control over private keys.

And then, when you combine audited controls over exclusive ownership and exclusive control, audited procedures for keeping the key safe, and the ability to audit the transaction record from a controlled environment with controlled nodes, then we begin to envision a future where blockchain solutions can recognize their potential in a way that is also compatible with existing audit standards and accepted practices.

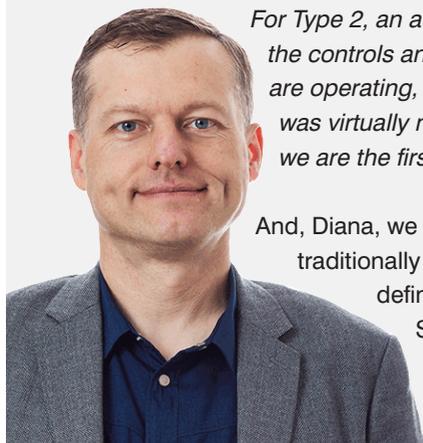
Di Krupica: Just to clarify, a SOC 1 report is a report on the controls at a service organization which are relevant to user entities' internal control over financial reporting.

A SOC 2 report is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

When a SOC 1 type 2 report is not available there are challenges related to auditing the valuation of digital assets when a portion of the processes and controls are performed by a third-party service organization.



Nick Ogurtsov: There's SOC 1 and SOC 2, and there's also Type 1 and Type 2. Type 1 is a single point in time which frankly doesn't mean that much.



For Type 2, an audit firm comes in and audits your systems for six months, to ensure that you are following the controls and they are doing random sampling. It's a very extensive process to make sure the controls are operating, as I mentioned, over a period of six months. And so, Type 2 is the much stronger one and was virtually non-existent in the crypto space, and so we actually did this at Lukka last year. We believe we are the first SOC 1 firm to obtain the Type 2 classification last year.

And, Diana, we struggled with the exact thing you are describing, because some of the process aspects traditionally are in SOC 2, not SOC 1. And so, what we ended up doing was to expand voluntarily the definition of SOC 1 to include additional controls that traditionally are not required to be part of SOC 1. This year we are doing both and are currently in the middle of the six months period to do SOC 1 and SOC 2, both Type 2.

Teddy Fusaro: At Bitwise we have a unique vantage point because we have done direct due diligence on the cryptocurrency custody firms that provide services into the institutional market through a competitive RFP process. We currently work with Fidelity Digital Assets, with whom we were the first external client for their Bitcoin custody business, and Coinbase Custody Trust Company.

What we have learned is that because the SOC 2 has some degree of malleability in terms of management creating what processes are that are going to be tested, it is both attainable in a shorter period of time and somewhat less concrete than a SOC 1. And as Nick pointed out, of course, Type 2 of each is also a higher bar because it is the actual operating effectiveness of the controls – which requires ongoing testing – vs Type 1, which merely reports on the description and suitability of the controls. The view is that there is really no flexibility with a SOC 1 because it relates to control over Financial Statements – Management's design of the controls doesn't matter as much as the end result, which is the statements themselves.

In order to sign off on a financial statement, it then must include many of the things that you would have to test in a SOC 2 assuming you designed one, and perhaps even more stringently or specifically. And therefore, in that regard, SOC 1 is viewed as the more comprehensive, the more difficult to obtain, the lengthier period to test, the less subjectivity in terms of what management's inputs are on procedures because ultimately, the auditor needs to resolve and sign off the financial statements. What we have seen in the crypto custody space is that in the development of SOC audits SOC 2s comes first because they have been considered attainable.

But we haven't seen the SOC 1 yet and we think that hopefully soon firms will be able to deliver that too. Out of necessity, it would be Type 1 first, and then we hope shortly or as soon as practical thereafter, the Type 2 next.

But we do know that the firms that are wanting to deliver this level of organizational control reporting, they are not going into the process saying, "Come take a look, and give us a SOC audit." They are saying, "Let's start with it a period of readiness preparation. Let's figure out if what we have in place now that's good enough. If it's not, let's change it. Then let's create the procedures, then we can work on sign off on the procedures, and then after that, we'll go to a place where we can test the procedures and get the SOC report in place."

We are well down the road of this process occurring. And if not in 2019 then in 2020, I expect we'll start to see those audits for custody become public.





DON'T MISS OUT

ACTION REQUIRED

Business decision makers LOVE online video because it gives them the most amount of information in the shortest amount of time.

– Bob Wies / President MV Digital

When done correctly, all you need is one video to build up highly targeted traffic for a really long time.

– Carey Lowe / Marketing Consultant

Video marketing is the most effective way for you to get someone's attention and engage them for a substantial period of time. Keeping someone engaged is the best and quickest way to gain their trust. Gaining trust is the only way to convert your audience into happy, long-term clients and customers.

– David Grimes / Marketing Manager

Video solidifies your online presence while building deep and meaningful relationships with your customers. It adds a personal touch to your brand while increasing your conversions! Videos are now an expected component of any website.

– Lilach Bullock / Marketing Consultant – Forbes top 20 women power influencers

It's more effective:

Video attracts two to three times as many monthly visitors, doubles their time spent on the site and has a 157% increase in organic traffic from search engines like Google.

– Marketing Sherpa

And more cost effective:

Video promotion is 600% more effective than print and direct mail combined.

– Diode Digital

One minute of video is worth 1.8 million words.

– *Forrester Research*

Video content can increase the chances of front page Google ranking by 53 times

– *Cisco*

And did you know that:

Online video is shared 1200% more times than links and text combined.

– *Simply Measured*

75% of executives watch videos while working.

– *Forbes*

“The Opalesque videos are a clever solution to the persistent problem of getting to know managers’ style and philosophy within a dizzyingly large universe of possibilities and with increasingly limited time. More managers would be wise to step out of their 20th century shells to embrace the new economy of communication technology to find more efficient ways to convey their story and message to existing and prospective investors.”

Adam Choppin, Manager Research & Investment Strategy of FIS Group

Opalesque videos are regularly featured among the best in any top 10 or top 20 hedge fund / investor video ranking, such as this one which lists 4 Opalesque videos out of a total recommended of 19 videos.

Opalesque started shooting manager videos in 2009 - you will probably know that **Julian Robertson, Izzy Englander, Jim Chanos, Jeffrey Ubben, Danny Yong, Elena Ambrosiadou**, and many other hedge fund legends have produced videos with Opalesque. We have also produced videos for some of the **biggest institutions** as well, such as **Morgan Stanley, State Street Global Advisors, M&G Investments.**

Save up to 50% in travel costs by making your first meeting the second one

Have you ever spent time and money to take a trip to present your fund, only to hear, *"Thank you for coming to our office, and please keep sending me your reports ..."*?

What if you had known before that the investor is looking for something else?

By sending their video to prospects **before the meeting**, the manager wins twice. Should the investor be looking for something else, the manager can focus his efforts on those investors who watched the video **and liked** what they saw.

In these cases, managers tell us that the first real meeting becomes more like a 2nd meeting (the 1st one being the video) as the groundwork has been laid and the meeting will be much more successful and achieve much more compared to a regular first meeting. By better **qualifying your leads**, you can basically halve your travel budget and raise more assets quicker.

Compliant

- Opalesque.TV videos are produced to comply with your regulatory requirements
- Allow for true reverse solicitation

You're in control

When you're doing a custom Opalesque.TV video, you have full control about any aspect of your message. This is not a given in any other regular media coverage.

A manager portrait on Opalesque.TV is generally designed to simulate a first time meeting with a prospective investor, meaning that questions like the following will be discussed:

- Please introduce yourself and your firm
- What is special about your strategy?
- How are you different from your competitors?
- What else is important regarding the asset class?
- Opportunities you focus on

Working with a trusted partner

Over 1.3 million people have watched one or more Opalesque.TV videos, which means that the people you may be targeting will already be familiar with Opalesque.TV videos.

Managers like **Julian Robertson, Izzy Englander, Jim Chanos, Jeffrey Ubben, Elena Ambrosiadou, Anthony Scaramucci**, and many others have done Opalesque videos, as well as institutions like **Morgan Stanley, State Street Global Advisors, M&G Investments**.

Broad distribution

You can either produce a private video with us, which will only be hosted on the non-public part of your website, or we can offer you the broadest possible multi-channel distribution on Opalesque.TV and our partners like Reuters and other leading platforms. Contact us to discuss your custom distribution package.

Managers have **quadrupled assets** thanks to our video (\$700m to \$2.4bn in 1 year) and also received a book contract or **invitation to speak at the World Economic Forum or at TED** through our video:

- View count: Over 1.5 million views (hundreds of thousands of people)
- Thousands of investors will view your presentations
- Longterm effect: Views do not drop significantly over time
- Without investing a single additional minute of your time - time required to record a video is approximately 90 minutes.

Costs

For a 10 minute video the all-inclusive package price is US\$10,000 which includes: travel (Europe and NY tristate), full production at your office, multiple edits (cuts), provision of the final video file, and a global, multi channel distribution package. A 15 minute video is \$15,000, so \$1,000 will be billed for each additional 2.5 minute above 10 minutes. The client determines the final length of the video.

Links

Opalesque.TV video which got 104 views over 2016 Christmas:

<http://www.opalesque.tv/hedge-fund-videos/patrick-stutz/>

Opalesque.TV videos sorted by number of views:

<http://www.opalesque.tv/most-viewed-hedge-fund-videos/>

Opalesque.TV videos sorted by number of social media shares:

<http://www.opalesque.tv/most-shared-hedge-fund-videos/>

Contact

Matthias Knab
Founder
Opalesque Ltd.
www.opalesque.com
Email: knab@opalesque.com
Tel: +49-89-2351-3055
Mobile: +49-170-189-0077

