SM254 | 10.25.2025
Re-engineering Tokenization | Episode 2
Ian Forester, Head of Product, Abaxx Technologies

This week on *Re-engineering Tokenization*, we continue our conversation with Ian Forester, Head of Product at Abaxx Technologies. David Greely sits down with Ian to pick up where we left off last week, digging in deeper on the use of cryptographically secured identity and signatures to take the next step from digitization to tokenization. David and Ian discuss Abaxx's approach to the four pillars supporting trusted commercial transactions: secure identity, intent, assets, and data.

Ian Forester (00s):
I don't know how a market can function as a truth seeking mechanism when it is surveilled top to bottom and all of its participants' actions can be predicted before they happen. I don't see how that market can function as a tool for discovery. And I think that's where I think we're heading with all of this, or at least making a very honest effort to right that.

Announcer (27s):
Welcome to SmarterMarkets, a weekly podcast featuring the icons and entrepreneurs of technology, commodities, and finance ranting on the inadequacies of our systems and riffing on ideas for how to solve them. Together we examine the questions: are we facing a crisis of information or a crisis of trust, and will building Smarter Markets be the antidote?
This episode is brought to you in part by Abaxx Exchange, bringing better price discovery and risk management tools to navigate today's commodities markets through centrally cleared, physically deliverable futures contracts in energy, environmental, battery materials, and precious metals markets. Smarter Markets are here.

David Greely (01m 17s):
Welcome back to Re-engineering Tokenization on SmarterMarkets. I am Dave Greely, Chief Economist at Abaxx Technologies. Our guest today is Ian Forester, Head of Product at Abaxx Technologies. We will be picking up where we left off last week and digging in deeper on the use of cryptographically secured identity and signatures to take that next step from digitization to tokenization. And we will be discussing Abaxx's approach to the four pillars supporting trusted commercial transactions: securing identity, intent, assets, and data. Hello Ian. Welcome back to SmarterMarkets.

Ian Forester (01m 55s):
Hey Dave, it's great to be here and I realize of the times I have been on the pod, this is our first time just you and me together, which is an exciting opportunity.

David Greely (02m 03s):
That's terrific. It's just you and me and I really appreciate you coming back so quickly, coming back this week. It was a really great conversation with you and Josh last week on the podcast and a great introduction to this podcast series and last week Josh noted that digitization has clearly been an ongoing path for decades and when we talk about tokenization, it's really the next step in that path and you remark that it's worth making a distinction between digitization and tokenization and that when you're talking about tokenization, you are almost universally talking about public key, private key cryptography tools. And I would like to pick up our conversation this week there because I feel we need to understand identity and how we demonstrate it online in order to understand how we can trust commercial transactions done in a digital environment. And that's really where we want to be moving to in this series.

David Greely (03m 05s):
But before we take that next step into tokenization, I wanted to start our conversation with the idea of identity in the more familiar context where all of us and our listeners are at now digitally. I know for most of us our digital ID is our email address and we're all accustomed to demonstrating that it's us by showing that we can receive email at that address. Is that essentially right? The way I put that in terms of our, our email address for many of us is essentially our current digital ID. And what are the strengths and weaknesses of that current approach to identity online?

Ian Forester (03m 46s):
Yeah, I think so sort of when we are talking about digital identity, I think it's important to make a couple of distinctions and put some definition around what a digital identity is. Because the truth is that each of us have a multitude of digital identities that get tacked onto us the same way that a farmer tacks an ear tag onto a cow, right onto cattle and this is represented in everything from cookies in your browser to your ISPs routing table. You can sort of think of the internet as a dark forest where platforms are running around sort of sticking air tags to people until they shake them off. And this world of digital identity is full of threads of activities that are tied to identities that exist as random serial numbers in a database somewhere. And I think what we are talking about when we are talking about digital identity are a sort of a high value subset of those identities.

Ian Forester (04m 44s):
And these are way more useful. And they have three qualities that I think define them that we can anchor on. The first is that they are persistent, right? So unlike, you know, when you are sort of online and you click a link and you see it has this question mark in it and it says UTM after you have seen that. So that UTM that stands for urchin tracking module and this is like one of those cattle tags, it's ephemeral, right? It sort of exists in your browser for as long as you use that link and then it goes away. But it helps ad platforms like Google and Facebook track provenance and user behavior across different domains. And I think that's important, right? That's what we are kind of looking for here is how can you track or how can you log activity across different domains. But you know, just for sort of practical takeaway from this podcast, if you take nothing else away, you can go ahead and delete all that stuff, right?

Ian Forester (05m 37s):
Like anything after the question mark, go ahead and delete it. Do yourself and your friends a favor. That's an example of a digital identity that's not really persistent, right? It doesn't persist with the user. So we want digital identities that are persistent. Those three characteristics that define this high value subset are that those identities are persistent. The subject of the identity can prove they control it so they can prove control over it. And they are portable. That means that they can be used across different domains. And it turns out that email is a great way to anchor those qualities, right? It's widely assumed to be adopted, secure, available. And for anyone who's downloaded Verifier Plus and created an identity using ID++ and using that app, they can tell you that we're using that same familiar standard in our own system. I think what's different about what we are doing is what happens on top of that, that email alias.

Ian Forester (06m 37s):
So we think of the email address as an alias, it's a way to prove control IDPs like Google do the same thing. And then what's sort of, I think under the hood and, and part of the plumbing is that those IDPs, they give you an identity, right? They, they give you another identity on top of that email address because While email is a great way to prove control, it's also not totally unique. Email addresses can be reused, et cetera, et cetera. So in and of itself, it's not like UID or a serial number or you know, a did, right? But it's a helpful alias and it's a way to, to sort of prove control. What happens after the email address is I think the important part because when Google gives you a number, that number becomes your identity and when you want to use that identity in another platform, you basically have to phone home to Google, right?

Ian Forester (07m 32s):
That that other platform that you are logging into has to give Google a call and say, Hey, is this, is this one yours? And they say, yep and then Google marks it in their book, oh, this person logged into here, or Oh they did this or Oh they used us here. Okay. And then sort of along you go on your way, I think the opportunity with decentralized identity is to remove that need to phone home, right. So by creating or sort of by using PKI, which is the abbreviation for public key infrastructure and the abbreviation for the stand in for public key private key cryptography by using PKI to prove control over an identity, we can sort of cut that phone home out of the loop, right? The DID is persistent. It's not reliant on a central system to maintain its integrity and a digital signature can be used to prove control over it. So there is really no need for that phone home. The authentication does not require daddy Google to approve it. It can be approved between two parties bilaterally. And I think that's a key intersection of, of where it becomes useful in markets.

David Greely (08m 56s):
And I'd love to dig into that a little bit more, but I want to come back to something you said. This is really interesting when you referred to the email address as an alias and then there is an actual equivalent of a serial number or a social security number that the email provider has use Google as an example, but I would never know it existed. I would never know what that was. Is that right?

Ian Forester (09m 20s):
Yeah and you can't directly prove control over it. You need Google to prove control over it. And I am picking on Google, but this is how all these systems work, right? Like any identity provider, you are sort of trusting them to prove control on your behalf. And did as stands for decentralized identity with decentralized identity, I think the exciting thing is the ability to you yourself prove control over it without anybody else's permission, right, without having to rely on that central counterparty.

David Greely (09m 53s):
Right and let's take that next step then into tokenization and public key, private key cryptography. First in layperson's terms, so talk to me like I'm a first grader here. What is public key, private key cryptography and how do we use it to create this new form of digital identity?

Ian Forester (10m 14s):
Basically the history of it, it's nothing new. It was first created in the 1970s. In fact, we are coming up on the 50th anniversary of Diff and Hellman's paper that they published at Stanford in 1976 detailing the implementation of the first public key private key protocol and today we use it as it is the foundation of trust and security online, you see in in the browser HTTPS, that little s. So that S means that there is a certificate somewhere that is signed from the publisher of this webpage that they are accountable for it. And they have done that signature, they have signed that certificate using public key private key cryptography. So each of us is benefiting from it every day and I think what's interesting in terms of the opportunity ahead is to take that same sort of signature scheme and use it in more day-to-day commerce sort of scale that out.

Ian Forester (11m 18s):
So I think that is to say that it's proven in terms of how it works. Basically it's skipping all the math. It's two keys, a public key which can be shared with the world and you can think of this as the address to your PO box. It's your PO box number and then there is a private key and you can think of this as the key to the PO box, right? So anybody can use your public key to send you mail, but only you can use your private key to get the mail and when I say only you, I think that's a really important aspect here and something that we have spent a lot of time on, how do we ensure that control of the private key remains with the rightful party and because really it's the controller of that private key who sort of says the key to the castle, right?

Ian Forester (12m 07s):
This is the, the key to everything related to that identity. Anything that gets built on top of that identity is subject to the that private key and the way that the keys work is that they're linked by math, by algorithms so that the public key can be derived from the private key but not the other way around and that's where we get that number two on the list of identity requirements, the proof of control, right through the exercise of that private key and that exercise is typically known as signing cryptographic signatures or, or signing is how that private key is exercised.

David Greely (12m 42s):
I just want to make sure people don't get confused since we were talking about email addresses a moment before. So when thinking of the public key and the private key, they're both basically numbers or strings of numbers and letters. Correct. And so if I have a private key, I can encrypt a message that I send to you and if you have the public key, you can decrypt it and read it and the same in reverse. If you have the public key, you could send me a message encrypted with the public key and only I with the private key could read it.

Ian Forester (13m 16s):
Yeah, what you are quoting, there are some really well known cryptographic signing protocols. So this is where we get into what's a protocol. It's a way of doing something, right? It's an agreed upon method of taking an action could do step one, step two, step three, step four. That's the protocol. So with a cryptographic signing protocol, you are absolutely right, you would sign using your private key, I would decode that encrypted signature using your public key.

David Greely (13m 47s):
Could you walk us through like an actual signing message that you send to me that's new relative to say an email?

Ian Forester (13m 54s):
First I am going to start with a story. So in the 80s and 90s, you know the rock band Van Halen, there was this rumor going around that they were they big divas because part of their contract when they showed up to do a live show was that they had to have a bowl of

brown m and ms in their dressing room and the rumor was that they were big divas, but the truth of it was that they were the first rock show with a huge setup that included a lot of pyro and they were playing venues like the electric factory in Philadelphia, which I think you and I are both familiar with, Dave and that's a small venue and you can get really hurt if some pyro goes wrong there. So buried in their rider, they had this Clause that said you had to put a bowl of brown M&Ms in the dressing room and this became their canary in the coal mine, right?

Ian Forester (14m 41s):
It was their shorthand to see if somebody had actually read the rider so that the pyro was set up correctly and Eddie Van Halen wouldn't get lit on fire, right and that was their shorthand. If there wasn't a bowl of brown M&Ms in the dressing room, they said, Hey look, we are not going on stage until literally everything is checked, which can take hours and delay the show. I say that in the context because a hashing function is sort of at the root of all this. The way that a message is assigned message is sent is that first, that message goes through a hashing function and this is like a one-way trans modifier from Calvin and Hobbes, right? Where like the message goes into the box and it comes out totally unrecognizable and you can't reverse engineer, you can't go backwards from a hash message to the original, but you can put the same message in and get the same result. So it's consistent.

Ian Forester (15m 35s):
And so what happens is the sender will hash the message and then they will encrypt that hash using their private key and that's sort of the signature and then they will send that package, they will send the original message along with the signature, which is the hash that's encrypted with their private key. The receiver will then, they will receive that package, they will hash the message again on their side to get their result, and then they will decrypt the signature from the sender using their public key and then they will compare the hashes and it's like the brown M&Ms, right? If the hashes match, then the brown M&Ms are in the dressing room and everything's good. If the hashes don't match, then you know that there's something fraudulent going on and not to trust the message and so that's I think, how assigned message works, right and sort of fundamentally how digital signature works too.

David Greely (16m 36s):
And that's simple but very powerful, right because it's conveyed a lot of information in a small number of steps. You have got the unencrypted message that you have received, which you could read fine, you know, just send over email, whatever. But you know that the message that you can read hasn't been altered from the message that was originally sent. So you know, it's the same message that you got that the receiver sent. So it hasn't been manipulated en route. You also know that it was sent by that particular signer. So you have kind of connected back to them and then you also get some measure of intent like they intended, they took a number of steps to get this to you, so they meant to send it to you and they meant it to be that document. So you have actually conveyed a lot of information that's necessary to trust the message in a pretty small number of steps.

Ian Forester (17m 29s):
Exactly and we think of those along sort of three lines. One authenticity, you sort of rightly stated. The signature is the attestation from the control of that private key that the message originated with them. It's an authentic message, the integrity of the message, packets get lost, data gets corrupted. How do you know that this is a full and complete record of that signer's intent? Well, because you have the hash and you can verify that yes, this was the complete message and then non-repudiation, and I think this one's incredibly important for our use cases in markets because that's signature lives with the record, the holders of that record have proof that the signer can't repudiate those claims later and I think that goes back to what you are saying about intent. I know we are going to talk about the four pillars of, of a transaction, but repudiation and re-characterization are two very pernicious challenges when it comes to digitizing and tokenizing assets and kind of moving, moving the world of, of money online. Because without digital signatures and cryptographically secure digital signatures so much can be, can sort of fall under the, under those buckets a re-characterization

David Greely (18m 46s):
Where you could just walk away and say, well no, I never sent that message.

Ian Forester (18m 49s):
Yeah, I actually had this experience when I was running my last company. I had a big contract that was going to come through for this agency. It was in the sort of marketing technology world and I had to hire very quickly to get this project done and it wasn't sure if the project was coming through or not coming through, but I was in a position where I had to commit funds right away and the head of the other company signed, I got the DocuSign that this thing was signed and so I started spending money and then a week later she came back and said, oh no, I never signed that. My assistant signed it on my behalf. That's not a genuine signature. I can't, we are not moving

this thing forward. And I was like, really? I was in a really tough position. So these things do have real world consequences, you know, that that was a case where she was able to repudiate her signature because it wasn't done in a secure way.

David Greely (19m 44s):
Maybe we need to get to this later after we have laid a little bit more groundwork, but how do you avoid repudiation with digital identities or decentralized identities?

Ian Forester (19m 53s):
I mean the most important thing, and this is why our, we have spent a long time with the Verifier Plus app, the most important thing is ensuring a solid connection between the person and the act of signing and we have this in the real world. The other thing is, none of this is new. We are simply doing our best to model in the digital space what we already trust in the analog space. I have sort of an unofficial motto that I don't really share with people, but I will tell you and our listeners, which is make the internet paper again, how do you take the secure and verifiable and provably scarce qualities of paper that have built so much of, and honestly data preservation. I mean papers have been a great medium for preserving data over the centuries. How do you take those qualities and move them into digital space such that we can preserve those tenants of analog real world deal making in and among the dark forest of the internet.

Ian Forester (20m 57s):
That's the challenge, those small feat, but that's the challenge that I think us and you know, everybody working in the space is really trying to tackle to. So again, it goes back to how do you tie back to that person? How do you take the action of signing this thing that we do with our hands and put it in a digital space? And you know, I think 20 years ago there wasn't really an answer for this. These days though, we all have this incredibly secure, highly personalized cryptographic signing device in our pockets. For us it's through the Verifier + app. For instance, when we do document signatures, we require a multifactor, multifactor authentication on, on device through Verifier +. So that's how a signature gets done. It's through proving control at the time of signature using that sort of secure pipeline that we build through Verifier Plus to the cryptographic material.

David Greely (21m 58s):
And this opens the door to many other use cases, right? From verifiable credentials to placing identity on data, not just people and I was hoping Ian, maybe you could walk us through one or two of these use cases and why they're so important?

Ian Forester (22m 15s):
Absolutely. I think what's important is that from a foundation of authenticity, integrity and non-repudiation, this allows us to build abstractions and assign information that can be very, very helpful. So one example, a really good example is a verifiable credential. What is a verifiable credential? Well, fundamentally it's token that has within it claims that are being made about a subject which could be a digital identity by an issuer of that credential and that issuer is signing these claims. The well-worn example is a, a university degree, right? Once you get your degree from a university, it's very unlikely that somebody's going to take that away from you. So a university can issue that degree as a verifiable credential and make the claims that this person completed this course of study and here is all the evidence for it and put that all in a machine readable format and sign it, right?

Ian Forester (23m 17s):
And so now when that person shows up to me and says, I went to Northwestern University or I went to University of Chicago, then they can present that evidence to me as a verifiable credential and as long as I trust the signature or as long as I trust the identity of the issuer that this is a genuine issuer, then I don't have to call Northwestern or University of Chicago and say, hey is this, did this person really go here? You know, I don't have to have them check their records because they signed it. I trust their signature and so now I can start to interact with people bilaterally using third party information that's been signed and attest it to, right? As long as I trust the signature, I can trust the information. As long as I can trust the information, I can interact with this party based on that information without anybody else having to know, right, without having to call a third party, without having to call daddy Google without having to independently verify and somehow docs myself that I am engaging in this transaction or engaging in this, this interaction with a person.

David Greely (24m 29s):
And so it's a little bit like making, as you said earlier, making the internet paper again, right because now you and I could meet, you might not know me, I could say I am going in for a job interview, right? I can pull out my driver's license and that's issued by the state of Connecticut and signed by the state of Connecticut that says, hey this is Dave, here is his picture, this is where he lives, here's his

birthday. Could pull out my passport from the US government, another signed document. I could pull out a my degree from college, I could do all these things and I could show you the paper, but now I could present that to you in a digital format and you would be able to check it without having to talk to the state of Connecticut or the US government or the University of Chicago or what have you.

Ian Forester (25m 22s):
Exactly and so we are sort of taking the best of that paper-based technology and then because it's digital, we can add to it where, hey you are Dave, you want to prove to me that you went to the University of Chicago, but for some reason you don't want to tell me what year you graduated. Well if you are showing me your degree, I am going to see that information, right? If you are showing me the paper degree but because you can show this information to me using a assigned presentation, you have the opportunity to pick and choose which data you show me. You have the opportunity to using zero knowledge proof, say, Hey, you are asking me this question that's a yes no question. I am going to reference the data that supports my answer of yes or no and provide you a yes no answer that you can trace back to the verifiable credential without seeing what that answer is. Right, so there's all sorts of ways that we can use this to not only accelerate the, what we can already do on paper, but actually add these capabilities around privacy to keep interactions on a need to know basis.

David Greely (26m 35s):
It also raises the idea too that you can raise the level of proof depending on the level of trust required for that transaction you are entering into, right? Like there could be one level of transaction where, hey, I just want something equivalent to like knowing it's you. Maybe that's the driver's license. There could be others where, oh, I want a lot more layers of trust, I want more third party endorsements, maybe even before the driver's license. It's just somebody we both know saying, yeah, that's Dave. But I feel like in kind of the current environment, things are often very binary, right? You have control of the email address or you don't, and that might be fine for certain degrees of transactions. For others you might want a lot more proof about who this person is and what they are capable of and from maybe higher trust third parties kind of vouching for them.

Ian Forester (27m 30s):
Well yeah, and I think you hit the nail on the head with the third parties because that's how 90% of information online is, is validated through trust in third parties and I think this really limits our ability to create transparent functioning markets that are based in technology. Because if you always have someone else in the room watching you transact simply because you are using their platform, if the data around a transaction is trusted because it is held by DocuSign should be unrelated third party, you know what happens is this third party sort of gets put right at the center of each transaction and then we have seen this happen in other markets and advertising media and I think commodities markets participants are smart enough to have seen this trend and say, no, no thank you we are not going to do that. We are not going to give technology provider perfect knowledge over our market activities. Because what inevitably ends up happening is that technology provider at scale becomes the most important person in the conversation, right? Google and Facebook have edged out advertising and media companies and sort of created this barbell effect where because they are in the room for so many of the transactions, there is no competing with them, right? You have this sort of monopoly power and it's not because either of the founders were incredible media creators or publishers or advertisers, it's simply because they controlled the venue and the source of truth.

David Greely (29m 06s):
There is a lot of the ideas that are floating around in this conversation. I would love to kind of bring them to a focus and really talk about how we use these to do real important commercial transactions. Ones where things are at stake, we have talked about digital identity, the ability to cryptographically sign a message and want to see how that kind of all comes together. And I know you have talked about your approach in terms of the four pillars of a transaction. Some of you could walk us through those pillars?

Ian Forester (29m 40s):
Yeah and I think that's a great place to anchor. So when looking at how we apply these, these systems that use cryptography to make information portable and trusted, no matter the domain, when we look at how to replicate instruments that confer ownership based on identity versus possession and when we look at aligning this with the market and with the use cases in in our markets, I think we have to look at it. We sort of have broken it down on four axes, which we are calling the four pillars of a transaction and this is for any transaction, right? Sort of scales, but certainly gets more important as the stakes get higher and those four pillars are secure identity. You have to be secure in who you are dealing with, right? You can't have a transaction with one person and then midway they switch to a different person that doesn't work, right?

Ian Forester (30m 42s):
Or you need to have a consistent secure identity throughout the transaction. The intent has to be secure and the data has to be secure and I am sort of bunching these together because they are related. So transactions are all about intent at the time of transaction. You have to make sure that your, what you intend to happen is what's actually happening and what you are agreeing to is what you are actually agreeing to. And then your counterparty needs to make sure that whatever you have agreed to, and we have talked about this several times, you know, you can't just say like, oh well I didn't say that right? I didn't sign that, or Oh my assistant signed that because they had my DocuSign login or something, right? Like, so that intent has to be secure both during the transaction and after and this is I think one of the biggest pieces because re-characterization and repudiation, if the system allows for those things then it's not a useful system.

Ian Forester (31m 33s):
Nobody can really rely on it, especially as the stakes get higher. So the tools that communicate that intent have to be secure, they can't be corrupted and then this is where secure data comes into play. The, the record of that intent must be stored alongside the transaction and the transaction data and that data must also be secure. And then obviously you have to have a secure asset and that's where I think we can rely on and you know, certainly many firms who are approaching this are relying on existing infrastructure, BNY, Mellon, you know, the sort of network of asset custodians and warehouses that currently exist. You have to be able to work with those systems, with those stakeholders. So that's the four axes and then how do we sort of bring that all together so that each of those pillars can be secured by the signature so that that digital signature that we place so much on can function as the anchor, as the trust anchor for each of these four pillars. That's really how we are approaching this build out with our various tools and APIs and workflows.

David Greely (32m 48s):
And how difficult is it to get the signature at the center and to have the signature accomplish so many important tasks that it secures the identity, the intent, the asset and the data?

Ian Forester (33m 02s):
Well I am not going to not say it's easy. It certainly take a while to sort of figure out and build out each of those pillars but fortunately there is a lot of prior art that we can draw on and I think that's important because if we were up here doing something entirely new that had no relationship to anything existing that would be very difficult to trust, you would need a decade of burnout before anybody could use it for anything. I think what's important that we are doing is we are looking at, okay, what are the absolute tried and true trust methods of working in that dark forest of the internet? What has been working for 50 years, for decades and decades? How do we combine these things in a novel way using advents like massive mobile phone adoption, right and acceptance of sort of mobile phone as a proxy for the body. Taking an action the same way that a physical signature is. The ways that we combine those things becomes very important and also I think a lot of fun because we get to see what works and people sort of say, what is the ID ++ protocol that that's what it is, right? It's the protocol that defines all of those interactions and the steps for doing these things.

David Greely (34m 28s):
Well thanks Ian. I appreciate you having this conversation because I know it you are working on many deeply technological issues and it's not always easy to express it as succinctly and at the first grader level and the relatable way that you have today, so I appreciate that. I know it's not an easy thing to do. I know you have got your head down working on a lot of next steps in the process. You've got a whole program of digital title pilots that you're conducting at Abaxx, but if you could lift your head up for a moment as we close out, kind of like to just leave it with you. Think about where all those steps are leading, kind of like what's the North Star that is keeping you on your path. And if you'd look down the road and said, hey, if in whatever number of years I looked back and the way we did things was different, you would feel good about what you had accomplished. What's that North Star that you are moving towards?

Ian Forester (35m 30s):
Well, I think it comes back to my personal North Star and the North Star for Abaxx are incredibly aligned and what it comes back to is the ideas of freedom. Permissionless action in our digital space as well as personal property and specifically personal property protected by the Fourth Amendment in digital space are almost non-existent. The way that things have been organized up to this point, sort of my personal mission is to restore those things. I think that we would have a better, just everybody would have a better time if that's the world we lived in. I think where that meets up with Abaxx is that we fundamentally believe in markets and markets as a way to discover the truth about something. That process of discovery requires that same level of agency and privacy and sort of control over one's information and sort of effects, right?

Ian Forester 36m 35s)
In order to work I think basically for markets to work, they must be free. And when we look at the trends around digitization and sort of the move towards electronic markets, what we see are a lot of central choke points or sort of said earlier, the daddy Googles, we see these companies that are really on a mission around creating perfect information and perfect visibility, creating the Panopticon where they sit in the middle and see everything that's going on. And I just don't know how a market can function as a truth seeking mechanism when it is surveilled top to bottom and all of its participants actions can be predicted before they happen. I don't see how that market can function as a tool for discovery, and I think that's where I think we are heading with all of this. We are at least making a very honest effort to right that.

David Greely (37m 39s):
Thanks again to Ian Forester, Head of Product at Abaxx Technologies. We hope you enjoyed the episode. We will be back next week with another episode of Re-engineering Tokenization. We hope you will join us.

Announcer (37m 53s):
This episode is brought to you in part by Abaxx Exchange, bringing better price discovery and risk management tools to navigate today's commodities markets through centrally cleared, physically deliverable futures contracts in energy, environmental, battery materials, and precious metals markets. Smarter Markets are here. Contact sales@abaxx.exchange to get started.
That concludes this week's episode of SmarterMarkets by Abaxx. For episode transcripts and additional episode information, including research, editorial and video content, please visit smartermarkets.media. Please help more people discover the podcast by leaving a review on Apple Podcast, Spotify, YouTube, or your favorite podcast platform. SmarterMarkets is presented for informational and entertainment purposes only. The information presented on SmarterMarkets should not be construed as investment advice. Always consult a licensed investment professional before making investment decisions. The views and opinions expressed on SmarterMarkets are those of the participants and do not necessarily reflect those of the show's hosts or producer. SmarterMarkets, its hosts, guests, employees, and producer, Abaxx Technologies, shall not be held liable for losses resulting from investment decisions based on informational viewpoints presented on SmarterMarkets. Thank you for listening and please join us again next week.