Episode 151: Dylan Dewdney on Truly Private Crypto Transactions

Kelley Weaver: Welcome to Crypto Token Talk, a crypto 101 podcast exploring how blockchain applications like Bitcoin, Ethereum, and other crypto assets could change the world. Learn from watching experts, thought leaders, and founders of some of the most innovative companies and world-changing ideas of our time. I'm your host Kelly Weaver, CEO of Melrose PR, a leading blockchain communications agency. Thanks for joining us today.

Today I'm here with Dylan Dewdney. Welcome, Dylan.

Dylan Dewdney: Hey, how's it going? Thank you.

Kelley Weaver: Going well. So tell us a little bit about who you are and how you first discovered crypto.

Dylan Dewdney: I am a boy from Iowa, originally, and then I discovered crypto. I'm now in Toronto. I discovered crypto ... I guess it was late 2012. I think it was 2011 the first time I read an article that was on a news aggregator called Metafilter about people transacting in this crazy thing called Bitcoin, sort of had some initial interest that was primed at that point.

Then I think late 2012, I started to really dig into it. And then on 2013, there was a bit of a jump, as we all know, in price. And I really dug into it at that point, and read the white paper, and then got involved in a mining capacity, mining Litecoin at the time, some of the [inaudible 00:01:18] that was coming out, and then eventually got turned on to Ethereum, and then participated in that idea. Just got involved in the community to some extent in Toronto and that is the beginning of it. And then from that point I got involved with a founding team on the [inaudible 00:01:36] token that later became a protocol called Harbor. Most recently, and the thing I'm really excited to talk about today is my involvement in another protocol called Mimblewimble and my team, our project's implementation of it which is called Beam.

Kelley Weaver: Fantastic! So, tell us a little bit more about the backstory behind Beam Mimblewimble or however you want to phrase it.

CRYPTO TOKEN TALK

Dylan Dewdney: It's actually... yeah! No problem. It's actually got a very compelling backstory to Mimblewimble. The protocol or the idea rather, or the protocol, was dropped very anonymously on an IRT channel just by totally anonymously.

Kelley Weaver: What's an IRC channel?

Dylan Dewdney: It's basically a private, anonymous channel for mostly a lot of developers use it and hackers [inaudible 00:02:27] to do messages and forums and stuff like that.

Kelley Weaver: Okay.

Dylan Dewdney: Its like basic paper or outline for the protocol was sort of dropped there anonymously. I think it was in late 2016. I think it was November 2016. And some notable sort of cryptographers looked at it and said, "Oh, hey! This actually makes sense! This is really interesting. And has maybe some legs to it."

It's very similar to the way Bitcoin sort of started in the sense that it was an anonymous start and then later developed on by other people. The person who dropped it, it's called Mimblewimble, and there's a lot of Harry Potter references throughout the lore of this protocol. Whoever started it was obviously a Harry Potter fan. Mimblewimble is a spell in the Harry Potter series that basically tongue-ties whoever the receiving end is of that spell so they can't say any spells themselves. And I guess the idea behind this is that the Mimblewimble protocol itself doesn't allow anyone to look into what's going on within the ledger.

So, opposed to things like Bitcoin and Ethereum, where we have an idea that there's an anonymity to it, or that people won't really be able to track our transactions or anything. They're highly auditable and they're public, basically. So, the idea behind Mimblewimble as a protocol is that there's going to be a way for people to transact privately and anonymously through some elegant cryptography that's probably way beyond my expertise, but nevertheless works under the hood. And the guy who dropped it, his name is Tom [inaudible 00:04:22] which is a French jumble of Voldemort or whatever way Voldemort is written in French. It's Tom [inaudible 00:04:31].

Kelley Weaver: [laughing]

Dylan Dewdney: Yeah, it's very similar to Toshi Nakamoto. Very, very similar genesis story or origin story to this protocol.

Cryptotokentalk.io   **#askCryptoKelley**   **@cryptotokentalk**

Don't forget to subscribe so you never miss an episode!

Kelley Weaver: What types of applications are going to be built on top of this for people who may not be as familiar with protocol layers. What sorts of things are going to be powered by this?

Dylan Dewdney: Our project, we really hope that it's going to become a pretty pervasive store of value is sort of the main application at this point. One of the things that it's ability to be so private sort of [inaudible 00:05:09] or cuts out of the picture, as opposed to Bitcoin or Ethereum, is the ability for scripting. Basically, when the information doesn't become necessary between transactors and the ledger, so when that gets [inaudible 00:05:26], doesn't really... but it doesn't really allow you to do scripting. You can't really do a programming language or do, say, like, when someone turns eighteen these funds will get released. That sort of thing you see in Ethereum, but that's okay because it does satisfy two of three very important and very hard to nail objectives or watching technology which is scalability and privacy. It nails those two things.

Kelley Weaver: Mm-hmm (affirmative).

Dylan Dewdney: And I think that's something that people are willing to give up in order to nail those two things almost one hundred percent. And the way it achieves this privacy is actually through its scaling, so it would end up being a tenth of the size of the blockchain for Bitcoin. That's awesome, and it's also a hundred percent private. It's theoretically and practically impossible to know what people transacted. There's nothing stored in the ledger between two parties that are transacting that would be able to be seen.

Kelley Weaver: So is it going to be used as a currency, do you think? Like a private currency?

Dylan Dewdney: To be used as a private currency, I think that you need something to be super scalable. I don't know. It's hard to say at this point. We don't expect we'll be the very last word on [inaudible 00:06:56] blockchain or a private blockchain. I think at this point it's got great utility as a stored value that would never be beholden to any central authorities or really anybody except for the parties that are transacting. So, I think that's really it's main value. Even if you look at...

Kelley Weaver: So, it could be used more like a Bitcoin versus something for day-to-day transactions or, I'm sorry, like a long-term store of value like gold?

Dylan Dewdney: Yeah, we believe it's definitely a store of value, and there's definitely transaction ability too. It's very similar to Bitcoin although Bitcoin is clearly auditable, and

you can tell who is transacting with whom if you really want to. With Beam and our implementation of Mimblewimble, there's really no way to tell who's transacting. So our mission really is that whatever money you hold or value you hold should be completely yours and private to you with no scrutiny by anyone else on that.

Kelley Weaver: Interesting. I have a question about financial privacy technology. Do you think that regulation will be a threat to this or do you think it's totally bulletproof as it relates to... I mean you mentioned that no government or anything could have access to this. What do you think about that?

Dylan Dewdney: Regulation is precisely why these privacy chains are coming to the floor and becoming more important as we go on. Because we're seeing the regulatory pendulum swing back now, right, from the hay days of, you know the summer and spring of 2017 with the [inaudible 00:08:41] and everybody saying the regulators are coming. Well, they've come now, and not only have they come, but they've also [inaudible 00:08:49]. I think something that is an Achilles heel of the ascendant and dominant blockchains right now which is that they're not [inaudible 00:08:55] to central authority the way that the initial [inaudible 00:09:01] we all hoped, right? Regulatory frameworks will not, theoretically, be able to get into... I mean nobody can really audit an implementation of Mimblewimble in a classic sense the way that you would audit a public blockchain like Bitcoin or Ethereum or ever private coins or chains like Monero or Z Cash or Dash because of the completely different technology, and it's a completely different protocol cryptographically speaking.

The only way, theoretically... I guess you would have to have a human hack or a social hack where you would literally have to be... you'd have to have four people. Somebody transacting on a computer with somebody else using Beam, and then you'd have to have somebody next to them Face timing what was happening in real time at the same time. That would really be the only situation where people could know anything.

But my expectation is that... there's probably going to be... just the same way that regulators are kind of coming down a little bit on exchanges. Exchanges are kind of the fail point and success point, if you will, of the whole ecosystem. So, exchanges have this undo influence and dominance that I don't think anybody foresaw in the beginning.

Kelley Weaver: Because you need them to trade one this for another.

Dylan Dewdney: Yeah, yeah. Right, right.

Kelley Weaver: So, fundamentally, you need them...

Dylan Dewdney: I mean they're kind of the gatekeepers right now. And they're making massive amounts of money. It's fine. But I think that would be the point where I think that you could argue, hey well, if exchanges aren't listing any of these privacy coins or maybe then Beam, which I don't think is going to happen by the way, but let's say that they don't. That could be a point where at least indirectly regulators could put pressure on those kinds of points.

I'm a really firm believer that people will find a way to transact privately if the technology is out there [inaudible 00:11:18] them to do so. And I also think that centralized exchanges are on the way. I'll make a prediction right now that in a few years, and I know I'm keeping this vague by saying a few years, let's say two-to-three, I really don't see the longterm defendants of centralized exchanges. I mean eventually the technology is going to be to a point where centralized exchanges will become sort of defacto. I think that will go a long way in stopping the point of failure, I guess, for the ecosystem if you want to call it failure.

I mean it's also a great success too.

Kelley Weaver: The only thing that I foresee is that you're always going to need a centralized exchange to convert [inaudible 00:12:01] currencies like to US dollar into cryptocurrencies. That on ramp is always going to have to be regulated, so it's always going to have to be somewhat centralized, but I don't disagree that once you get a step beyond that... let's say you have Bitcoin or Ether or whatever...

Dylan Dewdney: Mm-hmm (affirmative).

Kelley Weaver: Then you could find a place to exchange that isn't centralized, but...

Dylan Dewdney: Agreed.

Kelley Weaver: I feel like that's unfortunately just par for the course.

Dylan Dewdney: You're right. There are themes out there right now, one project which I'm an investor in, so [laughing] full disclosure, ramp network which is making it super easy to on ramp to crypto.

Cryptotokentalk.io   **#askCryptoKelley**   **@cryptotokentalk**

Don't forget to subscribe so you never miss an episode!

Kelley Weaver:	That's cool.
Dylan Dewdney:	Yeah, and I think that those types of projects will sort of lessen that friction and also take it away from the province of exchanges and maybe arguable make it a little bit harder to come after people who are going [inaudible 00:13:02] to crypto or whatnot. I take your point. It's true [inaudible 00:13:08] to crypto is also a bottleneck too.
Kelley Weaver:	Yeah, but, you're right, as these systems are created from a user-friendly standpoint, the friction is going to be less so it's not so clunky to do that. But, you mentioned a term I want you to explain a little bit further: fungible. Can you explain that for those who may not be familiar with that term?
Dylan Dewdney:	Yeah, I'm sorry. Fungibility is just really basically the idea that if I go to a bank and I have a hundred dollar bill and I give them that hundred dollar bill it's the same as any other hundred dollar bill. It doesn't matter if that hundred dollar bill came from a drug dealer or if it came from... at least the country I live in [inaudible 00:13:54] but Justin Trudeau, right? So every unit has to be the same as any other unit. And the thing that ensures that is the anonymity and the privacy of those units. We don't know necessarily where those dollars came from.
	Sometimes you get outlier situations where you'll have a celebrity that signs, for example, a dollar bill, but even that, now that dollar bill is worth two dollars or whatever the case may be. It's imbued some extra value. Although, I might add, it's illegal to deface bills, and the reason for that is that they remain fungible, that they can't be necessarily discerned from any other.
	Now you might argue that every bill has serial numbers or something like that, but in terms of practical, everyday use we don't care one bill to the next. It means the same thing. Correct or incorrect?
Kelley Weaver:	Yeah.
Dylan Dewdney:	That is the idea of fungibility, right? And the problem when you have blockchains or cryptocurrencies that are easily auditable is that all of a sudden you know where all this stuff is moving, right? There's huge implications here. Not the least of which is protection of commercial interests, right?
Kelley Weaver:	Mm-hmm (affirmative).

CRYPTO TOKEN TALK

Dylan Dewdney:	Do you really want every transaction of your business to be known to the world?
Kelley Weaver:	Right. I feel like that's a fundamental difficulty with crytocurrencies is just the fact that if I send you Eth, you can check on Etherscan and then see exactly how much is in your wallet, how much is in my wallet, I mean granted you might have multiple wallets, but it is clunky. We don't live in a society where there's that kind of transparency. Or people don't even want that kind of transparency.
Dylan Dewdney:	No! Privacy is super important. And I think everybody who has transacted either in Bitcoin or Eth has a little bit of... especially if they keep the same wallet or they've kept the same wallet for some time, it's like, is someone going to go through my wallet and you can actually look at all my transactions right there for everyone to see. And it's almost like anybody could do that. Unless you just send from a different wallet every time. It's super clunky, right?
	Anyway, going back to that point about commercial interests. It's highly important that we protect this misinformation. I don't want, for example, a vendor to know that I paid the other vendor less than I paid you, right?
Kelley Weaver:	Right!
Dylan Dewdney:	Because you should get the same deal, et cetera, et cetera. That's why things like Bitcoin or Ethereum, any public blockchain is going to have some serious issues when it comes to business applications, right? And that same idea comes all the way down to the individual. Do I want people to know that I bought an electric skateboard for a couple thousand dollars, which I did by the way.
Kelley Weaver:	Right.
Dylan Dewdney:	Which is like... oh, and I guess I'm telling everyone that now.
Kelley Weaver:	[Laughing]
Dylan Dewdney:	But that's super extravagant and maybe, maybe not extravagant, but I love it, right? But do I necessarily want everybody to know that I spent that much on something? Not really. Right? They could easily see that in an auditable, public blockchain.

Anyway, going back to your question about fungibility, one of the, I think, ways that fungibility is ensured is through privacy, it's through anonymity, and yet, the idea that we can't track these transactions. If I walk up to you on the street and give you a dollar unless I'm being followed by a private investigator, no one's going to know about that, right? Unless I want them to.

Kelley Weaver: So the Beam Mimblewimble protocol is going to, you mentioned that this is going to solve for a longterm store of value. Are there any projects out there that you feel like are doing the same thing that are solving for more day-to-day transactions or not that you know of at the moment?

Dylan Dewdney: Well, there's a number of different scaling solutions out there that are being tested at the moment. We'll see, and that's true for Ethereum, and that's true for Bitcoin, and a lot of other blockchains. And that remains to be seen, so I don't know. I guess the kind of holy grail or the idea is to get the point of being able to process millions of transactions a day like Visa. Not even a day, but I think like a second or a minute?

Kelley Weaver: A second or something like that?

Dylan Dewdney: A second? A minute?

Kelley Weaver: But yes, volume. [Laughing]

Dylan Dewdney: Volume, right? TPS - transaction per second. That's right. There's solutions out there. I don't know of anything that right now, this second, and my research has been minimal by the way on what's out there, but as far as I know nothing out there is at the point of Visa or MasterCard levels or the combination of the two.

I mean, if you look at Bitcoin though by way as an example, if you're trying to get it to scale to those levels, I think from the research I did on that at least recently is it would be able a hundred and twenty-seven terabytes to download the full blockchain. And that's through some research by a guy by the last name of Nadeem. So, nothing yet that I can tell as far as anything that approaches how credit cards work today. But that said, I think it's on the way. I don't think it's an insurmountable problem or it's a challenge, it's not an obstacle at this point, I think. And I think that Ethereum and Bitcoin, both those teams or projects are trying to figure out different ways to solve that through [inaudible 00:19:43] or et cetera, et cetera. There's a number of different things out there.

CRYPTO TOKEN TALK

Kelley Weaver:	Is there a reason Beam has chosen to tackle the longterm store value?
Dylan Dewdney:	Beam is focused first on... right now Beam scales way better than Bitcoin ever could.
Kelley Weaver:	Mm-hmm (affirmative).
Dylan Dewdney:	At this point. But the idea of it transacting in the millions of transactions per second is probably a long way off. Our first mission and our first goal is to have a completely private blockchain that's also highly scalable which this is. That's our first mission. And in terms of being a world currency or whatever, we'll see. We have a great team of developers and we're building a great community, so who knows?
Kelley Weaver:	Yeah. Tell me a little bit more about your involvement specifically with the project.
Dylan Dewdney:	My involvement specifically is to sort of evangelize the project and basically bring our implementation of Mimblewimble to broader awareness to build communities around the world. We have a number of communities that have already begun in Toronto, Tel Aviv, believe it or not, San Juan is now a crypto hub in San Juan, too, Dublin, and New York we've also started. So, we're sort of building organically. We're organizing meetups very similar to I guess, if you will, the Ethereum model when they first started they were just getting people excited about this protocol because I think it is something to be very excited about.
Kelley Weaver:	That's awesome, and you have plenty of experience building communities through past projects that you've been involved with. [inaudible 00:21:25]
Dylan Dewdney:	Yeah, I think so.
Kelley Weaver:	Fantastic! Well thank you for taking the time. Do you have any resources that you recommend for people who are looking to just get started in this industry? I think you're a big fan of Reddit, right? And places like that?
Dylan Dewdney:	Reddit is great. And really just Google and people are great. But I'd say really just ask the right questions is the main thing. And get involved in people that you know. From the very simplest, Google is probably your best friend, right? So I would go that route. But, yeah, meetups are cool too. Like, if anybody's

listening that's from Toronto, come to our meetup coming up in the next couple weeks actually.

Kelley Weaver: Fantastic. And how can people join the Beam community or keep in touch with you personally?

Dylan Dewdney: They can come to our website beam-mw.com.

Kelley Weaver: Fantastic. And then are you on Telegram or Twitter or any of these things? Email?

Dylan Dewdney: Yeah. We have a Telegram and it's beam community, I think. And we have an Instagram. I think we have a Twitter now. There's a lot of different ways to get in touch. So our Twitter is beam privacy and our Instagram, I think, is beam privacy as well.

Kelley Weaver: Fantastic. Well thank you so much, Dylan, for taking the time.

Dylan Dewdney: My pleasure. Thank you.

Kelley Weaver: That's all for today's episode of Crypto Token Talk. To learn more about blockchain and keep up-to-date with this fast-paced industry, subscribe at cryptotokentalk.io where you can also find today's show notes. If you have suggestions for topics or guests, please drop me a line on Twitter at cryptokelly or you can follow the show on Twitter at cryptotokentalk. If you enjoy this show, please rate and review it on iTunes and share it with family, friends, and colleagues who want to stay up-to-date on how blockchain technology is changing the world. Thanks for listening.

This podcast is for entertainment and informational purposes only and does not constitute financial or investment advice of any kind. Cryptocurrencies are an extremely volatile and risky investment. You should not make any decision financial, investment, trading, or otherwise based on any of the information presented in this podcast without undertaking independent due diligence. Anyone wishing to invest should seek his or her own independent financial advisor.