Mathieu (00:25)

Yeah, so big news today, I guess, in Europe as we're recording this. As I was preparing for this, I was reading a blog post that you guys had written and there's a section on regulators and there was a quote from there that says "*regulators can make or break markets. one of the main barriers to the widespread adoption of decentralized identity was the lack of data sources that could issue trustworthy digital identity credentials.*" And today we see identity regulations emerge across the globe, spearheaded by the European Union with its eIDAS 2, which will pass into law in less than three months. Well, it seems like it's as of February 29th, 2024, that it's passed into law.

I'm sure there's a lot happening around that and a lot of excitement. It would be interesting if regulation really could make or break new markets that we kind of start there, at least from a European perspective, just to understand the significance of what just happened with eIDAS 2.

Dominik Beron | walt.id (01:29)
Yeah, sure. Happy to talk a little bit more about this. Let's kick off with the eIDAS 2. I think we picked a good date for hosting this conversation because as you said a little bit earlier today, the eIDAS 2 went through the formal voting in the European Parliament and it passed. And so we're one step closer to formal adoption of eIDAS 2 regulation, which is obviously big news because as you know, eIDAS 2 is really the first globally the first legal framework to introduce identity wallets and holistic digital identities for citizens and organizations across a very large economic zone in the world. And so you touched upon a very important point, which is the problem that decentralized identity used to have, or still having to a certain extent, the lack of access to good data and data sources.

And as you know, one of the reasons here is really that in many ways organizations that are authoritative data sources or organizations that have a lot of valuable information built their business models around, you know, walling up that information and selling access to it. And so what eIDAS 2 is definitely changing here is that it will force governments not only to provide identity wallets to citizens in order to facilitate the whole rollout and make sure that every European citizen organization can have a wallet that they can use to share identity information with. They will also issue identity information to these wallets. And once certain core information about people is in their wallets, a lot of other people will follow, or let's say a lot of other data sources will also follow to issue these credentials.

So regulations in that sense, and the eIDAS 2 especially, is something that's crucially important or let's say a great driver of all of this in decentralized identity because it's not only providing you with wallets, empty wallets, but actually with wallets that have identity information with it, which you can use in a lot of different use cases. So definitely a big day. I don't want to say it's the only important driver or trend that we're seeing. Right now, there's a couple of other things happening, which clearly show that even without eIDAS 2 decentralized identity is happening, whether you like it or not. But it's definitely great to see that even regulators are pushing this new technology or this new, let's say, way of thinking about identity.

Mathieu (04:09)
Are you seeing interest from organizations? You mentioned that the traditional model is to have your data sitting within the four walls. I've always wondered what the economic model is for organizations to invest in making or offering their closed data to their customers or employees or whatever in a way that would make it more open because I always wondered what the benefit was to them. But I think we all… everyone has the vision that as an ecosystem grows and there's more people or more organizations contributing credentials and more exchange, like there's more and more value that gets unlocked and you could kind of hit a hockey stick type of thing. But are you seeing more interest now from organizations that because the credentials are coming to citizens and organizations from authorities, are you starting to see more interest in not only wanting to consume, but looking at issuing credentials themselves?

Dominik Beron | walt.id (05:08)
Yeah, for sure. I mean, I think talking about these traditional business models around trusted identity information, we definitely should distinguish public and private sector data sources, right? I mean, selling access to trusted data is also something that's happening in the public sector. If you think about stuff like company registries, for example, in many countries, including mine, you would have to pay a fee to access company registries, which makes sense because it's used by the private sector and so in a way, it's been used to fund this public service.

But taking away the public sector, which I believe is and will be changing as this whole mindset of regulators changes and is aligned with an understanding that people and organizations should be in control of their own information, should be able to freely share it without unnecessary barriers. Looking at the private sector, we're also seeing the same thing happening. And so, traditionally you had identity verification companies, background check companies, all of these organizations that perform some kind of identity verification, doing this one -off verifications and over time building a pool of data about verified users, which could potentially be reused.

I mean, you even see this today where some identity verification services talk about reusable identity. And it's not decentralized identity. What they're meaning is, they verify a person for one customer, and then they kind of share in the background with a centralized database. They kind of share this verification for the other customer to make it a little more cheaply. And what we're seeing is that, a lot of folks in those spaces are now looking at decentralized identity for different reasons. The most important one, I think, being that if somebody's starting to issue credentials and offer identity wallets and make this available, then that destroys the whole ecosystem. If not everyone's walling off the data and following the same model, then it's very difficult.

And so we're actually working with a number of different companies in the background verification and identity verification space already, who are really looking at transforming their whole business model, understanding that in this new world where you don't have the walled gardens and the silos, but a new world where people have identity information in their wallets and can freely share it.

They rather be first to adopt this and push this and have a very important position in the ecosystem for the use cases and their existing buyers to monetize it in a different way than being late to the party. Obviously, that means being brave and potentially cannibalizing your own business model. And so it's definitely not everybody doing, but we're working with a number of folks already.

And so I think that's definitely something very important and a big trend that we're seeing. I mean, probably you've seen a lot of the announcements of acquisitions in the identity verification space, identity verification companies starting to announce identity wallets or joining projects and consortia, which are all about enabling wallet -based identity. So I think everybody knows about this.

And with eIDAS 2, especially in Europe, this becomes even more interesting because now it's basically a situation where they all know that in a certain period, in a certain, like in, let's say, the next two years or so, governments will give out identity wallets with identity information that you will also be able to use for AML regulated use cases, or let's say, generally user onboarding, right? And so if this is provided, what is then the new model that they would have to offer to their own customers and the product such as that you can have more seamless user onboarding?

And so I think many understand that they have to get into the game quickly to remain relevant. Maybe one last thought here. I'm not at all saying that traditional identity verification will become obsolete. Of course, it won't. Even looking at identity wallets in Europe and the UDI wallet, we won't have 100 % coverage from day one. And so there will always be a number of a certain subset of people who won't have identity wallets or will only have them after a couple of years. And so there will always be room for traditional identity verification. There will definitely always be room for companies providing biometric verification, right? Because that's something that's inherently not included in decentralized identity, as at least we're doing it.

And so, you know, the products are just changing a bit and the dynamics are shifting. But that doesn't mean that, you know, you will see a complete eradication of companies from one day to the next. It will rather be a slow, not when I want to say slow, but an iterative or a transformative phase where you will see decentralized identity gaining more and more adoption and market share for these types of, you know, markets around identity verification, access management, and so on.

Mathieu (10:28)
Yeah, I always felt like the identity verification companies, at least like kind of what you're talking about that, that do like a document authentication type of thing would be disrupted by this. Not that, you don't need it sometimes for onboarding. You definitely will continue to need biometrics in certain situations, but I always felt like their investments in more the transactional monitoring businesses that kind of fit into AML over time was kind of a move to de-risk that so that you're not just left having to do a doc auth or a biometric for onboarding transactions or very few transactions, but you could at least have the life cycle afterwards and just plug into all sorts of

transactional data sources from banking to crypto to all these other things. Do you see a lot of pushback against this eIDAS?

Dominik Beron | walt.id (11:29)
Because I think that's also important to understand. There are certain decentralized identity companies that are talking about actually replacing those identity verification companies or identity access management tools. I don't see it. I don't believe it. In a sense that, you know, we are actually working with those companies, helping them adopt decentralized identity. From our standpoint, decentralized identity is something that you could use across verticals, across industries. It's very broad, right? We're working with customers from more than 15 different industries on all kinds of use cases from, I want to say, the traditional user onboarding, which falls into the scope of identity verification to stuff related to education, employment, supply chain, organizational identity, and identity of things. And so for us, this whole topic is much broader. We're generally not interested in you know, going into a specific vertical or a specific use case. Instead, what we really want to do is work with those companies that already have a customer relationship, right? They have distribution. They already know the customer. They know the pain points. So for me, it's much more about enabling those companies, just like we're enabling AdTech companies, HR tech companies, GovTech companies, right? Offering these services to their existing customers. So I mean, I'm seeing it more in a sense that different services are becoming more important, but I don't think that this would necessarily mean that companies will vanish. If they adopt, I mean, they already know how to sell identity verification solutions. They know their customers. I think they're very well positioned if they just adopt the technology.

Mathieu (13:13)
Yeah its almost like just using a different input that becomes available to do the similar types of things that you're doing. Do you see any pushback against the eIDAS 2? I think we've been talking a bit about disruption in particular technology providers. Do you see pushback or people that have negative sentiments and which I'm sure you do and would you be able to talk about maybe some of these negative sentiments that people have and then we can maybe have a discussion around just the, hopefully more nuanced discussion, around like the validity and just talking about these concerns that people have.

One that I hear is that the European Union is trying to regulate too soon before adoption is happening type of thing. So it's almost like creating the standards, creating the regulation before you even know how the market's going to play out. Whether that's a valid criticism or not is the type of thing I would like to maybe discuss with you.

Dominik Beron | walt.id (14:20)
Yeah, for sure. I mean, let's start with that one. I mean, it's a European regulation. So there's obviously lots of different voices that don't like different parts of the regulation and that see issues. And I mean, it's very difficult to hit the right balance for these regulations. I mean, especially when we're talking about identity, you have to balance trust, security, and privacy, which to a certain extent are exclusive.

So you will hear people say, well, you know, it's not really decentralized or self-sovereign because, you know, it has many centralized aspects to it. And then you will see people criticize certain decisions with regards to maybe implementing acts or the ARF or, you know, more of the technical things that are coming with the regulation because they see privacy issues. And so it's you know, it's very difficult to say what's right and what's wrong. At the end of the day, you just have to look at look at what people are saying and you know, make up your mind about it on your own, right?

Is security more important in certain aspects than privacy? Depends, everybody will have a different opinion. But I think the point that you're making is quite interesting about regulating too soon. I mean, I think the European Union and the Commission, they are very much aware that they're fast in regulating this. I mean, in many ways, it feels like eIDAS 2 is just a necessity, and that's also one of the reasons why it developed so quickly. You just had a number of issues with the eIDAS 1 regulation that were in a way unintended and really detrimental for adoption.

So you had issues around the harmonization. And so you really saw different ways national governments started to implement the eIDAS 2 and look and make sense of the different parts of the regulation. And so that definitely wasn't helpful for adoption. And as a result, you've also seen, you know, limited adoption by the private sector. And so at the end of the day, what that means is you have some countries like Germany, which had a very secure system, for example, but very low adoption. Because I'm sure you know, Torsten Lodderstedt, in a meeting, he actually showed me his card reader, for example. So you actually needed hardware for it. And then there's countries like Austria that managed to solve the whole signature service in a better way. And especially thanks to COVID, made sure that a large percentage of the population could use it.

But even then, it's not like you could use your signature or authentication identification in the private sector. So it was,it's really limited to public sector interactions and even there mostly to basic use cases. And, you know, coupled this with this understanding of regulators that more and more power is aggregated in the hands of American companies, especially, you know, all these large social media companies being outside of Europe. And so I think regulators just had this urge and need to be quickly about finding a way for giving citizens more control over their data, making Europe less dependent on companies outside of Europe for this. And maybe even aligned with the thinking behind GDPR, be the force that is spearheading something that people in Europe feel is better than what we had before.

And so going back to this point about being the first regulator. I mean, it's definitely not making things easier. What the commission has been doing is, you know, they have tendered a reference implementation for the wallet. There are a number of large scale pilots where big consortia of public and private organizations are coming together to build use cases across different verticals like education, insurance, payment, travel. We're also working on a couple of these large scale pilots.

And so there was definitely thought behind, you know, putting these RFPs and large scale pilots on track too, while the regulatory process is ongoing and while they're even after, you know, the final approval also after the vote by the council, there's a, you know, a certain phase for implementation, making sure that while this is happening, people are actually using it and they can get feedback to get the ARF and de-implementing it as good as possible.

How good the implementing acts and the ARF will be, we will see. Right now its too soon to say. I think what's great for the whole decentralized identity space is that if you look at the ARF, there are a lot of the technologies that we know, like W3C verifiable credentials, SD charts, mobile drivers license, OpenID4VC. So a lot of the credential formats and protocols that are not new to us, as well as this whole concept of having issues, verifiers and a wallet.

And so, yeah, I think the next two years will be very interesting because, you know, the regulatory process is not stopping. Once the law is like a formal law is recognized as a formal law, this period for implementation will just start to run. And then after, I think, 24 months, there will just have to be adoption. Governments will have to provide identity wallets. Businesses will have to accept identity wallets for authentication identity, and identification of customers. And so this will just have to be there. And so it will be definitely a stressful time for everybody involved, for businesses, for governments, for the regulator and the folks working on the technical aspects of the regulation.

But on the other hand, you know, maybe mistakes will be made. Let's see how severe they are. But the whole regulation is definitely pushing the space forward and is driving, I think, a model for identity that's just much better than the last model has been. Regardless of all the discussions around privacy, security, I don't want to say small issues because some are big issues, important issues, and they shouldn't be neglected, but the idea behind this regulation is to have a user -centric model where people have an identity while they can control it. And so, yeah, let's see.

Mathieu (21:19)
You mentioned under eIDAS 1, there were different digital identity systems that different European nation states were offering to their citizens. They had various levels of adoption. I think you mentioned the German system and if you contrast that to maybe the Swedish digital identity or even the Italian digital identity system, they maybe saw a lot more adoption and integration within their daily lives.

With eIDAS 2, there is now alignment kind of foundationally from a technology perspective. You named some of the credential formats and the standards, the model, the credential exchange protocols that are being kind of mandated for these high assurance credentials. Do you think there's going to be more alignment in the digital identity offerings of the different nation states than during eIDAS 1.0 or do you think they're going to still be very divergent, one from another, if that question makes sense?

Dominik Beron | walt.id (22:24)
Yeah sure it makes a lot of sense. As I mentioned, people are really aware that the lack of harmonization introduces too much complexity for this to be really adopted broadly. And so one of the main goals of eIDAS 2 is actually to change that, right? It's to give people identity wallets that can hold potentially a lot of identity information for you. So there's just much more utility for you because the more information you have in your wallet that you can share, the more use cases you can build, the more interactions you can make more seamless. But making sure that there is interoperability and that this stuff actually works across border and across different organizations is definitely another vital goal. Because if it's not adopted, then what's the point?

And I think right now we're also at the point where it's quite clear that if it's not regulated in a way that makes sense, if we're looking at unregulated use cases, so let's say not AML regulated use cases, like opening a bank account or use cases related to gambling, for example, then the void will just be filled by offerings of the private sector, regardless of whether that's really user centric and user controlled or not. And so I think there's lots of strong motivations for getting it right.

What I also know is that there are different plans for making sure that in the course of these next two, three years, be it in the course of the large scale pilots, as well as outside of large scale pilots, having interop events and interop testing between different vendors. I mean, what I can tell you is that, as I mentioned, we're in a couple of, we're in different large scale pilots. Some are focused on UBSI, some are focused on eIDAS 2, and there's lots of other technology providers there as well.

And in these large scale pilots, we're already talking about and planning to build the use cases in a way that you can just replace one vendor with the other, issue with one vendor to a wallet provided by somebody else. And then there will also be formal interop events in the context of eIDAS too as well. So, you know, I think that people understand the importance of interoperability. I also think that folks at the commission and at the members states who have been engaged in the space since 2019, which is basically when the European Blockchain Partnership started to build EBSI and work on the European Self Sovereign Identity Framework, have been aware that interoperability was always a huge topic in the space and that if you're looking at decentralized identity model where you want to have different vendors be replaceable: If there's no interoperability, it doesn't make sense. It doesn't work.

And so I think a lot of effort is going into this and you know, it may still go wrong or there may still be hiccups. But I think that there's a lot of focus on this and a lot of awareness. So I'm confident that we'll get it right or at least better than the last time.

Mathieu (25:36)
You mentioned the European blockchain services infrastructure, EBSI. There's blockchain in the name. I think there's been ups and downs on just the utilization of blockchains in the architecture altogether. Have things changed since the formation of EBSI? And one of the other

things I find interesting, and it would be great if you could talk a bit about is, they have mentioned the things like smart contracts within the network that they have running as well, which goes a little broader than just using it for public key infrastructure or for storing schemas or certain things.

Could you talk a bit to the direction EBSI is going in and where it fits into everything we've just been discussing around the eIDAS and the architectural reference framework?

Dominik Beron | walt.id (26:31)
Sure, sure, happy to do it. Maybe starting with where EBSI started with, which was 2018/2019 or so, which was also the time that I got involved and was working with the commission and the member states, which I did for roughly two years, helping come up with the concepts for the governance and trust ecosystem, like the trust registries for different purposes, the data and verify our credential specifications, these kinds of things.

And since then, definitely, a lot of things happened on many different levels. As far as I know, I mean, I still know some of the folks deeply involved in EBSI and EPSI. And they're really, really good and smart people. You probably know, for example, you probably know Alan Horvath. He could probably tell you much more about EPSI than I could, but he's still involved and he's been there from the earliest days. And then you've also seen EPSI become more professional in the sense that initially they wanted to build or set up this blockchain, but there was not much thinking around building this ecosystem. You had the early adopters, wave one and wave two, but if you go to EPSI's website today, what you will see is a lot of documentation of how you can use it, of how it works, explanation of the trust and governance frameworks. You will see a diverse set of technology providers providing conformance solutions. And so I think they've really improved in the way they're communicating and in the way they're making it possible for developers and builders to engage.

Obviously, everybody can always improve, but comparing today with a couple of years back when we started out, you really can't compare it. And so I think why is EPSI interesting and how is EPSI tying into eIDAS 2?

So one way of thinking about it is that if you look at eIDAS 2, eIDAS 2 per se is not directed or does not directly enable all kinds of use cases across all kinds of industries. So the main focus is really around having a certain core data set for your identity wallet, which you can then reuse. And so one way to think about EPSI is as a complimentary identity ecosystem that is using different technologies to establish trust, like EPSI as a blockchain. And an ecosystem that may be a little bit more open, a little bit easier to build use cases on top because there's maybe less strict requirements in terms of the technology that you would have to use or certifications that may be necessary, for example, for wallets.

And so I can see a future where you have EPSI, the identity ecosystem for Europe that is being used by, you know, organizations working in the education space or in the HR space or other verticals. And I mean, we're seeing this already today with large scale pilots that are focused on

EPSI and building use cases in education and insurance, in user onboarding, and in travel. And so, you know, I wouldn't look at it as something that's competing, which is definitely not. I would look at it as two complementing ecosystems for slightly different purposes that can work together. And that at the end of the day, companies like us will just be abstracting so that at the end of the day, a citizen or a business won't even have to know in which ecosystem they're at as long as their trust requirements are satisfied. Does that make sense to you?

Mathieu (30:33)
Yeah, it makes a lot of sense. And you could, if you're getting credentials from either one of these ecosystems based on their own trust frameworks, then you should be able to use them elsewhere. So it's just, it's just a different route of trust type of thing.

Dominik Beron | walt.id (30:50)
And you see this not only with EPSI, right? There's identity ecosystems emerging all over the place. Sometimes, I mean, on the one hand, you have ecosystems being driven by public sector or super national organizations. EPSI is one example, but you also have GLEIF, which is betting on a different set of technologies, but it's also quite interesting. And then you have ecosystems that are emerging that are focused on specific verticals like HR, or you have ecosystems that position themselves as a universal ecosystem to establish payment rails for decentralized identity. Like Velocity for HR, for example, or Cheqd for the payment rails.

And then you see individual customers that we're working with, both from the public and private sector, also thinking about, you know, would it make sense to launch their own trust ecosystem? Typically if they already have a lot of valuable information and just bootstrap from there and build their own ecosystem around it. So it feels a little bit like, you know, in crypto, when you had Bitcoin and then came Ethereum and then came all the other layer ones trying to challenge Ethereum.

And so, I mean, until today, you know, we don't yet know who will be successful and who will still be alive in the next couple of years. But it feels a little bit like in the identity space, where it makes even more sense to have different ecosystems driven by different organizations, considering that identity is just so... Identity is just very different from payments and that it's just not universal.

It really always depends on who says what about who, right? And do I trust that person? And so it makes sense to have different identity ecosystems for different governments or different industries, or maybe even identity ecosystems spun up by very powerful companies that just already build an ecosystem of suppliers or technology companies that are building on their own solutions. And so at the heart, we're just looking at a multi -ecosystem future and that needs to be abstracted and EPSI could be one of those.

Mathieu (33:12)
That's a really good point you made about identity not being universal, like payments. And there's going to be thousands and thousands and thousands of identity systems based on their

own governance, their own authorities that have the right context within their own domains. And these all become… you need these centralized authorities that are able to provide that root of trust type of thing. But then they extend that into credentials or whatever. And then these could all be exchanged on the internet and trusted because of that root of trust. But it's not going to be one of these things. There's going to be a lot of them. And so that makes sense the way you describe that. I always felt like digital credentials could be very valuable. We talked about kind of the eIDAS based ecosystem or EPSI based ecosystem.

But I know you've done a lot of projects with different blockchain or crypto platforms as well. But I always felt like digital credentials would be very valuable inputs on open permissionless blockchain networks, where today everything is based on kind of public key cryptography, whether or not you're able to make a transaction happen type of thing, but if you could actually start to add some business logic or some inputs based on credentials that are coming in, you could start developing much richer experiences on these blockchain platforms than you're able to do today. So you could imagine even credentials coming from an eIDAS based route of trust being able to be presented on an Ethereum network into a smart contract to be able to do something in a privacy preserving manner on top of it.

Dominik Beron | walt.id (35:05)
That's a super interesting point. And we've actually did some work that relates to that recently, which I can talk about because we also had a press release with our partners about it. But let's take one step back and talk about verifiable credentials or let's say off-chain identity credentials in the context of crypto.

So, I mean, obviously crypto started and had very much love for on-chain identity using NFTs and SBTs for identity use cases. And a lot of folks thought that, you know, they could just do it until they realized that there's lots of compliance issues around this. And so you basically cannot do it, especially not if it's an AML regulated industry, or if you're talking about European citizens.

And so the big problem then, however, is, well, if it's not on chain, then you need oracles, or you somehow need a way to get this data on chain, because how would then smart contracts or dApps use it? And so I think that's still a very interesting and to this day not completely resolved question of, if you're thinking about DeFi, for example, but could be basically any other type of decentralized application or smart contract. But if you think about DeFi, permission DeFi was always a topic and how can I make sure that I, to a certain extent, whatever the type of verification is can somehow verify the users that are engaging with smart contracts. With the transfer of funds regulation, this will actually become necessary, such as that, if I am interacting with a non -custodial wallet, let's say my MetaMask, with a CASP in Europe or a VASP in the US, a crypto or virtual asset service provider, if I pull funds or push funds, I have to prove that I'm the same person. So how do I do it? Especially considering that crypto wallets don't yet have identity capabilities.

But even in thinking about stuff related to DeFi pools and permission DeFi, how can somebody who's engaging with a non-custodial wallet or who just wants to engage with a smart contract,

prove certain things about that person? And so that somehow implies that you need some kind of tokenized identity proof. And I think there's lots of interesting projects going on.

We ourselves had a project with the IOTA Foundation and IDnow and Bloom Wallet. I think there should be information on our website and the partners all published nice videos and press releases. But the main idea was that we've been working with IDnow, which is an identity verification company, so that if you're a user, you go into a website, you go through the video identification process provided by IDnow, you connect your MetaMask, you get issued a SoulBound token to your crypto address from IDnow. Basically nothing else. It only says you're verified, but nothing else. The data is obviously stored with IDnow to comply with legal requirements such as that if an authority wants to verify that wallet, they could go to IDnow. In addition, we're spinning up an identity wallet and populating it with verifiable credentials. So you can use that off chain as well.

And so in this scenario, we tried to look at, OK, how can we achieve or cater to these needs for TFR compliance on the one hand, but then also in the long term, this idea of AML compliant wallet-based user onboarding. And so I think, you know, there's still some questions left to be answered by the regulators and the policymakers and the lawyers. And there's the EU regulatory sandbox for which projects like these are very interesting. But there's definitely a lot of room to grow and to explore. And I mean, looking at, which is another interesting thing, looking at crypto the last couple of days, you know, it feels like, you know, maybe we're out of the crypto winter and another crypto summer is coming and then there will be more attention in that field again. But this whole idea of using NFTs and SoulBond tokens in the context of identity is definitely not dead.

You've also seen lots of large organizations play more around with loyalty and memberships, all tokenized or tickets. And so I think we hit the peak in 2021, 2022, then we fell all the way down and now we're slowly getting back to the plateau of where everything makes sense again.

Mathieu (40:00)
I was frustrated this morning looking at coin market cap and looking at the Pepe token going up like 150% over the last day or the last week. I was looking at that token a couple of months ago thinking that's like a, it's a stupid meme token that's probably going to pump if the market pumps. There you go.

I'll switch gears a little bit. One of the topics I wanted to discuss with you was open source. Like everything we've been talking about today requires the need for open source code and open standards to be used for us to achieve what we're trying to achieve here, but as a company, walt.id has been very good at publishing code and putting projects out. I'm curious from your standpoint, do you have a background in open source or what was the genesis behind this open source strategy? And then as a company, how do you think about monetization around that strategy?

Dom | walt.id (41:01)
Sure, sure. So yeah, I mean, the origin story or why we chose open source, I mean, there's definitely a lot of different reasons. One reason is if you're building an open source company, you have a lot of great trickle-down effects from that related to your whole go-to-market strategy and how you can build teams.

Developers love to work on open-source software, so it's great for hiring. You create a lot of value for a lot of organizations by having open source software because you can just take it and try it and do whatever they want with it without even having to engage with the sales rep or with you or without having to fear about IP issues.

And so for Phil and me when starting the company, it was really about making it as easy as possible for organizations to adopt decentralized identity because we definitely wanted to get away from this old identity paradigm that we had. And it felt like open source is just the best way to make that happen. And also, you know, if you build open source software, there's just so much value that you are creating, even before you have to worry about monetization, right? Because there's so many organizations that now have access to decentralized identity tools and can convince their management if they're in a large organization or who could start building companies based on that if they're a small organization just getting started. And so it feels like the right thing to build a company that way.

And also, if it's open source, I mean, obviously you can also run closed source software on premise and have it self managed. But if we're talking about it, in decentralized identity, it just makes a lot of sense to have software that everybody can just run. Um, right. So to, to enable a really decentralized systems of issuers and verifiers and wallet providers, and so to us, it just felt like the right approach to build a company and also nobody else was doing it when we started or hardly anyone else.

And so, yeah, it just felt like the right decision. We've never really regretted it. I think we've just been doubling down. We started with, I believe it was building an open source identity wallet for a small European grant, and then, you know, it snowballed into building the whole stack and offering it and to this day, we've been super focused on building the best open source software.

So a couple of times, we've been talking about launching a SaaS service or building an enterprise version of our stack. But instead of focusing on these things, what we did last year, for example, was completely refactor our whole open source stack to make it even more useful for people. So yeah, so far, open source was the main focus, and it definitely will be for the foreseeable future.

Mathieu (44:16)
It's interesting in the space because there's no argument whether or not we need to be basing our stuff on open source. Like if you look in other technologies, like the generative AI, which is still going crazy from day to day from week to week, there's a whole competition between closed

source and open source. And some will argue that the open-source implementations are going to win in the long term, but it's interesting because we don't have that, like those competing types of implementations, let's say in the identity space, but it's, um, it takes a lot of talent. It takes a lot of money to continue investing, to build communities around this stuff. So, um, it's, it's interesting to build, um, you know, sustainability around these things because you don't want to just publish something and then you're not building a community around it. It's not being used. You want to build engagement, I guess. Are there key metrics like that you guys try to grow or achieve?

Dom | walt.id (45:26)
I mean, sure, of course, it's a goal to build an ecosystem of contributors, let's say to build a developer company, where you have developers contributing code or helping you identify issues or giving you input for new features. You also want to have an ecosystem of partnerships to facilitate distribution. I think the first is much easier to do if you're an open-source company. The second you can do also as a closed source company, but it's again easier if it's open source.

But to be very honest with you, while we're seeing engagement from the community and also from a number of customers, as they're being more invested and engaging more and contributing more, our expectation is that we are today and will continue to be the organization that's building this and that's building all important core features, right? Even if there's contributors who build great integrations or who may even be contributing to interesting or important parts of certain libraries. Our expectation is that we will be driving the development and we we're responsible ultimately for its success.

And so, you know, it really just comes down to, and I mean, you have your own company, right? It really just comes down to what kind of company do you want to build. And in the best case scenario, the type of company you want to build makes sense from a business perspective as well. And if you look at open source companies, I mean, there's a variety of very interesting open source companies that have been very successful.

You know, like HashiCorp, for example, is a great company. Although obviously, you know, looking at some of their products, they have decided to go away from permissive licenses and be a little bit more closed as they, you know, are growing post IPO, but, um, they've also been starting with building open source community, open source software, um, having adoption driven by the community, engaging a lot with the people who are using it to build the best possible products. And so I think as mentioned, there's just a lot of up sides from, from building an open source company and we've actually wrote a blog post about this. I think two or three years ago that you can also check out that explains why we decided to do it.

But yeah, going back to your answer, you know, we're responsible for the software and for its quality. And we're happy about contributions and about building developer community around it. But right now we're not really focusing or have metrics related to GitHub stars or, I don't know, contributions by third-party developers. Our metrics are much more focused on things that we feel at the moment are more important to keep us tied to reality. So our use of the metrics that

we're looking at are much more tied to, you know, ARR or revenue, top-line revenue or the number of customers that we're working with, especially paying customers.

We're also looking at open source users and metric around this, like unique GitHub clones and these kinds of things. But we're trying to build something that makes sense today as far as possible in the field that we're working in.

Mathieu (48:53)
Does walt.id contribute open source to different projects like either technology projects or even into organizations like OpenWallet Foundation and stuff like that, or is it more just walt.id hosting either like the libraries or SDKs and stuff like that?

Dom | walt.id (49:13)
Yeah, so far our main focus has been on building our own open-source software, not necessarily only contributing to or mostly contributing to third-party projects. If you know, this is directly related to our products or directly creates value for our products. We've been thinking, I mean, we're obviously in touch with the OpenWallet Foundation. I think what they're doing is super interesting. They already received a number of very interesting commitments for code contributions, so we're also thinking about, you know, if there's something that we could contribute, so that's definitely always on our mind.

To be very honest, we're just very focused heads down building and building also like building product as well as distribution partnerships and getting real clients, and so yeah, it's something where we're still looking at, we're evaluating. I think there's lots of value of contributing your code to foundations or communities that have a lot of traction and a lot of following, and it can definitely be a great enabler. At the moment, everything we're building is in our GitHub.

Mathieu (50:23)
You mentioned earlier you're focused on building the maybe lower level enablers for different implementers or for different verticals to build use cases based off of the stack. I'd be curious also from I guess a European lens of what you see happening in the wallet space. I know there's always tons of discussions about wallets, but how do you see or at least when you get the question from people if they should be investing or building a wallet with existing government wallets coming out with existing mobile phone wallets that exist through Apple or Google, that type of thing. What's your vision of the wallet space? Is it a good space to be in?

Dom | walt.id (51:09)
It's definitely an interesting space. So I mean, what will happen is it's very hard to say, right? There is definitely a future where we say, well, you know, 3 billion people already have payment wallets, and I think we'll be 5 billion, according to different estimates, in the next two years or so. And obviously, the biggest platforms are Google and Apple, and then, you know, maybe Samsung. And then maybe there's some large, maybe there's some large payment companies that also could achieve meaningful distribution. So there's definitely a world where you say, OK, well, those wallets are already top of mind for consumers. People already use them. They know

how they work. They trust these brands. And if those wallet providers just turn on identity capabilities, people will use that.

On the other hand, I mean, there will be definitely, at least in the short to midterm, folks building vertical or use case-specific wallet applications as well, because in this future where you only have your Apple wallet or your Google wallet or whatever wallet it may be, it's unclear if that would really work for all aspects of your life from a usability perspective or just how people are using identity wallets. Will they be using it the same way that people are using apps today?

Or will it be more something like a meta service that just appears whenever you need it? And so it's completely abstracted. But I think in the short to midterm, we will definitely see lots of folks building identity wallets for different use cases. I think you will see people who have a huge user base in different verticals, like education, employment, all the types of industries we've already been talking about will be providing their existing user base with identity capabilities for credentials that are useful in that specific context. I mean, you've seen, for example, LinkedIn do identity verification, rolling that out with Clear or with Persona. I've also been doing it. And so there's definitely also a future where my education credentials or work credentials are not in my Apple Wallet, but maybe they're on LinkedIn, because it feels like it makes more sense there. Or that's the place where I'm looking for where I'm looking for jobs. And so it makes sense to have my credentials there for a better user experience.

So lots of experimentation in the short to midterm. In the very long term, I think the goal would probably be that identity wallets disappear entirely. And it's more an experience of if you want to access a service, something pops up or scans your face or you give your fingerprint. And then the wallet is somehow, I don't know, built into the hardware and you don't even know what you're using necessarily. But it will be interesting in the next couple of years. And then government wallets are, for me, because you were also asking about eIDAS 2, government wallets will be completely out of scope here as well because in eIDAS 2, you have very specific requirements with regards to the EUDI wallets and also with regards to certification. And this whole way user onboarding works. And so, I think there will be government wallets. But knowing governments, even if they outsource the development of these applications, it will probably not be the best experience. And so you will have government wallets and then private sector wallets as well. And so the question then will become, what are the requirements for regulations on wallets as well? Also with regards to whether owners of platforms like Apple would have to open their hardware and open the products that they're providing to third-party services? Lots of interesting questions. So very difficult to say.

Mathieu (55:13)
There's also a big focus on digital signatures in the European Union. I think it's calling decentralized identity wallets "wallets", and then on the other side, having crypto wallets sometimes brings confusion. I think crypto wallets are actually a very good mechanism for signatures and there's nothing really else happening other than signatures. Nothing's sitting on there, nothing's on the edge. It's just you're interacting with a network or a platform and you're using it to sign.

How do you see that market developing for digital signatures? Because I think we're moving, well, we should be in a space already today, at least on the internet, that if things aren't signed, they're not to be trusted. Does the signature capabilities that come with eIDAS 2 start to solve some of these problems for citizens or will there be other mechanisms? I'm just trying to get a better understanding of how signatures fit into everything we've been discussing right now, which are at the core of credentials anyways, but there's tons of broader applications for them.

Dom | walt.id (56:23)
Yeah, sure. I mean, eIDAS 1 brought legal guarantees and facilitated the recognition and acceptance of legal signatures across Europe. So the whole idea was that an electronic signature can have the same legal value as a handwritten signature. So that was already eIDAS 1. But so obviously with the eIDAS 2, the eIDAS 2, the EUDI wallets will not only provide you with the ability to manage identity information and share that, but also with the ability to sign information like send contracts, for example, looking at use cases in education and employment, which are interesting because they concern everyone. Everybody has some kind of education. Everybody somehow works and gets a job. You will obviously be able to apply to get all your education credentials and then also apply for a job and then also sign the contract with your identity wallet, potentially disclosing more and more information about yourself as you move through the recruiting process.

And so the digital signature part, at least for documents, is definitely something that's baked into this regulation and that will come with identity wallets as well, because it's not really something new.

With regards to signing other stuff, I'm completely with you that it will become more and more important. Just think about the Democratization, I mean, there's lots of headlines that you see right now talking about, rising fraud, which is nothing new, but it's accelerating and how AI is democratizing this and how AI and generative AI, which you brought up before is democratizing deep fakes and all these other kinds of stuff that could be used for all kinds of nasty purposes, not only great purposes.

And so I'm completely with you. I think everything will have to be somehow signed, and everything will have to have to a certain extent some kind of root of trust in who created this? or is this really authentic?or does the person really have the IP? And I think being a lawyer myself, having left the field a while ago, I think there's just so many interesting questions to be answered. Before I briefly mention questions about whether regulators can or want to force platforms to open up, which has a lot to do with antitrust and monopolies and having a fair economy. But then looking at the whole AI space, a conversation that you hear more and more often is, how do you treat the IP? Like, if you have a model that generates content.

And that's inspired or takes up information that somebody has written or I don't know, drawings, paintings that somebody's drawn. Like how do you handle IP? Because at the end of the day, it's derived from something else. And so I think, why am I bringing this up? Well, if it turns out

that that's actually a real legal issue and that's actually a problem for AI, then signing everything and having a root of trust will actually become a necessity because otherwise it won't be possible to offer related services because you would have to prove that there's no IP violations and the product of what the AI model gave you. So I'm definitely with you. Signatures will become more and more important and everything will be signed sooner or later and probably also somehow linked to some form of, I don't know, identity proof or authenticity proof, which could be tokenized on a blockchain, right?

Mathieu (01:00.10)
Yeah, the good old blockchain. Domonik, thank you a bunch for doing this with me. I really appreciate your time and spending time on these topics that I think are going to be quite valuable for our listeners. So I appreciate you doing this.

Dom | walt.id (01:00.28)
Sure, thanks for having me again, always a pleasure to chat.