

Forging Ahead: Succeeding in the Digital Trust Business

Analysts and journalists meet two founders' ideas for changing the industry.

PARTICIPANTS



Donald Jacobs

CEO, E^NAT IP



Dan Pratl

CEO, Quadron



Scott Bicheno

Editorial Director,
Telecoms.com



Ryan Jefferies

Founder,
Passionate About OSS



Prakash Sangam

Founder,
Tantra Analyst



ENAT IP (Donald Jacobs):

Argues telecom, security, and identity systems each work well individually, but "context" - who authorized an action, under what policy, on whose evidence - doesn't survive handoffs between domains, especially once AI agents act autonomously. Calls this a governance-continuity gap, distinct from Zero Trust or PKI, which verify moments, not persistence across time and organizations. Cites NIST's February concept paper (which explicitly defers external/untrusted agent authorization) and the EU AI Act's recent high-risk deadline extension (to Dec 2027/Aug 2028) as evidence that standards aren't ready. E^{NAT} IP has created a proprietary framework (white paper at enatip.com), which would allow alternative implementations from their own.

Quadron (Dan Pratl):

Frames expertise as the scarce resource in an AI-abundant world. Proposes a decentralized, evidence-based "GitHub for expertise", capturing verified human judgment/work and using tokens, prediction/"credibility" markets, and trusted execution environments to reward and authenticate it. Positions LinkedIn as an example ripe for disruption. Explicitly rejects centralized arbitration in favor of peer-to-peer mechanisms with programmable economic penalties, plus GitHub-style on-platform remediation.

Cross-cutting issues raised by the panel:

- Standardization: Fragmented verification standards undermine trust; unclear who sets them.
- Arbitration/centralization: No clear "arbiter" for agent trust; centralized control contradicts the trust goal, but pure peer-to-peer lacks legal recourse comparable to existing regulated arbitration (e.g., credit disputes).
- Agent identity: Unresolved. Agents lack the permanence/definability of human identity; "what is an agent's identity" is still unanswered.
- Sovereignty vs. regulation: Decentralized, disintermediating models will clash with government control; Pratl expects eventual regulatory accommodation (SEC token exemptions, UBI pressure) but concedes this is speculative.
- Risk of dystopian social-credit outcomes if governance isn't transparent.
- IP ownership ambiguity: Who owns "expertise" generated under employment remains unresolved.

Overall the panel was impressed by the ambition and concepts involved. There is a distance to go before these concepts become mainstream.

TRANSCRIPT

AL

Hello there, and thank you all so much for joining Forging Ahead today. My name's Alex Lawrence, the managing director at Telco Forge, and I'll be your guide to the hour ahead.

Telco Forge was built from the fact that, in many corners of the industry you'll find people unhappy that telecoms doesn't seem to be succeeding quite the way it could or should be with initiatives like Forging Ahead. We're highlighting people doing things differently who might hold the keys to new opportunities and new perspectives. But we're not just showing you. We're also introducing them to a panel of analysts and journalists from different parts of the telecoms world to get their reactions, questions and comments.

Now, the session today is all about trust. As individuals, we're usually pretty good at figuring out who to trust in real life, but online, we're lost. We just don't have the same heuristics that we've evolved for the physical world to understand whether what we're being presented with actually is what exists out there. And cyber security is one thing for keeping you safe, but can the telecoms industry help actually create that online ability to discern between what to trust and what not? If so, there's a huge value there.

So, in terms of format for this hour, if you're familiar with briefings to the press and media, this might ring some bells. I'll give Dan Pratl, the CEO of Quadron, and Donald Jacobs, the founder of E^NAT IP, a brief time to introduce what they're doing. But the majority of the hour is for conversation and questions arising from those introductions.

It's unlikely to be a straightforward ride for Dan and Donald. So I'm sorry to you both for that, but you're in front of people who make their careers saying what they think and asking difficult questions, people who've been around long enough maybe to have acquired a certain sheen of cynicism. So we'll give them the chance to put your ideas to the test and sound out what you're doing. But for those of you in the audience as well, you're welcome to pitch in with questions in the chat, which I'll pick up and pass on too.

Putting Dan and Donald to the test today we have three long time three thought leaders from different backgrounds:

- Scott Bichenno, the editorial director at Telecoms.com
- Prakash Sangam, the founder of Tantra Analyst and
- Ryan Jeffrey, the founder at Passionate About OSS.

We'll be hearing plenty from them shortly. But for now I'd like to hand over to Donald Jacobs for five minutes or so just to introduce E^NAT IP and your key thesis.



Okay, well, thank you, Alex. I'm Donald Jacobs, founder of E^NAT IP, and I work on a problem that most of digital infrastructure hasn't fully named yet, even though it already determines whether anyone can prove who authorized what. Here's the way in.

Over the last few decades, every layer of digital infrastructure has become genuinely good at its job. Telecom, with continuity of communications and mobility identity systems now have federation so we can log into one service using credentials from another. Things move, failover and they keep running. Security now has zero trust and cryptographic attestation. And each of those is a real achievement. And I want to say clearly that this is not a story about anyone failing. It's a story about what happens at the edges of all that success.

Because when something moves, like a workload or an AI agent acting on someone's behalf, it crosses from one governed domain into another. And the thing that quietly gets left behind at that crossing isn't the data and it isn't the connection. It's the context. Who authorized this, under what policy, and on whose evidence? That context doesn't automatically travel with the activity. It has to be engineered to survive the handoff. And today it mostly isn't.



As an example, you ask an AI assistant to sort out a billing dispute. Your AI assistant authenticates to your account on your provider's customer portal. That's one system. In the first organization, it pulls your usage records from that provider's billing platform. That's the second system. It escalates the dispute to a third party adjudication service which issues a credit; that would be system three, organization two. And that credit triggers an adjustment on a partner's settlement ledger.

So that would be four systems, three organizations all from one request from you.

Now suppose something is wrong - the credit was too large or it should have never fired at all - and someone asks the simplest question possible: "Who authorized this?" The honest answer is that even if every system did its job, every handoff checked out at the moment it happened, still nobody can reconstruct the line of authority from the original request to the action. Every link was valid. However, the chain wasn't.

"low if you know this space you may already been thinking isn't that what Zero Trust and PKI are for?" And that would be a fair challenge. And the honest answer is that they help genuinely, but they verify moments and credentials, a signature, a session. Zero Trust verifies each moment, but pretty much in isolation. Governance continuity, which is what I'm here to discuss today, asks whether a verified context from moment N still holds at moment N+3, in a different organization under a different policy regime. This is a persistence and traceability problem, not an authentication problem. It's a gap between the disciplines, not a flaw inside any one of them.

I didn't really invent this problem. This gap has existed since the days I was in the satellite business or the first workload migrated between cloud providers and first identity assertion crossed the company's domain. What AI does is put this all under a spotlight. Because now the thing crossing the boundary can act, chain into other systems and make decisions with no human in the loop to quietly cover for the missing context.

DJ

Institutions are now naming this carefully. In February, NIST's National Cybersecurity Center of Excellence published a concept paper on identity and authorization for software and AI agents. If you read the possible use cases section, the project will focus on enterprise agents, where organizations keep control and visibility over both the agents and the systems they touch. The challenge of external agents from untrusted sources will not be addressed under this initial effort.

Then if you read the questions that they put to the community, some of their questions were, "What are the mechanisms for an agent to prove its authority to perform a specific action? How do you handle delegation of authority on someone else's behalf? How do you bind an action back to the human who authorized it?" Those are E^NNAT IP questions; NIST is now asking them too, but they're not answering them yet. And NIST has deliberately deferred these questions to a later iteration.

And now two weeks ago the Council gave final approval to an amendment deferring the high-risk obligations to December 2, 2027 for standalone systems and August 2, 2028 for embedded ones.

As of this morning, it still hasn't been published in the official journal, which means the original August 2nd date in three weeks is technically still the law. Europe is moving the deadline with three weeks to spare.

I want to be careful here because the reasons were mixed. They gave competitiveness, administrative burden, a fair amount of lobbying, and I'm not going to pretend it was purely a technical delay, but one of the European Commission's own stated reasons was that the harmonized standards an organization would use to comply were not finished, the standards bodies had not delivered them, and the Commission had even missed its own deadline for issuing guidance on how to classify a system as high risk in the first place.

AL

I'm sorry, Donald. I am going to jump in there because I think there's been a lot of material there already which is going to be food for thought for people to ask about. And I do want to make sure that we give you and Dan both some time to do your introductions.

But before I hand over to Dan to take his turn as well, I just wanted to check with Scott or Prakash whether you had any immediate questions or comments based upon what you've heard already about E^NNAT IP and this idea of the continuity of governance.

SB

What Donald said about standardization was interesting, because of the way he was describing the process of a bit of data or a customer journey, how it has to go through several platforms, several bits of manipulation. There's got to be some kind of standard to ensure that's still the thing we thought it was at the start of the journey once it gets to the end of it, if I understood Donald correctly, and that presumably is a matter for standardization because you can't have 100 different types of verification because they're not necessarily going to agree with each other.

So it's not necessarily a question, but that really jumped out to me from what Donald was saying is that one of the keys to trust is successful standardizing. And if we're struggling in that area, that strikes me as an issue.

AL

That is such a telecoms comment - one of the keys to trust is successful standardizing. It's a really interesting point though, and I would like to come back to that, but I'm keen to make sure that Dan also gets his time in.

DJ

Just so you know, I haven't told you about the continuity governance, but the whole meat of it, basically is in the last minute here.

AL

I'll throw the question back to you later on then, Donald. For now I'll hand over to Dan Pratl, the CEO of Quadron, for his introduction.

DP

Thanks, Alex. Much appreciated. Dan Pratl, CEO, Founder of Quadron. Quadron is the summation of, in retrospect, a very serendipitous path, starting at the Securities and Exchange Commission in the Great Recession, then into open source, into crowdfunding, and then into crypto. So a very odd, strange path that led me to the realization that we need a new systems architecture for the next generation of verification and identity.

So what is Quadron? Well, I'll tell you a little story about where we are today and where we're going.



Expertise is becoming the new scarce resource in the world; that really matters, and is going to matter more for the next generation of identity verification, because AI is making polished output incredibly abundant. Anyone can generate a proposal, a memo, a pitch or a strategy that sounds incredibly impressive.

So the old signals for recognition and articulation and reward of expertise are starting to break down. The question is no longer just can this person produce something that looks good? The question needs to become can this person be trusted to know what they are talking about?

That fundamentally changes identity. For the last Internet era, identity was mostly about access. Are you a real human? Do you control this account? Captcha helped answer that first question, and passwords, logins, two factor authentication help answer the second. But in an AI-driven economy, especially when more agents are acting on our behalf, that's simply not enough. An agent, an employer, a customer or a counterparty will need to know something more, deeper. What is this person actually trusted to know, decide and do?

Quadron's built around the idea that verification is the byproduct of real personal human ambition. When people pursue meaningful goals, they naturally leave behind evidence. The decisions they make, the standards they apply, the corrections they accept, the work they improve, the judgment they show over time. Quadron turns that evidence into a living system of record for expertise.

But we're not simply putting credentials on chain. A bad claim on chain is still a very bad claim. The harder problem's actually upstream, creating records that are worth credentialing in the first place. So the simple way to think about all of this is: Captcha proved you were human. Quadron helps prove what you're good for.

In a world of AI agents and abundant synthetic output, what becomes a new kind of identity layer is dynamic, evidence-based and continually updating information that actually helps individuals prove their work and reward them for it.

AL

In some ways very straightforward in terms of the concept. I certainly have a lot of questions there, but it's not necessarily my role to ask that. So again, I will chime in if need be, but I'd like to hand over to Prakash and get your first impressions of this.

PS

Sure. Yeah, Dan, what you said. So you're suggesting a third-party system that the systems will go check for, instead of credentials, the expertise and presumably you will manage that system. And for every query you provide a response on whether that person's expertise is valid or not. Is that what you're thinking?

DP

Yeah. We need to probably take a step back and think about what identity and verification look like in the future. I was there for the NFV and the SDN revolutions in telco when I was working at Red Hat. This is not a technical approach to this very critical question going forward. It's not what you would call a liberal arts or a humanities approach, like a compliance based approach. It's a blend of the two.

We need a new economic framework for evaluating human ingenuity and rewarding it outside of the intellectual property system today. And we need a new technological framework for deploying agents based on verifiable work that human beings actually are standing behind.

So think about this: we don't have a finishing layer for work that actually functions in the AI era. Individuals have gotten very good at creating memos, presentations, sending that to their boss in their Slack and their emails and calling it a day, right? And the presupposition there is that last thing you sent is the good and finished thing.

Agents don't work that way at all. Human beings need to work with agents in a meaningfully different way, that integrates a new technological framework for deploying agents on verified, finished work that individuals have been rewarded for.

And individuals need to actually accept a new technological framework from a company that actually rewards them for showing and giving the good work, the finished work. Because a lot of individuals in my personal experience view these new institutional AI solutions that aren't ChatGPT and Claude as either surveillance or training your replacement.

DP

So if you try to create a verification infrastructure that basically uses the information from individuals for an enterprise AI approach, you're not going to get the highest quality work from people, because they are very concerned with being replaced. You need a materially new systems architecture that does reward recognition and actually allows information to persist throughout an enterprise over the course of time.

That simply is not a technological or a liberal arts approach. It needs to be a mixture of both. It's a new economic model for identifying value and rewarding it.

I realize that was a little bit outside of the question that you asked me, but it's a more robust answer that I think sets a little bit of a different foundation for the conversation.

PS

Yeah, thanks. And I mean I'm happy just to go back and forth, but I noticed that both you and Donald have been talking about the role of AI in this, and how in particular agents change the game. So that said, if we go first to Donald and then to you, Dan, you can talk a bit more about this and how you see those agent frameworks fitting into your thesis and maybe find some parallels and differences between what you're both up to.

DJ

I think it would be good to have a little bit more understanding of the governance continuity product because I kind of had started the background and I don't know if you'd have a clear idea of where I'm coming from. So if I could go back a little bit. The governance continuity that I'm talking about sits in between the 3GPP, OAuth and zero-trust. It's in the gap because these agents now, they move between domains and context gets lost in that transition. So I believe it changes what we need to be concerned about.

We need to make sure we can maintain attribution, explainability, verification and accountability throughout the lifecycle of these agents and the networks. The way that the networks are currently set up today, I don't believe we have that capability. That goes back to, in my opinion, why we've needed to delay these rules and laws because the standards necessary for this to occur do not currently exist. And that's what we are able to bring to the table.

AL

I see Ryan nodding there quite carefully. So I'm interested to see what you make of that, given your background with OSS.

RJ

Yeah, I'm kind of fascinated what the arbiter is actually, because I guess I'm coming from a world where we've got things that are a little bit more of a tangible identity - you know, your customer verifications and things like that. I'm really curious as obviously we've got different actors now; we're not just talking about the humans that you're doing the KYC on, but you're actually now looking at agents and various other entities. And so yeah, I'm really interested in the arbiter of all of this. Is there a single entity like with KYC, where there's a level approval of identification of individuals.

DJ

There needs to be. There isn't at this point. The standards have not been created to put that in place. It is absolutely what is necessary, full stop.

PS

Yeah, just following up from that - if you, if you look at what like Google and others are doing, taking MCP protocol was the beginning for agents to communicate. Now they're taking to ATP and other protocols. So you have enough good interfaces to transfer as much information, and as much needed information as possible between the agents. Not too much either.

And it's a natural progression, because right now most of the AI is still human-in-the-loop when it comes to commercial implementation. And, and these systems will have to be put in place before we take the human out of the loop, right? And it is a progression and the development for this new world, in my view.

DJ

Yes, and I believe that's where the industry is trying to go. Of course humans are going to continue to use the Internet, but where we're at right now is in this development of these agents; AI systems that operate very differently. And the different solutions that I have witnessed thus far, they cannot keep track of the attribution, explainability and verification and accountability through the whole chain. None of them. When you ask "what happened?", the different parties can answer what happened inside their own domain. They might be able to tell you the change that they received, but you don't have this layer that can see everything and log everything and keep it as evidence.

DJ

I seriously doubt though there will be a centralized entity or a function that will oversee all of them, because there's so many different parties. I don't think the different parties will agree to be managed or controlled by single entities. So it has to be more a distributed, cross-vetted system where one agent not just talks, but directs the other agents to do something. It basically authenticates and establishes its authority and then communicates; then the other, the receiving agent receives information, orders or whatever that is.

PS

Yeah, they would have to possibly refuse the connection unless the authority is established. Right?

DJ

Absolutely. Because these applications need to be secure from end to end. And, you have parties on either end. The way that I view it, if they're not both part of a single fabric, I don't see how you can establish trust.

RJ

Yeah. And also, I mean there is also a little bit fundamental question as well. I mean there is identity. When you talk about persons, you know how you define the identity of the person. When it comes to agent, we still don't know how to identify an agent.

DJ

Exactly.

RJ

What are the characteristics of an agent? And human identities are permanent; the agents may or may not be permanent. Agents are created for specific tasks, they may disappear and so on. So - you might be going there - first you have to establish what are the attributes of an agent's identity, and then second step is how you manage and transfer and authenticate that identity, right? I think we're still at the first stage, of how do you define the characteristics of an agent? What do you mean by identity for agent?

RJ

The credibility or the reputé of an individual may only be credible within a certain domain. So there are certain areas that we're restricted to for the credibility or reliability of the expertise that we have as individuals. I'm quite interested along those lines of how that evolves with agents. In what domains are they credible that we can trust? What the actions they're trying to perform or the information that they're putting forward?

Similar to the question around the arbitration, I also wonder whether we've sort of talked a little bit about centralized arbitration versus we also almost got into peer-to-peer arbitration, peer-to-peer trust. So that where I was kind of going in terms of where is the arbiter? Where does it sit? Maybe it's at different levels across the estate.

PS

I certainly believe it's impossible to have a centralized arbitrator, because there'll be so many agents. And then that brings in Dan's question - so you are saying the authentication or the expertise level that you will certify or whatever, is that limited to humans, individuals, or that can extend to agents as well? Because agents, not exactly the same but similar to human beings, might also learn based on the repetitive tasks they do and then develop expertise, right? So you basically need to grade, if you will, these agents as well on doing something. It's like almost certifying whether they're level one versus level two or level three, for example. Is that what you're thinking as well?

DP

Yeah. I envision a world where - first off, Quadron's very much a social play as well as an institutional AI play. But the notion is there needs to be a GitHub for expertise, so to speak. And critical to that is the encoding and then the redeployability of verifiable expertise. I think skills markdown files very early lean towards this notion of "I know something that you don't know. Let's put it out there. I'll show you how smart I am." GitHub, Star, all of that. What about the evolution of that? The pride of authorship that I create. I think we're in the very early days of seeing personal achievement being replicated and redeployable in code.

I also think that the platforms we see today, where you go to someplace to meet other people, are largely going to go the way of dinosaurs, as will the advertising model. Over the next 10 to 15 years I think we're going to see a more of a decentralized approach as sovereign identity becomes more critical to our value proposition to the world, both from a pecuniary sense as well as a reputational sense.



And with that in mind, I think we see a very peer-to-peer, me-to-you transfer of value where agents become the conduit and the intelligence lives in network to enable those agents to do very discrete and specific things.

Humans are still in the loop, but only passively to provide guidance on what the aims actually are. Not to get too wonky, but I think prediction markets are quite valuable as a signal today to look at the appetite for individuals to actually start using speculation as a language of conviction about things.

I come from a Web3 background, so tokens are going to come into play here. And apologies for everyone who wants to roll their eyes on crypto, but I think all of these technologies are incredibly immature and there's goodness in all of them, and we need to package them together and do something productive with them. Like for example, open source. The development framework of the past 35 years never had a remuneration structure. It was always obligation or fascination that maintained these repos and we saw those failures time and again.

If we create some type of reputation based compensation structure using speculation, all of a sudden you can fill that gap. You can help people collaborate more effectively, by dynamically updating who you are, who you're engaging with and enabling your agents to have a basis of trust to engage with numerous individuals in a decentralized network with actual skin in the game. Like there's a loss there which forces people to do the right thing.

So, like I said, we need a new systems architecture for all this that's fully decentralized, based on real economic value changing hands with a basis of "If you do something wrong, there's a real economic impact on you, in the negative sense. This is this confluence of all of these technologies and philosophical frameworks we've developed over the past 30-odd years coming together to create new micro economies, new value structures, where network connection and intelligence in the networks is absolutely integral to all of it coming together and making sense.

AL

What struck me with both of you then is actually you're moving outside of, if you like, a very traditional structure whereby national regulation is the way to govern a process and this creation of trust or confidence, and instead moving much more to something which is trying to replicate on a huge scale, what we see in the physical world on a small scale. In a village, you know, somebody has the reputation so that, if you need help, go to them and they'll be able to do it. The other person knows about medicine and so forth. I mean, is that a fair thing to say? You're sort of trying to create this world village?

DP

Yeah. I mean, Reddit showed us the path of networks of communities. Reddit centralized, admittedly, but there is this situation where I opt in as the node connecting a number of different communities, and they can be as weird as they need to be. But the point is that individuals opt in to being the evaluators of very different communities and they create this dense tapestry of value. That's why the advertising graph on Reddit is so very valuable, because individuals are very much showing their hand on what is and is not valuable to them. Very different than Facebook with the infinite scroll. And you see everything now that is, I think, absolutely critical into the economy going forward.

I think we all can agree that headless solutions are where the world is headed. You don't have a rich UX anymore. You simply have intelligence that's giving, notifying, suggesting information to you from other individuals. And then the question becomes, "Can I trust this? Is this credible?" Then the next question is, "How do you actually do verification and trust in a headless environment, when you have to rely on the agents and where that information is coming from?"

It's an incredibly difficult question if you don't have economic value at hand. You actually have to risk losing something, which is basically capitalism writ large.

So to your question about a global community, we already have a global community and it's called capitalism. That's called public and private markets. My proposition is that expertise is the hidden, invisible value that actually supports all of the economic systems we have today. We've just never had the systems to capture and encode it, and then evaluate it and then monetize it effectively. And I think that's absolutely integral and to the notion of identity and verification going forward.

PS

Conceptually I get what you're saying. In terms of implementation, in a model that you can actually commercialize and implement, how do you see this being implemented? So you'll have an entity, maybe peer-to-peer, but there is a repository of feedback from all the peers about specific people? If I want to know if my agent wants to check with Dan and wants to hire Dan's agent for doing some work, this agent can basically query the repository on the reputation of Dan's agent, which will be built by all the peer agents, and then get that authority and then proceed. Is that kind of the system?

DP

You asked me a couple questions there. How do we monetize? I think it's a three-step journey. First off, you know, I'm not jumping to monetize it. I'm talking about how you put up a system and then use it to monetize. If this were 2021, I'd look you straight in the face and say "We're a Layer-one blockchain and we're going to launch a token, then we're going to reach escape velocity and then we never consider or get concerned with customers ever." That's not today. No.

I think that LinkedIn is a very rich target for the notion of professional and personal identity. I think if anyone's been on LinkedIn in the last six months, we all can agree it's just a social network and you're not really getting a lot of value out of it anymore. You can change your cv. There's no proof whatsoever.

That is an opportunity for us to conflate the personal and professional and then use that as the basis to start creating an agent layer for your value writ large. Not just professional value, but your value writ large.

So what we do there is we actually start thinking about creating a metacognition, we call it a future you that starts getting you outside of the using the AI Easy button. Everybody uses the AI Easy button to create this document, send this email, polish this, create that. What about the notion of skills? What about your expertise? Why was your judgment here so useful in going this direction or that direction?

DP

You start taking those interstitial decision moments across tools and you start mapping agents that actually feed from using MCP and other approaches. We're kind of at the vanguard of taking all of the information from those interstitial moments and creating very opinionated perspectives on who you are, and then baking that into an agent and then having conversations with you as you move from development work to distribution work to say, "Is this who you are?" And this Metacognition becomes more robust over the course of time, fades into the background, sits on surfaces that you already use - Telegram, WhatsApp, SMS, et cetera.

And over the course of time it doesn't become a brain that simply sits alongside of you, it's a true helper that helps you on discrete activities as well as thinking long-term about your utility writ large and telling stories of provable progress that are highly valuable to future employers, potential collaborators, et cetera. It creates a decentralized corpus of knowledge that then finds potential collaborators and uses features like prediction markets - we call them credibility markets - to create structured collaborations. And all of that is driven by a series of agents that are deployed by you, by the system, passively, manually.

So Prakash, it's not so simple. It's a fully decentralized approach with individuals operating as their own node as they see fit, deploying agents in the manners that frankly, if they want to optimize for streaming insight and monetize that way, using it to turn themselves into an API layer, they can do that. If they want to go and do discrete a la carte selling of their expertise, they can do that too. We want to optimize for full flexibility and create that sovereign identity.

PS

So you need agents to do all of that and you need trust in those agents to do that.

DP

Yeah. Go deeper down. So I view a time where this thin client right here (points to mobile phone) has a trusted execution environment on hardware where we're actually running small models at the edge. I think that's where the world is going. Good enough is good enough from an agent perspective, from a model perspective. And then agents have a continuous feedback loop running on the trusted execution environment, validating on the dynamically updating information being fed from that network.

I don't view that as in any way breaking the methodological approach to trust that we've identified.

AL

Scott, I'm aware that you've been quiet for a while. You look sort of deep in thought here. I want to make sure that we're covering all the bases. Thoughts?

SB

Thanks Alex. I have been deep in thought. I mean, what Dan describes I will only obviously understand it superficially, if only because I've only just been introduced to it, but it seems incredibly ambitious and far reaching.

When he was first doing his admirably succinct elevator pitch, one thing that sprung to mind was "Like Google page rank, but for people." Now I don't know how, presumably it's a bit more complicated than that, but at least you're nodding. So I'm not a million miles off. And yeah, I just thought, "Wow, what an ambitious thing."

And I note that you have this experience with crypto and blockchain and that sort of thing, and you talk a lot about distributed and decentralized. I mean, that's the only way it could work, because such a thing, if it did exist, if there was a central point of control, that would be a ridiculous amount of power to have in the hands of whoever had that control.

And obviously back to theme of this conversation. The fact that someone had that power would fundamentally undermine the trust that it's designed to create. So it would have to be really decentralized. And I certainly don't understand blockchain well enough to know how you do it.

But yes, if you could pull it off, and if there was a trusted system - obviously it begs all sorts of questions about what the criteria are and for it not falling into some sort of dystopian social credit system type of thing where you end up having some kind of punitive de-ranking for some fairly sort of accidental or trivial thing - but yes, if it did work as a concept, great.

That was why I was looking so contemplative, Alex. I was just trying to get my head around a world where such a thing existed. And I think it'd be fascinating, but it's so ambitious that I think you got your work cut out, Dan, getting there from here.

DP

Yeah, I wouldn't leave a cushy job making a bunch to do something that was 'AI for accounting', you know. No, it is ambitious. I also think we've seen this episode before. We did this with code 20 years ago, except we've identified now that the intellectual property system is anaemic and not suited for the times. And also we now have the ability with performant blockchains and AI to actually build something like this, and build that very distributed compensation mechanism or that remuneration structure that simply wasn't possible 20, 25, 30 years ago. So completely understand the scope of it and don't walk in with eyes shut.

PS

Scott, you make a good point about, you know, in terms of comparing it to Google page ranks, but the fact of the matter is still it's managed by one company with unknown algorithm, which supposedly changing very frequently as well.

So, yeah, I agree with what Scott says, extremely ambitious as well, right, because not many established systems of that sort exist now. Of course there is blockchain and crypto.

DP

Yeah. So, I'd posit that the way they approached page rank was groundbreaking. But you know, academic citations already exist, patent citations of other patents already exist - these methodological frameworks of mapping who did what and what does that mean and where did the impact go? It's already there. I think social credit scores are inevitable. It's a question of how we do them productively.

If you look at the sports analytics revolution over the past 30 to 35 years, that created greater opportunity for individuals to actually advocate for their own value. I see all of this coming together in the professional context and collapsing that into the personal context.

The question then becomes how do we do this productively? Do we use standards bodies, or do we adjudicate this in the courts like actual legislation and then adjudication by judicial bodies? And I think that's much more apt because I think this is much more broad in terms of its societal impact and I think it's going to devolve.



DP

You were asking me more of a technical question - how do you trust agents? I'd say this is more of a question of a non compete. Does a company own your expertise, your skills, the things that you've done for them when you leave? I think that's the level where this actual question of it's going to inevitably a decentralized system that allows individuals to have the value of their sovereign identity.

But then the question is going to become - when you're employed by somebody, do they own the expertise that generated the artifact? I think it's at that level.



PS

That's where I think the centralization and the impact comes in the regulatory and the judicial context and also in terms of arbitration. You know, this entity or whatever that is deciding an agent's or my expertise. What if I don't agree with it?

Reddit is a good example, but a lot of those are not related to, for example, financial transactions. So today if I have an issue with the bank not offering me credit because your credit ranking is such and such, I have mechanisms within the legal scope to go contest that. There is a regulator and arbitrator, local or centralized government, which stand behind those arbitrations.

How would an independent peer-to-peer arbitration mechanism look? Especially when we're talking about basic things that people and the systems will do. It's not optional, right?



DP

I think it's three layers. One is person to person, peer to peer. And that's the great thing about a programmable token. Using a programmable token means that if there is identified, rules-based malfeasance you can actually have negative consequences that you can't do with fiat with a normal currency. If you do something bad, you have something taken from you. That's programmed into the system, that's not a central actor.

Second is the same thing GitHub does when something bad happens. Remediation, on-platform remediation. Very clear rules and pathways to claw back, take things back, make them private, so on and so forth.

DP

Last thing I think comes to exactly what you've identified, which is arbitration in more of a formal context. And I don't think as an infrastructure solution we want to be in that. I think that's coming back to it where it gets into legislation, regulation. Again, because this is so critical - we're talking about our livelihoods and our value here - I think that does become societal at that level.

But what we can do is offer person-to-person engagements – “You did something bad to me. I don't like you. I'm going to file something.” The system takes care of it and it is that simple. You can encode a token to do that and then it becomes organizational. Very similar to what GitHub does.

RJ

A question for Donald. So the question you and E^NAT IP posed about trust, about agents and so on. Is the system that Dan is suggesting, would that be a solution that NIST would look at or be thinking about? Does that tie both the conversations here?

DJ

So yeah, well there are some ties, but I guess from my perspective that does go along with this point: trust has to be engineered into telecom networks. It's a property that must be built into the infrastructure the same way we build for latency or uptime. It's not going to happen by accident and the tools don't exist today to accomplish it. That's why they haven't been able to identify the standards to be able to bring these agentic AIs to market at scale. This trust has to be engineered into the infrastructure.

DP

I will say that Donald, you and I are using trust definitionally differently. That's one thing I've identified.

DJ

Yeah, yeah, yeah, absolutely. What I do, it's all around some intellectual property and I've built this architecture to satisfy what I consider probably one of the biggest questions in telecoms currently. I mean it's to the point to where in three weeks these rules were supposed to go to in effect, and as of today they haven't even published the document to extend it.

I think there's a lot of people that understand that these changes need to be done. It just hasn't been determined how we're going to go about it.

PS

So Donald, is your company suggesting solutions to on this front?

DJ

I have a complete framework that I've been working on. I mean we looked at this 15 years ago, we knew that this time was coming. This problem has existed for some time, but right now with agentic AI trying to come to industrial scale, we have to address these problems before we'll be able to move.

PS

With the time we have, can you give us an outline of what your solution is?

DJ

Probably not, no. It's, it's mainly a framework. It is all online at enatip.com. I've written a white paper that explains the framework. It's there to be tested and abused and see if you can dispute it in any way. I think we have actually figured it out.

I think one of the biggest issues of doing what needs to be done at this point comes back to your comment - that is, you don't see how you could have a centralized system to handle this. But at the same time I haven't been able to see how you don't. I suspect that there are a lot of the major tech companies who don't want to go that route and, like you say, maybe it's too much power in one organization.

PS

Yeah, I do believe we need a layer to be able to engineer this trust into the architecture. And are you contributing that to the discussions happening and looking to formalize and standardize your approach, or..?

DJ

Well, I don't know about standardized. I've put out the framework. There may be other multiple ways to do it, which I explain in the paper. Anything that can accomplish the goals set out would actually comply. You wouldn't need to use the specific tooling that we have developed. But, but anyway it is all there in a white paper to be reviewed and I would love to get feedback.

AL

We do have a couple of minutes left. So actually this is something where, Dan and Donald, maybe you can both comment - because you're right, these are global problems inherently with an online system. But we're seeing governments increasingly looking for sovereignty or the ability to protect their citizens and so on. And I wonder if you're seeing some kind of tensions in how you create your solutions to satisfy the fact that we do have these centralized systems called governments.

DJ

Yeah, that's tricky. That's a tricky one.

DP

Yeah, yeah. We're entering a new age where a lot of the pre-existing systems that had real good swim lanes are starting to collapse and it's because centralized value and intermediaries are collapsing, frankly. Disintermediation was the whole point of crypto. The technology and the philosophical frameworks undergirding it lend themselves to value creation, for individuals to capture more value and use agents to capture more value for themselves. That sovereign identity narrative, that is incredibly powerful. I think that's the arc of the narrative from a technical perspective for the next 10 to 15 years, if not longer.

There's the question of how we harmonize these technologies to do things in a bottom-up way for individuals to capture value. That is going to be the challenge of our times. Do it in a secure way, in a high trust way, in a way that individuals actually see real value accrue to them rather than from the top down. If we can't do that, then all these technologies won't fully bloom in the way that they should.

All that starts at the regulation side and with the governments. And I think that's inevitable because the impact is going to be at that societal level.

So all of these questions, all of these conflicts I think are somewhat inevitable. The sooner we can wrap our heads around the harmonizing of these technologies, societal and philosophical issues, the more we can congeal them and think bigger, the more effective we are going to be at finding viable solutions that are transnational, cross-cultural. It's really going to take a lot of really flexible thinking.

PS

So a quick comment there. This is going to have the same headwinds that crypto has right now, cryptocurrency, because it is wrestling the control away from the central governments and government are not good at giving away control. Right.

DP

Yeah, I can go deep. I was at the SEC I know the FTC quite well. The digital utility token exemption from the SEC is the pathway. The question then becomes "How this is going to be bottom-up, consumer centric?" Are they going to stand in the way of individuals using a LinkedIn 2.0 that also becomes a platform for generating economic value? I don't really see that.

I actually see them leaning into that as well, frankly. Our Social Security system in the United States starts to fail as Universal Basic Income becomes more of a proposal that gets, you know, greater support over the next 10 to 15 years. I think something that looks like a passive annuity structure based on actual work, verified progress is going to get a lot more support.

So I understand the SEC and the FTC and others really stand in opposition of this stuff today. But as consumers start recognizing their value creation opportunities, encoding their expertise, building their credibility on that, I see that the winds are going to flip. I think that's somewhat inevitable.

AL

Excellent. And with that, I know we could go on for a lot longer than this, but I think we're pretty much out of time for this broadcast. So if you're watching this and you have questions or you want to follow up with any of the speakers, please do drop us a line. You can contact me at alex.lawrence@telcoforge.com and I'll help to connect you; or obviously you can find Donald and Dan at E^NAT IP and Quadron respectively.

For now, though, I'd like to thank Donald, Dan, Ryan, Scott and Prakash for their time and their insights. And thanks to all of you for watching. Goodbye.

ACKNOWLEDGEMENTS

The TelcoForge team would like to thank the participants for their time and insights making this report possible.

We look forward to many other constructive insights.

The TelcoForge team would also like to thank National Instruments for supporting this summer's Forging Ahead.



CONTACT

Alex Lawrence
Managing Director

alex.lawrence@telcoforge.com
www.telcoforge.com
+44 7713 086721