EPISODE 719

[INTRODUCTION]

[00:00:00] JM: Parity is a company that builds blockchain infrastructure. Parity has built several open source projects and works with enterprises to put blockchain technology into production. Gavin Wood is the founder of Parity and he joins the show to talk about the state of blockchain technology and what his company is currently focused on.

Four years ago, Gavin helped start the Ethereum project. So he has lots of context on decentralized technology. Gavin envisions a world with many different blockchains for many different use cases. These blockchains will interact with each other to enable trusted relationships between parties. One project that Parity has created is Substraight, a technology that allows developers to quickly standup a blockchain with the right privacy level. Another project is Polkadot, which allows blockchains to connect and interoperate with each other.

Gavin and I discussed why the world needs a variety of blockchains and whether all of these different blockchains should need their own cryptocurrency. Gavin described the use case of blockchains for mediating supply chain trust. We also talked about the technologies that are used to build these projects, including WebAssembly and Rust.

[SPONSOR MESSAGE]

[00:01:23] JM: Kubernetes can be difficult. Container networking, storage, disaster recovery, these are issues that you would rather not have to figure out alone. Mesosphere's Kubernetes-as-a-service provides single click Kubernetes deployment with simple management, security features and high availability to make your Kubernetes deployments easy. You can find out more about Mesosphere's Kubernetes-as-a-service by going to softwareengineeringdaily.com/mesosphere.

Mesosphere's Kubernetes-as-a-service heals itself when it detects a problem with the state of the cluster. So you don't have to worry about your cluster going down, and they make it easy to install monitoring and logging and other tooling alongside your Kubernetes cluster. With one click install, there's additional tooling like Prometheus, Linkerd, Jenkins and any of the services in the service catalog. Mesosphere is built to make multi-cloud, hybrid-cloud and edge computing easier.

To find out how Mesosphere's Kubernetes-as-a-service can help you easily deploy Kubernetes, you can check out softwareengineeringdaily.com/mesosphere, and it would support Software Engineering Daily as well.

One reason I am a big fan of Mesosphere is that one of the founders, Ben Hindman, is one of the first people I interviewed about software engineering back when I was a host on Software Engineering Radio, and he was so good and so generous with his explanations of various distributed systems concepts, and this was back four or five years ago when some of the applied distributed systems material was a little more scant in the marketplace. It was harder to find information about distributed systems in production, and he was one of the people that was evangelizing it and talking about it and obviously building it in Apache Mesos. So I'm really happy to have Mesosphere as a sponsor, and if you want to check out Mesosphere and support Software Engineering Daily, go to softwareengineeringdaily.com/mesosphere.

[INTERVIEW]

[00:03:42] JM: Gavin Wood, you are the cofounder of Ethereum and the founder of Parity Technologies. Welcome to Software Engineering Daily.

[00:03:49] GW: Thanks. It's good to be here.

[00:03:52] JM: It's 2018. You helped start Ethereum about four years ago. When you look back at your vision for Ethereum in the earlier days, how does that compare to the vision you have today?

[00:04:05] GW: In the very early days, I think I had slightly grander ideas about what would happen one to two years into the project. I thought there'd be a lot more progress on some of the other components. I'm pretty happy with what we got out within the sort of time that I was involved in the project, but yeah, we have this whole idea of like web 3.0 with this idea of that being not just Ethereum, but also really a sort of a great browsing experience in Swarm and Whisper in order to allow you to publish content and send messages between nodes peer-to-peer in a sort of privacy preserving way. That's still very much a work in progress.

[00:04:50] JM: Is it a question of just the maturity of the technology? Because I mean people had – This is an analogy that people have drawn all the time, but people had visions of grocery delivery by internet in 1994 and – I don't know, summoning a taxi easily. I don't know if that was as much a vision. But these things where early on that infrastructure was not there, but once the infrastructure was laid, you could get those sorts of things. The potential is still there, right? Or have you lost faith in the potential as well or is it just losing faith in the time horizon?

[00:05:29] GW: No. I think the potential is still very much there. What we started with Ethereum, this sort of notion of trust freedom. This idea that you don't have to trust that intermediary, you perhaps don't even have to trust the counterparty. It's still very much a theme as more and more technologies come out and more and more gets delivered.

I think the hype surrounding Ethereum was sort of descriptive, indicative, but I don't think Ethereum 1.0 is ever going to deliver on all of the sort of visions surrounding this smart contract centered world. It was the first platform of its kind. It was essentially an MVP and there's always the case that over the years there's going to be Ethereum 2 and Ethereum whatever and there are inevitably going to be other projects that we're going to also be contributing to this technology and to this vision. I haven't sort of lost faith at all. I think that perhaps there could have been more progress on some of the ancillary things. I think the ecosystem is progressing, but perhaps not as fast as some people would have liked. But nonetheless, we're working towards that goal.

[00:06:47] JM: In the last four years, it seems like things have really changed on the internet, even though it's just four years. It seems like things have gotten a little more dystopian. It's become clearer why centralization is problematic on the internet. I mean, I think four years ago, people could easily say, "Okay. Look, centralization at the financial system is dangerous and scary and kind of opaque in many ways." But I feel like four years ago we had a little more faith in the centralization of social networks, or your Gmail, or your search engine. Obviously, there were people who were sounding the alarm bells back then and much longer ago, 10 years ago, 12 years ago, people talking about the dangers of centralization. But today it just becomes so clear the dangers of centralization.

You've written about some ways that the internet is broken in your eyes, and it's certainly not going to get less as long as we have these centralized systems. We're only going to see more and more problems like this. What are the ways in which the current internet is broken most acutely?

[00:08:02] GW: If we're talking about like sort of detailed instances, I think the main issues with specifically the internet being broken, I guess overtime there's certainly two to three years ago before the sort of wave of HTTPS that encrypted an awful lot more of the traffic on the internet. Certainly like pre-Snowden revelations. By far the most acute thing was simply the most traffic on the internet, certainly in the western world, was being rooted by sort of three, four, five major nexusis and it was fairly trivial for agencies that perhaps didn't have the legal backing, but certainly in an opaque fashion when monitoring things.

I think that we don't really have the legal basis, the sort of fundamental understanding within the political world in order to properly police these sort of aspects of the security services even in the west. Certainly when you go further afield, then with governments that have even sort of less oversight, then this becomes much more of a problem.

I think today, as I said, that still extends to metadata. You can still quite easily see the rooting if you have access to these sort of nexusis of rooting. You can still see who is talking to who. In a sort of a dragnet fashion, you can collect all of these information, which I find quite worrying. But beyond that, it's also things like advertising and tracking user habits, user behavior. It's already at the point where face recognition is such that I could be traced – Certainly when I go to the U.K., I can be traced as I move around the country, and there's really nothing, the sort of security safeguards on my privacy are minimal. Governments, certainly the U.K. government is dead-set on reducing it even further.

I think eventually the time needs to come where the sort of privacy that people generally expect to happen of free society really doesn't need to be retaken. I don't think that the legal method, the political method is an effective way of retaking it in the near term.

[00:10:19] JM: Right, and really puts a finer point on just the most quite basic use case of cryptocurrency, just the idea that you could have uncensorable payments and how payments are such a fundamental form of speech, because by transferring value to somebody, you are showing that you support them in some dimension, whether they're offering a product or service, or they're representative of certain ideas, and the idea of being able to have uncensorable support of somebody else is fundamental to that kind of freedom that you're talking about.

With that said, what are the use cases for cryptocurrencies that have been validated today? I think uncensorable payments is one that is one that is probably on the cusp of being validated, it's like sort of validated. But maybe you could shed more light on what kinds of things you think have truly been validated at this point.

[00:11:18] GW: I think in terms of, let's say, social use cases, we're still at a relatively early stage of experimentation. I think it's pretty clear that, as you said earlier, society has problems with centralization, with intermediaries often being incompetent and sometimes abusing their power. Notably with WikiLeaks at the time where a bunch of diplomatic cables were released – WikiLeaks is found up, Assange is looking for some support with his legal costs. Let's be clear, legal costs are something that is a fair right of every citizen. It's in a free sort of law-based society. We expect there to be able to some sort of freedom to be able to pay lawyers to defend ourselves. It was very notable that WikiLeaks had its funding root shut off by the major payment processors and as an internet-based entity that was a big problem. You couldn't use cash. They didn't shut it off with any real basis. It was simply as a sort of high-level political favor towards the sort of U.S. establishment in order to sort of carry favor and sort of let them know that they were on the side of the establishment so to speak rather than in any way trying to support this journalism.

It was there that sort of Bitcoin, crypto, provided the one sort of refuge for those who did want to sort of give a bit of contribution to the legal defense. I think that's a fairly sort of clear case, where these days it's a bit sort of conspiracy theory-esque with Trump and the sort of the old right largely in ascendance. But I think there is some sense of the deep state, some sense that the sort of establishments sticking together and the payment processes and the banks are very much part of the establishment, and it was pretty clear that they were acting in a very biased fashion over their policy with WikiLeaks.

[00:13:22] JM: I mean, that's a great example. The other one that comes to mind is the Alex Jones being deplatformed from all of the different media institutions. Not a fan of Alex Jones, but the idea that you – I thought podcasts were the most horizontally accessible, uncensorable form of media distribution relative to YouTube, especially because it's not ad support – Or like Apple doesn't need to have an AV Network, because it's Apple. They sell iPhones and make plenty of money that way. Yet Apple still removed Alex Jones from the podcast distribution world. Now it's kind of a wakeup call. Again, I'm not a supporter of Alex Jones to think he spread lies basically and not to get political, but it was scary to me as a media person that you just can get deplatformed by these kind of centralization.

I think if we can prove that uncensorable transfer of value is possible, at some point we can have uncensorable transfer of higher bandwidth information formats, which I think we're going to get into, the issues of scalability. Before we get into the kind of technical lower level details, what are the use cases for cryptocurrency related technologies, blockchain technologies? What are the things that you think we're going to see come to market first or come to market in the next 5 or 10 years?

[00:14:59] GW: I'd say that the most sort of pressing use cases are things where we can't reasonably setup entities that all parties of a system can trust in order to get some information between ends of economic conduits. A classic example of that is supply chain pharmaceuticals, for example, and where it's very difficult to – If you're buying some, I don't know, aspirin or whatever it will be, and perhaps not aspirin. Maybe some – I don't know, anti-AIDS medication in Eastern Europe, it can be very difficult to know that it's the sort of real thing and not some counterfeit.

The reason that it is so difficult to do is just because the supply chain goes between different countries, different cultures and there is very little way to connect to the end user with the producer in a way that the end user has a substantial degree of ability to believe that that sort of reading are truth when this thing presents itself as a genuine article.

I those sorts of situations, this kind of trust-free technology; blockchain, cryptocurrency to some degree, I think that's just one use case, but these are ways of mitigating the issue of having to trust third-parties in order to collate this information from different corners of the world, different jurisdictions together in a very cost effective manner, because we're essentially using computers for the intermediaries now. We can really drive down the margin to the basic sort of IT level.

I would say that sort of supply chain is a big one, and things that – Here in Germany where I live now, buying a house is an incredible ordeal. In terms of the taxes involved, the sort of stamp duty, the sort of transaction tax, it's very substantial and this isn't a value added tax. This is simply a sort of – It's not actually technically a tax, but a fee for the notary runs to about 1.5% of the total transaction value and this is enforced by the German government and it's basically making a bunch of people whose main job is to sit on a chair and read out a contract, a few pages, for about 1 hour, 1.5 hour and watch a couple of people sign.

It's kind of crazy and now – Okay, 100, 150 years ago, this was pretty important, because you needed to make sure these transactions were done by sort of an agent of the state, otherwise there will be an awful lot of fraud and theft and whatnot. But these days we really do have the technology in order to remove this very clear example of a middleman. I could see in the states that allow it, which are probably the ones that are poorest simply because the rich states can afford a little bit more flab in terms of their processes and legals. But the states that are poorer, where the margins are much less and where the difference between a 1.5% cut on the value of the house that you're buying is the difference between being able to afford another child or not. It will be a huge advantage to use this technology.

[00:18:04] JM: Okay. The idea of a supply chain monitoring system, so there's an anti-AIDS drug and there're all these steps in the supply chain between the producer of the drug and the person who consumes the drug. You've got purchasing middlemen. You've got distributors. You've got distributors of distributors. You've got warehousing. Let's say there's 8 points of selling and reselling that occur in the value chain between the AIDS drug company and the end user. People who might want to counter-argue the idea that you need a blockchain for this would say, "Okay. So you set up a Rails app, you put a PostgreS database behind the Rails app." You give different permission levels to the different types of users, the person who's making the drug, the person who's producing the drug, the person who's distributing the drug, the person who's manufacturing the drug and so on. All of these people can log in. They can somehow sign and verify their face in the process. Maybe there's some kind of hashing and verification system they can go through at each point in the supply chain, and then at the end of it, the user who wants to consume the drug, they can login and they can see the entire supply chain and the verification process. Why do you need a blockchain for this use case?

[00:19:33] GW: You're absolutely right. Technically speaking, that would do a perfectly good job. The issue isn't one of technicals. The issue is one of socials. You would have to find someone that would do all of that and do it for free, or for extremely low cost, like at cost, and would have to be utterly trustworthy so that all of the people in system, particularly in the end users or course, are guaranteed that this will – The no information has been tampered either through corruption, or through coercion, or through incompetence. To combine that with low-cost is essentially impossible without the blockchain.

[SPONSOR MESSAGE]

[00:20:22] JM: Managed cloud services save developers time and effort. Why would you build your own logging platform, or CMS, or authentication service yourself when a managed tool or API can solve the problem for you? But how do you find the right services to integrate? How do you learn to stich them together? How do you manage credentials within your teams or your products?

Manifold makes your life easier by providing a single workflow to organize your services, connect your integrations and share them with your team. You can discover the best services for your projects in the manifold marketplace or bring your own and manage them all in one dashboard. With services covering authentication, messaging, monitoring, CMS and more, Manifold will keep you on the cutting-edge so you can focus on building your project rather than focusing on problems that have already been solved. I'm a fan of Manifold because it pushes the developer to a higher level of abstraction, which I think can be really productive for allowing you to build and leverage your creativity faster.

Once you have the services that you need, you can delivery your configuration to any environment, you can deploy on any cloud, and Manifold is completely free to use. If you head over to manifold.co/sedaily, you will get a coupon code for $10, which you can use to try out any service on the Manifold marketplace.

Thanks to Manifold for being a sponsor of Software Engineering Daily, and check out manifold.co/sedaily. Get your $10 credit, shop around, look for cool services that you can use in your next product, or project. There is a lot of stuff there, and $10 can take you a long way to trying a lot of different services. Go to manifold.co/sedaily and shop around for tools to be creative.

Thanks again to Manifold.

[INTERVIEW CONTINUED]

[00:22:36] JM: In this case, you would want to have some kind of checkpointing system along the way to have people be verified – Or how are you removing trust from that system? Do you have these eight people, like the eight people that are in the loop; the customer, the manufacturer or the producer? Are all of these people kind of watching each other in just a consortium blockchain or is there some means by which this supply chain dedicated blockchain would be checkpointing with, for example, the Bitcoin blockchain in order to ensure tamper proof?

[00:23:13] GW: The Bitcoin blockchain, because it's not sort of Turing complete, it's not a smart contract blockchain, it's not in any way – Well, okay, slightly programmable, but not nearly programmable enough for this use case. Couldn't really do anything beyond indeed sort of checkpointing so you can ensure that the state of the chain can't be reverted, the transactions, once they sort of make their way on to it, can't be undone. But that's not really sufficient for this use case, certainly not for validating these kinds of transfer transactions that could actually be fairly complex in how sort of things come in and go out. You might have mergers and forks and all the rest of it.

The way it would probably work, it would either be a consortium indeed where the eight players would each watch each other. Eight is still fairly centralized, but we're doing a lot better than one that isn't really paid. An even better way would be to use an open and transparent platform, whereby each of the, basically, end users, people that sort of have their own – Sort of taking this medication, would be able to download all of the transactions that sort of prove, and this isn't 100% proof. It's very difficult to prove anything 100%, but this is something that's 80%, 90% of the way there from what we have now "prove" that the things that they have that are labeled the right drugs are actually indeed the things that came from the stated manufacturer.

[00:24:41] JM: Interesting. Let's just go a little deeper on this example. At each of these points in the supply chain, what are the different players doing to sign off on the validity or the trustworthiness of their handoff? For example, I produce the drug, I hand it off to a warehousing system or a warehousing company, and then the warehousing company is going to hand it off to – I don't know, FedEx, or somebody who's going to ship the drug. The warehousing company could swap out that drug for a counterfeit version of the drug. What is the warehousing company doing to sign and verify the safety, the trustworthiness of their package that they're going to then handoff to FedEx? How are they interacting with that consortium blockchain?

[00:25:32] GW: There's a few ways, sort of the very naïve way that's a good first step would simply be that whenever any package left the original manufacturer, it would leave the original manufacturer with a sort of a hash, some sort of cryptographic document almost, documentation, that's sort of one of a kind. That hash would have placed on the blockchain. So there're only a specific number of these hashes. They would represent a consignment of this medication.

Now, when it arrived at the distribution warehouse, maybe via carrier, whatever it will be, then that hash would be – The way that the distribution warehouse will be able to say, "Yes, I received," whatever, "100 kilos of this medication." They would sort of scan this hash. This hash wouldn't be previously sort of unknown to any others. It might be covered before. Maybe they have to sort of scratch something off or whatever else, but in essence they would take ownership by claiming this hash on the blockchain. So the blockchain would record that this particular consignment, which we know is valid, because this hash was signed on the blockchain by the original producer would not be sort of cosigned by this warehouse that would essentially be proving firstly that the producer no longer has ownership or stewardship of this medication. Secondly, that the warehouse indeed does. Thirdly, it's this medication and only this medication. There's not that they've got like this 100 kilos of medication is turned into a ton of this medication.

They can't sort of pretend to have more than they really have, because we always check all the way back to the producer to see which consignments they actually ever produced, and if we ever end up with a consignment that didn't come from the producer, that's a different hash. Then we know that something's wrong. Similarly because the blockchain is always tracking the ownership of the consignment as it goes from warehouse to warehouse to distributor. We know that at most, one counterfeit could have been swapped in. We don't know for sure that the thing that we have is definitely the thing that entered the warehouse at this point, but we do at least know that if they swapped it out, their business model is pretty rubbish, because all they can do is swap out one counterfeit for the thing that we believe is true. They can't do that very many times, because as soon as, of course, the final receiver sort of scans their hash, if someone else has already scanned the same hash, or if it's not the hash that came from the original producer, then we know that this is not good medication.

[00:28:02] JM: This hash would have to be on – If they printed it on the – Like if it's pills, you would need to print it on every individual pill, because otherwise I guess you could swap out the containers. So if you printed it on the container, the warehousing person could potentially just swap the container and still have the pills. But if you printed the hash on every single pill, then you can have some verification.

[00:28:30] GW: This wouldn't be something that goes on every pill. Essentially, what you're doing is you're saying, "Well, assuming every eventual consumer –" Let's assume it's printed on each box, so each container of pills, because you know it's printed on every pill. People don't check each individual pill is something – The consumer eventually gets a box of these things. You might print it on the box. I think that would be fairly reasonable.

The eventual pill consumer would simply scan their QR code that has this hash on on to the sort of a line and check that this QR code, and they could do this even at the point of purchasing the pills with their smartphone and it would just check that the pharmacy that they're buying it from did indeed take consignment of these specific box of pills from wherever, that that's irrelevant. The main thing is that they did indeed take ownership and that no one else has so far scanned this hash. If those two things are true and if the producer did actually produce this box of pills with this hash. Those three things. If those three things are true, then we know that if this box of pills has been swapped out, then it's very unlikely that anyone's making any money by swapping this particular box of pills out.

In principle, someone could have switched the pills from inside the box, but then there's no real sort of why would they do that? Then they now have sort of a bunch of pills that they can't actually sell, because they can't prove that these are the pills that they are, because they've just put the hash on another box of pills. Unless they could kind of flag these pills like for a discount on the black market and sort of try and say, "Well, these pills are legit. Honest." But even though, we don't have a hash to prove it. It doesn't really make any sense. They might get – I don't know, 5% of the actual price. So I think it would be worth their economic effort in doing them.

[00:30:18] JM: Not to spend all the time on supply chain applications of blockchains, but can you just – Just to put a finer point on this, explain why the model of just using a Rails app with a PostgreS database and sharing that hash or writing that hash to the database and everybody along the supply chain just checkpoints that, yes, this box still has the proper hash on it. Then maybe you have all the – Well, I guess if you have everything that goes on in the operating system, you could write it to a log, but then you would be trusting the operating system that'd be centralized to some extent. Why do you need a blockchain for this use case?

[00:31:02] GW: Essentially because you're dealing with a fair amount of data. You're dealing with a number of different players. You're dealing in terms of relatively high stakes. So whoever is operating your server – This is a server, right? There's going to be a single operator, and they're the guys that run the Rails, sort of database. They're the ones that have the PostgreSQL. They're the ones that have the admin account. They have to basically say no when the Eastern European mafia comes knocking on their door to say, "Come on. Just put an extra 10X of these pills in, because we stand to make $10 million, and we won't break your knee caps." They also have to be sufficiently competent that hackers that, again, let's say Eastern European mafia hire a couple of fairly decent hackers to go into the Rails application with a zero day, add an extra 10X of these consignment. They also have to do it for basically free. These three things of what blockchain achieves that you will not be able to achieve all three of them with a standard centralized service provider.

[00:32:01] JM: You would not necessarily need a cryptocurrency for this kind of model. You could probably have – Let's say you wanted to have some degree of resiliency for this supply chain blockchain, but you don't necessarily need the global resiliency of a global reserve currency like Bitcoin is trying to be. Maybe you could just have a thousand people validating the supply chain blockchain. Is that your vision for how the validation process and the blockchain process would work?

[00:32:30] GW: Yeah. I mean, actually at the end of the day, it doesn't actually matter so much how many people validate as long as a barrier to entry of validation is sufficiently low. It might be that you actually only have 10 or 20 validators, but as long as it's possible for anyone to come along and get the whole of the data and check all of the transactions and make sure that everything actually does add up, then it's basically fine.

Now, actually, if you look at the number of full nodes on the Bitcoin network, so the nodes that actually compute every single transaction that's ever happened on Bitcoin, there really aren't all that many of them. I might be getting mixed now, but I think it's in the four or five, if not four figures. It's certainly not sort of crazy super computer sort of numbers and the super computer numbers as far as Bitcoin is concerned only reach as far as the hashing algorithm and how many people are trying to solve these pointlessly hard puzzle.

[00:33:31] JM: Why don't you need a cryptocurrency for each of these enterprise or consortium blockchains that we might need to create – Maybe let's say we want micro-networks of trust around supply chain and a variety of other things. Maybe we want to blockchain around our local weather reporting so that the weather reporting cannot be politicized. Do we need a cryptocurrency in all of these different domains, or can we achieve a trustless information sharing network without a cryptocurrency?

[00:34:08] GW: Cryptocurrencies generally fulfill two significant requirements. The first is requirements of these systems. The first is that they provide a basis for the security operators of the network. In Bitcoin's case, miners get paid in the cryptocurrency itself in order to ensure that it's very difficult to rollback any transactions on the network.

If Bitcoin were not worth very much and they are plenty of cryptocurrency where their currency isn't worth very much and therefore the network is much easier to rollback. If that was the case for Bitcoin, then it wouldn't be able to hold nearly as much value as it could. It's kind of a self-fulfilling thing going on there.

The other reason that these networks, these blockchains tend to have a cryptocurrency behind them is one of ant-spam prevention. Essentially, if your transactions – If you don't have a cryptocurrency, it's very difficult to prevent the general public sort of attackers and spammers within the general public from just filling up your blockchain with useless transactions. You attach a cost to processing these transactions, and that cost is sort of managed and ministered as a cryptocurrency payment and that's what Bitcoin did and that's how Ethereum works as well and there's a bunch of others. I don't know of any public blockchain that doesn't use this mechanism.

Private blockchains or consortium blockchains are a little different. They don't need this, because they have different economic motivations, or different economic motivators to make sure that, firstly, there's no spam. Secondly, that the network is sufficiently secure, that its maintainers don't just sort of rollback blocks when something happens that they don't like or in an attack circumstance. They do that basically by legal methods or by them all being within the same company and just sort of telling them, "Look, this is what we want to happen. If you're going to do your job, then make sure you do it this way."

That's fine. In my sort of vision of how things are going to sort of pan out, I don't think we're going to see blockchains always have cryptocurrencies attached to them. I think we both start to see blockchains that's piggyback on other cryptocurrency blockchains. The project that I'm working on at the moment, Polkadot, is one way of achieving this. But that said, Tokenization is a really easy way of not just funding a project, but also sort of continuation of the sort of payments and services within that project to make it so that sort of payment processing and this notion of an economy forming within the project to the users and providers all being part of the same market is very useful to actually achieve that. So, I don't think it's going away either, but I think we'll eventually find a sort of middle ground.

[00:36:57] JM: I feel like I'm in the minority thinking that consortium blockchains, private blockchains, enterprise blockchains, the things along the gradient between enterprises like PostgreS database and the Bitcoin blockchain. I think I'm quite interested in these. I find them potentially quite useful. I know that there's a lot of – There's kind of a lot of rejection of the idea of enterprise blockchains. I don't know. I think they could be quite useful to have these. I mean, in traditional computing, you have granularities of permissions and I don't know why the same wouldn't be the case with trust-based systems.

[00:37:39] GW: Yeah. I guess I generally agree. I think that we need a little while longer for many of the CIOs, many of the sort of IT leaders of enterprise to really get to grips with what this technology can provide. Moreover, I think there's a little bit of a paradigm shift required. One of the projects I'm involved with, the EWF, Energy Web Foundation, is a consortium blockchain, or based around the consortium blockchain within the energy sector. Inevitably, it's going to take a while before more traditional businesses and business models that operate on traditional business models come to grips with how sort of living in a trust-free world, how this trust-free technology can actually sort of help them.

I think the original way, the sort of when we saw blockchain-based POCs come out in the enterprise about two, three years ago, focused a little too much on reducing trust from inside a single business and not enough on trying to cut down enterprise transaction fees. I think that's really where this can help, this technology can help. I think it may well optimize certain processes within a business. Maybe it'll help you police certain processes within a business, but I think its real value out of a traditional businesses is in helping them interact with each other with much less cost, much finer granularity and in a much more adaptive fashion.

At the moment, if businesses want to interact, they pretty much in any circumstance have to go via lawyers. Going via lawyers, I don't know if you've ever done that, but it's a very expensive and time-consuming task. Often, that doesn't have a very adequate end. At least with blockchain, it costs you very little to find out whether or not some particular sort of ongoing deal or transaction is going to work between you and whoever it is that you want to deal with.

[SPONSOR MESSAGE]

[00:39:41] JM: Data holds an incredible amount of value, but extracting value from data is difficult, especially for non-technical non-analyst users. As software builders, you have a unique opportunity to unlock the value of data to users through your product or service. Jaspersoft offers embeddable reports, dashboards and data visualizations that developers love.

Give users intuitive access to data in the ideal place for them to take action within your application. To check out Jaspersoft, go to softwareengineeringdaily.com/jaspersoft and find out how easy it is to embed reporting and analytics into your application.

Jaspersoft is great for admin dashboards or for helping your customers make data-driven decisions within your product, because it is not just your company that wants analytics. It's also your customers that want analytics.

Jaspersoft is made by TIBCO, the software company with two decades of experience in analytics and event processing. In a recent episode of Software Engineering Daily, we discussed the past, present and future of TIBCO as well as the development of Jaspersoft. In the meantime, check out Jaspersoft for yourself at softwareengineeringdaily.com/jaspersoft.

Thanks to Jaspersoft from being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[00:41:14] JM: You started Parity, and Parity has a widely deployed Ethereum client. I would like to talk some about the Ethereum client, but I’m hoping to spend – I’ve spent so much time talking about supply chain. I think we should probably focus on Polkadot and Substraight. Polkadot is a protocol that you created around blockchain interoperability. The idea is to allow different blockchains to interoperate with each other and be compatible.

Substraight is a system for launching blockchains quickly and effectively. What is your vision? What are you trying to build with these set of technologies? What kinds of applications are you trying to enable with improving blockchain interoperability and allowing people to standup blockchains on their own quickly?

[00:42:08] GW: I think if we're talking grand strategy, I guess I'm coming from the idea that when we started Ethereum, for me, Ethereum was always about building out turbo charging and innovations commons. The idea was that we were going to put this commons down, lay down this sort of very public owned piece of IT, and the idea was that people could come to it, coders by and large, but in principle, businesses and whatnot. Could come to it and they could lay down their own economically independent, economically autonomous and processes essentially laying down business models, but doing so live. Slightly, you can just imagine a business model, you can code it up and then you can lay it into this blockchain and it will just work and it will interact with all of the other smart contracts as we call them, the sort of business models there.

This was kind of crazy. It's like, "Wow! People are going to do this and that. It's going to be amazing." To some degree, we saw some of that. We saw some pretty interesting applications, pretty off-the-wall applications. But it's following in that vein and it's basically saying, "I don't think that the smart contract model is – The sort of compute model behind Ethereum is everything. I think that there are some applications of this technology where it makes more sense to have your own distinct blockchain," and that might be just as an optimization, as an efficiency thing. But it could also be that it just fits better within a different sort of consensus method. It may just be that it's got different parameters. Maybe it's got faster block times or slower block times or whatever else. It's got different crypto, needs different database backends.

There are all sorts of ways that you can optimize for certain use cases. The smart contracts is a very sort of blunt knife in order to do that. Whereas if we allow teams to experiment with their own blockchains, it becomes that much easier for them to hit the right solution. What I wanted to do is not just create a platform for making and deploying these chains, but also a platform to actually connect them altogether so that they get the same sort of benefits that we had with smart contracts with Ethereum so that they can be combined and composed and generally create a sort of large ecosystem of otherwise independent economic algorithms.

[00:44:27] JM: I think that's great, because you contrast it with the centralized world. You take something like WordPress. You could build whatever you want to on WordPress. You could, but

Ruby on Rails is a little bit better if you want to build something like Airbnb. You could build Airbnb on WordPress. It wouldn't be as great an experience, but you could do it. Similarly, on Ethereum, you can build whatever you want in the form of DAPs. You can build systems of smart contracts that have robust sets of functionality, and people have done that. You can launch your own token-based economy on top of Ethereum, but you're kind of offering more of a flexible full-stack model of deploying your own infrastructure it sounds like.

[00:45:15] GW: Yeah. I always look at things as where they sort of sit on the stack, on the software stack. I see you got your fixed function things, like Bitcoin, and they're very difficult to program. Then you've got Ethereum that sort of sits below it, and it is programmable. It's sort of notionally Turing complete. I would actually argue, it's not really Turing complete, because it has this gas mechanism that prevents you from running programs that take too long when you use too much memory or the rest of it. It's actually quite strict in how long programs are allowed to run. How much resources they can take.

Then all the way at the bottom, there's like just make your own chain and program everything yourself, and that takes a very long time to make a secure well-supported blockchain with all of the stuff that goes around it, block explorers and telemetry services and UIs. It really does take a very long time and a lot of effort to get all stable and secure. So what we're doing is saying, "Well, let's try and find a middle ground with Substraight." Let's say, "Well, you can build your own chain. If you want, we'll give you all of these sort of standard components, RPCs and databases, all that sort of thing, and you just have to fill out the blanks at the state transition function. The bit that sorts of processes the transactions and decides what to do." But we'll also provide you with a bunch of modules so that you can build it from a bunch of basically sort of components that you can plug together. This is the development platform that I want when I'm building Polkadot. It's like, "Right. Well, first, I'm going to build – Develop a platform that I want, and then I'm going to build Polkadot on top of it." I figures, "Well, I may as well make it free and give out to everyone else, because Parity is pretty much all about open source."

[00:46:52] JM: Across all your projects, Polkadot and Substraight and the Ethereum client, do you use WebAssembly? How is WebAssembly useful to blockchain development?

[00:47:05] GW: One of the questions I got asked back in 2014 when I was first sort of doing an Ethereum – I think it was actually the first proper Ethereum meet up I spoke at. It was in Silicon Valley. We got a guy ask me at the end of the meet up, “What happens when you want to upgrade the blockchain?” At the time I thought, “People will just upgrade the software and eventually it will fork.” He said, “Well, isn’t that going to be pretty hard to organize? What if some people don’t want to? What if some people don’t know, forget?”

I kind of dismissed that at the time, but it turns out that it’s actually a pretty important point. Blockchains aren’t upgradable. I mean, these days, pretty much any consumer product that can possibly upgrade thus upgrade. I mean, I’ve got a pair of headphones on. They upgraded the other day. I got like an addition of active noise cancelling. It’s like, “These weren’t active noise cancellation headphones, but not they are.”

Upgrading is a fact of modern technological life. It’s the idea that you release an MVP first and you add features to it as its product life cycle goes on. It’s pretty important and it’s what you need to do to be competitive. Blockchain couldn’t really do that until we figured out how to get a platform neutral language that encoded the bits of the blockchain that we thought were most important to upgrade, and that’s what WebAssembly does.

WebAssembly is basically our language by which we define how a blockchain should work. We define how it should process transactions, how it should process blocks and which consensus algorithm it should use. Using WebAssembly, we can then just roll out a new WebAssembly blog, which is completely platform neutral. It’s nicely designed so it’s actually fairly optimizable. You can sort of compile it or trans-compile it on to native instructions set for relatively sort of decent performance. It allows us basically to roll out upgrades on the chain.

The nice thing is because the upgrades are determined by on-chain mechanisms, we can use all sorts of interesting and cryptographic algorithms in order to determine when an upgrade should happen. So we can do things like implement all sorts of interesting governance and potentially futarchy algorithms for that.

[00:49:21] JM: It also has – It has memory constraints too, or you can control the memory on it unlike, for example, JavaScript, right?

[00:49:30] GW: Yeah. The general architecture of WebAssembly is pretty decent for when you want to do consensus algorithm specifically. Consensus algorithm is basically when you need all executions of it on all platforms, on all instances, to always come to the same result. If you remove, basically, the floating point instructions from the WebAssembly spec, then you end up at something that can be made sort of consensus proof. You have something that no matter how the program is executed, on what platform, on what computer, under which WebAssembly? As long as it's a standard binding WebAssembly implementation, you will end up with the same result.

Yeah, the memory – So the aspects of the environment that control the memory are a part of that. You can basically sort of ensure that it only allocates a certain amount of memory and it can't use anything beyond that. You get all sorts of traps – You get a trap is it tries to sort of access something that you know –

[00:50:29] JM: To wrap us up, what's the hardest part of starting a company in the space of cryptocurrency technology?

[00:50:38] GW: It's convincing people that you're not just the hype, I guess. The problem is with hype cycle, I mean, it draws a lot of attention into the industry as a whole. It draws a bunch of money into the industry as a whole. But it becomes almost like a popularity contest. People start to forget to look a little deeper beyond what they see to see whether the true value is really being created here, or whether it's just a bunch of very effective communicators and spreading some dreams about what it is that they may or may not hope to be producing.

Because of that, it's actually kind of difficult as a company that's busy building stuff that's dedicating its resources to building stuff to get the level of attention beyond others and sort of have it signal amplified beyond the noise. I'd say that, as much as anything else, is a pretty big problem for starting up.

[00:51:30] JM: Well, Gavin, I want to thank you for coming on the show, and I know we spent a lot of time talking about the supply chain example. But I think the reason I wanted to go deep on that is because your company is – The things that you're focused on are about this idea, this vision – First of all, I completely agree with everything you said about it being so early that we really don’t know how this space is going to evolve. But I think your thesis around the idea that we’re going to have a lot of blockchains. It’s not necessarily all going to be stuff that’s built on top of Ethereum, or built on top of Bitcoin. It could be disjoint and distributed and we want these things to be interoperable. We want them to play nice with each other. We want to have some standards around that. It is not easy to assemble the plane while you’re falling down from the cliff in the middle of a hurricane.

I mean, if people talk about – People talk about starting a startup business, you’re assembling a plane while you’re falling off a cliff, and that’s hard enough. But the blockchain space is completely up in the air. It’s like nobody knows what’s going to happen. So you’re also in a hurricane. So it’s like there’s so much movement. It’s really hard to have a strong thesis about anything. You can have a strong thesis about some things like, yeah, how do you mediate trust in a world where we’re relying on centralized organizations. How do you change things so that it can be trustless? But that’s about all we really know.

We have kind of a bright vision for the future, but we just don’t know what the implementation is going to look like. So I appreciate you taking the time to really break down some examples of why you might want another blockchain. But you also have the humility that you’re not really sure that this is how things are going to work out.
Anyway, I’m fascinated with your company. I’m fascinated with the work that you do, and I look forward to covering it more in the future as this stuff makes its way into the market.

[00:53:31] GW: Cool. Cheers, Jeff.

[00:53:32] JM: Okay. Thank you, Gavin. Good talking to you.

[00:53:34] GW: Likewise. Thanks.

[END OF INTERVIEW]

[00:53:39] JM: GoCD is a continuous delivery tool created by ThoughtWorks. It's open source and free to use, and GoCD has all the features you need for continuous delivery. Model your deployment pipelines without installing any plug-ins. Use the value stream map to visualize your end-to-end workflow, and if you use Kubernetes, GoCD is a natural fit to add continuous delivery to your project.

With GoCD running on Kubernetes, you define your build workflow and let GoCD provision and scale your infrastructure on-the-fly. GoCD agents use Kubernetes to scale as needed. Check out gocd.org/sedaily and learn about how you can get started. GoCD was built with the learnings of the ThoughtWorks engineering team who have talked about building the product in previous episodes of Software Engineering Daily, and it's great to see the continued progress on GoCD with the new Kubernetes integrations. You can check it out for yourself at gocd.org/sedaily.

Thank you so much to ThoughtWorks for being a longtime sponsor of Software Engineering Daily. We are proud to have ThoughtWorks and GoCD as sponsors of the show.

[END]