EPISODE 457

[INTRODUCTION]

[0:00:00.3] JM: Cryptocurrencies give us a decentralized financial system. OpenBazaar is a decentralized commerce system. A merchant can log on to OpenBazaar and post a listing for an item. For example, a t-shirt that I want to sell for $15. My item listing will spread throughout the OpenBazaar, peer-to-peer network.

A shopper can download the OpenBazaar desktop application and see my listing for a t-shirt. The shopper can pay me $15 in Bitcoin and I will send the t-shirt to their address. If I were selling that shirt on Amazon, the corporation would take a cut of that transaction. OpenBazaar has no transaction costs, so users get to save some money.

However, users also miss out on the benefits of a corporate marketplace. Amazon makes sure that the seller will send the item to the buyer and makes sure that the buyer pays the seller. On OpenBazaar an escrow system is needed to place money in the hands of a neutral third party until the goods are delivered. Amazon ensures that the distributor sends the item to the customer. On OpenBazaar, users need to figure out how to send those goods to each other.

Brian Hoffman was the first developer to start working on OpenBazaar, and the project has grown significantly since his initial commit. OpenBazaar now has buyers and sellers and open source committers, and there’s a clear desire for an open system of commerce.

Brian is also the CEO of OB1, a company that provides services on top of OpenBazaar. OpenBazaar is a protocol and other companies will undoubtedly emerge to build on top of it as well.

In our conversation, Brian discussed how OpenBazaar works, the peer-to-peer protocol, the escrow system, the dispute resolution system, and the open source community management. It’s a fascinating and unique project and I hope you learn something about it from this episode.

To find all of our old episodes about decentralized technology and blockchains, you can download the free Software Engineering Daily app for iOS or for Android. In other podcast players, you can only access the most recent 100 episodes, but with these apps you can get all 600 of our past episodes, you can get recommendations based on your listening history and they're open sourced at Github.com/softwareengineeringdaily.

If you're looking for an open source project to get involved with, we would love to get your help. A shout out to today's featured open source contributor, Justine Lam, he has been working on improving the iOS code base, and I know all of the Software Engineering Daily mobile users appreciate his effort. Thanks Justine, and thanks to all of the open source contributors.

Let's get on with this episode.

[SPONSOR MESSAGE]

[0:03:00.3] JM: You are programming a new service for your users, or you are hacking on a side project. Whatever you're building, you need to send e-mail. For sending e-mail, developers use SendGrid. SendGrid is the API for e-mail trusted by developers.

Send transactional e-mails through the SendGrid API. Build marketing campaigns with a beautiful interface for crafting the perfect e-mail. SendGrid is trusted by Uber, Airbnb and Spotify. But anyone can start for free and send 40,000 e-mails in their first month. After the first month, you can send 100 e-mails per day for free.

Just go to sendgrid.com/sedaily to get started. Your e-mail is important. Make sure it gets delivered properly with SendGrid, a leading e-mail platform. Get started with 40,000 e-mails your first month at sendgrid.com/sedaily. That's sendgrid.com/sedaily.

[INTERVIEW]

[0:04:14.3] JM: Brian Hoffman is the developer of OpenBazaar and the CEO of OB1. Brian, welcome to Software Engineering Daily.

[0:04:22.0] BH: Hi. Thanks for having me.

[0:04:23.0] JM: OpenBazaar is a decentralized marketplace. With Bitcoin, we have decentralized money. Why do we also need a decentralized marketplace?

[0:04:34.4] BH: Well, I think very early on when Bitcoin – after Bitcoin was created, it was realized that if it's going to service some kind of payment mechanism in addition to be in a store value, there needs to be somewhere to use it.

Early on, people were just sending it to each other directly in forums and things like that. But there was always this idea that maybe there could be this more advanced marketplace that would match up buyers and sellers and allow them to spend their Bitcoin to receive products or services.

This never really happened in a concerted way until there was some websites that would accept it and things like that, but there was never really like a good marketplace.

[0:05:19.8] JM: I sell Software Engineering Daily t-shirts on Shopify. That's a centralized marketplace. How is it different if I sell those t-shirts on OpenBazaar?

[0:05:31.9] BH: The idea behind OpenBazaar is to accomplish a similar goal, which is to get Bitcoin for a t-shirt. But we do it in a much different way behind the scenes, and in a way that creates a lot less requirement for centralization and trust.

If you were to sell t-shirts on Shopify, let's say you sell Donald Trump t-shirts and all of a sudden the people who run Shopify say, "Well, we don't like Donald Trump, so we're going to remove all of the stores that sell Donald Trump t-shirts." Your business could instantly disappear, because you're at the behest of this company or centralized organization.

In our case, because OpenBazaar is completely peer-to-peer, it's up to the participants of the network to decide what stays and what goes. Those Donald Trump t-shirts would remain for sale just like if you were running your own website. That's one primary advantage of it.

With Bitcoin, we have permissionless money, so no one can tell you how to spend your money or where to spend your money or who you send it to. They can't take it from you. In this way, your online business can't be taken away from you as well.

[0:06:51.0] JM: Would OpenBazaar work without Bitcoin?

[0:06:54.5] BH: OpenBazaar was designed to be agnostic to the payment mechanism. We have a smart contract type system for how you set up a trade and how you list your product, how people say I want to purchase the product and so on. But one of the most unique aspects of it is the idea of this escrow system.

What that means is if I want to sell something to you with Bitcoin and I send you Bitcoin, I can't get a refund unless that person gives me the refund. It's quite risky to say, "Hey, I'll buy your t-shirt. Here is the Bitcoin. Please send me the t-shirt." Do you have no recourse.

In OpenBazaar, what we have is a special type of Bitcoin address, which the merchant and the buyer co-own. The money can't really go to one or the other, unless they both agree. It serves as this escrow.

When you're going to buy the t-shirt from somebody, you would put your money that you want to pay to the merchant into this special account, and when you receive the t-shirt and you're happy, then you guys both agree to give the merchant that money out of the escrow address. That actual capability really only exist in these cryptocurrencies. There is no real way to do that with like a PayPal for instance. That is necessary. That's why Bitcoin is necessary in this case. But there are other cryptocurrencies that have similar functionality and could replace Bitcoin there.

[0:08:27.1] JM: Like we said, I am a merchant, I want to post my t-shirt, my Software Engineering Daily t-shirts on OpenBazaar. Describe the process that a merchant goes through to post an item.

[0:08:42.0] BH: Right now, OpenBazaar is a desktop application that runs on Linux, OSX and Windows. You would go to the OpenBazaar.com website and download the app and install it, which is really simple. But once you're running the app, there is no registration or anything involved with it, because it just runs on your computer.

Then you're immediately presented with your store. It's like a couple clicks. Say create a new listing, you fill out the information for your item, add a photo, add a price, shipping options. Pretty simple. Seems similar to other marketplaces. Once you hit save, your listing is live on the network and people can go and buy it immediately. Within five minutes, I would say for most people they can have at least one product up and running in the store created.

[0:09:32.3] JM: Describe the process by which somebody makes a purchase on OpenBazaar.

[0:09:37.4] BH: The same thing would be required to get started. You download the app and run it. You can search for item in the app, or you can browse through the main pages and see what you want. Once you click on the item, you have a buy button.

You can either pay using the OpenBazaar wallet, which is in the app itself, or you can pay from any other Bitcoin wallet you have if you already have that, and you would just basically pay the amount of Bitcoin that's required. Enter in your shipping address where you want your product to be sent if it's a physical product. Then once you pay, the merchant will fulfill the order.

[0:10:21.5] JM: Okay. Now we can get in to the lower level aspects of this. We've talked about the high-level user experience. Okay, it feels like an e-commerce site. I go on the website from a merchant – I'm sorry, I go on the application, the desktop application. We'll get into why it needs to be a desktop application. I post my items and if somebody wants to buy them, they have to download the application, they open up the app and they make a purchase.

Under the hood, like you said, OpenBazaar runs over a peer-to-peer network. It's a Kademlia style peer-to-peer network. I think people know what a peer-to-peer network is. It's decentralized network where peers are communicating with each other and information spreads, and maybe kind of a epidemic style, or what's the – just a gradual gossip protocol, that's a typical peer-to-peer protocol the way information spreads. What is a Kademlia style peer-to-peer network?

[0:11:25.9] BH: On our network, rather than spreading – if I connect to the peer-to-peer network and I want people to know that my store is out there, some networks will do the gossip and just gradually tell the entire network that they exist. But the way that we do it is we use something called a DHT, or distributed hash table.

What this allows you to do is rather than as the network gets bigger and bigger and bigger, let's say there is a million stores on it, or million users, you have to track a million users and understand what the state of the network is for all million.

You basically have a subset of those and you're able to branch out using the DHT to find someone that you're looking for. The entire network is partitioned into a list of a range of hashes. The way it works is in our case, a Kademlia style is like let's say you have a million nodes, you probably only have a couple dozen in your writing table and you would say, "Hey, I'm looking for this store with this hash."

You look in your local table, "I don't have that hash. Okay, so what's the hash that's closest to this guy that I do have?" Then you ask that person. Okay, do you have this hash? If they don't, then they give you the closest hash. It keeps going until you find the actual hash, or you realize it's not in the network.

That allows you to do a much less – it's much less intensive to try and find that node, rather than have to search all the table, or keep track of all the table locally. That's this kind of in a nutshell how it works. Kademlia is just one style of that, and there's an algorithm that goes along with that that's much more detailed.

Most importantly, we use something called libp2p, which is being built by a company called Protocol Labs. They're also responsible for interplanetary file system IPFS, which is what we use. I mean, early on we had our own homegrown P2P protocol that we built on top of Kademlia, but we've since migrated to IPFS.

[0:13:48.3] JM: Yeah. I'd love to get into that migration a little bit later, because that sounds like an interesting process. The model of your network allows for lighter weight nodes than the Bitcoin blockchain. It's not like the Bitcoin blockchain where you have to download the entire transaction history of the Bitcoin ledger. Explain why that is.

[0:14:14.5] BH: Just you know, first there is two modes you can use Bitcoin in. One is the full node, which is probably the best option, but the most resource intensive. You have to download the entire blockchain in your computer. It validates all the transactions. In some cases it sends out transactions to others if they need it or they request it from you.

This takes up many, many gigabytes of space on your computer. It takes a long time to sync up the entire blockchain. It's really hard for users to get up and running immediately. Also for mobile clients, it's almost impossible to run a full node on your iPhone or your Android, because of that requirement.

There is something called SPV wallet, which is a simple payment verification, which basically it connects to other nodes and kind of asks for validation and does that, then it listens from the time that you created your wallet for transactions that come in for your wallet.

In OpenBazaar, we didn't want to have to burn users and say, "You have to run a full node in order to just buy things or sell things." Initially, the first version of OpenBazaar we just said, "We're not going to create a wallet. We're just going to let people use whatever wallet they want." But this was kind of kludgy, because when you wanted to buy something or sell something you had to jump out of OpenBazaar and go to your wallet of your choice and deal with that.

In 2.0 we created our own SPV wallet. It's inside the app, and you can use that by default. It doesn't require you downloaded the whole blockchain. It doesn't require any of that. You can immediately get going and make some payments and make payments out of your wallet. It's much more light on your computer. Hopefully, that will transfer over when we release the mobile and web version.

[SPONSOR MESSAGE]

[0:16:17.4] JM: Spring Framework gives developers an environment for building Cloud-native projects. On December 4th through 7th, SpringOne Platform is coming to San Francisco. SpringOne Platform is a conference where developers congregate to explore the latest technologies in the spring ecosystem and beyond. Speakers at SpringOne Platform include Eric

Brewer, who created the CAP theorem, Vaugn Vernon who writes extensively about Domain Driven Design, and many thought leaders in the Spring ecosystem.

SpringOne Platform is the premier conference for those who build, deploy and run Cloud-native software. Software Engineering Daily listeners can sign up with the discount code ‘SE Daily 100’ and receive a $100 off of a SpringOne Platform conference pass, while also supporting Software Engineering Daily. I will also be at SpringOne reporting on developments in the Cloud-native ecosystem. I would love to see you there and have a discussion with you.

Join me December 4th through 7th at the SpringOne Platform conference and use discount code ‘SE Daily 100’ for a $100 off of your conference pass. That’s S-E Daily 100, all one word for the promo code. Thanks to Pivotal for organizing SpringOne Platform and for sponsoring Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:17:49.1] JM: How does identity work in OpenBazaar? Because obviously, if I post something on OpenBazaar I want my merchant ID to be associated with my postings and purchasers want their purchase ID to be associated with their purchase. How does identity work?

[0:18:10.8] BH: Your identity in OpenBazaar is very similar to your identity in Bitcoin, which is there is no registration process where someone is tracking your name or social or whatever it is that you used to uniquely identify your e-mail address.

Basically, your identity is your key that gets generated. In OpenBazaar, we create – we use a pneumonic, which is a phrase of keywords to generate a key. From that key, we create your Bitcoin wallet as well in your store on IPFS.

The key is basically your identity. If you have control over your key on a network, then that’s who – whoever controls the key basically is the identity. Now, going forward, we’re working on ways of integrating other projects that can tie to that key. For instance, we’re working with Blockstack and they have a naming system.

You could go to Blockstack and sign up for a Blockstack ID, which is like say, “I own BrianHoffman.blockstack.id. I own that pseudo domain name,” and I can tie that to an OpenBazaar key, so I can prove ownership of the OpenBazaar key and I can prove ownership of the Blockstack and link those, and so people can find me on OpenBazaar using my Blockstack ID instead of a key basically. That makes it much more convenient.

We’re looking at ways of using that Blockstack and perhaps Ethereum’s naming system and there’s a couple other options. Really, it’s opt-in, but ultimately it’s really just about the key. I mean, if you own the key then that’s the identity.

[0:20:00.2] JM: Right. For people who aren’t familiar, this is the idea of public key encryption where you have a public key and that public key also is associated with a private key and you can use your private key to verify that you created a message. People can verify that you created that message with a public key so you can sign it.

You can also encrypt messages, or people can encrypt messages to you using your public key, and that you decrypt with your private key, so it allows for – it’s a generalized way of doing identity-based transactions.

We did a show about key base. It was actually released today. What about the key-based protocol for letting people have their public keys, would that work with OpenBazaar?

[0:20:56.0] BH: It doesn’t currently right now, but this is something that has been requested. The answer to a lot of the engineering questions is like, “Well, how much time do we have and what are our priorities?” Yes, certainly something like that could be integrated into the system.

I mean, early on we had a GPG feature. It didn’t get used a whole lot, and we didn’t carry it over to our new version. But there’s a lot of different ways things could be tied in. We just have been staying simple for the most part.

[0:21:31.8] JM: I actually haven’t done any shows about Blockstack. I’m a little curious about that. What does Blockstack do in terms of identity? Why is that your identity system that you’re looking towards working with?

[0:21:47.2] BH: Things move fast in the blockchain space. But originally, Blockstack was called Onename, and their primary service was they used something called Namecoin to create domain names. The idea was like, we'd have this decentralized domain system to replace DNS.

For us, we thought a couple years ago that's exactly what we need. We need to decentralize naming systems so that people can reach stores. We went with one name when it was back with the basic – the basic concept was just that. We still use mostly just that feature out of Blockstack, but Blockstack has grown – I mean, they change their name because they wanted to grow past just naming systems and they're creating more of like a decentralized internet approach.

They want to have storage, decentralized storage and everything that's used – or needed to create a decentralized web. That's their new vision. We use part of it. I mean, it's a whole stack of capabilities, but we're looking at what else they offer as well. Right now, we use IPFS mostly for storage and stuff, so we didn't really have a need to use a lot of the other Blockstack stuff.

[0:23:03.1] JM: I see. Okay. They have some stuff that overlaps with the IPFS Filecoin etc. project.

[0:23:09.9] BH: Exactly. Yeah.

[0:23:10.9] JM: Okay. I think, well maybe not obvious for some people is that in a peer-to-peer world, a lot of the things that are simple in decentralized world are less simple. For example, if you just want to do a search over the listings in OpenBazaar, it's not exactly like searching over Amazon, hitting Amazon servers and they search over some centralized database that has all the listings, it's a little bit more complicated.

To help illustrate to people why this is not as straightforward as certain centralized things, and this is like totally a trend in the shows about Bitcoin and decentralized stuff that I've done is like, the temptation is always to go decentralized or like, "Let's make a decentralized search engine. Why not?" But you can't do that if you want to adhere to the decentralized nature of what this movement is trying to do. It contrasts the centralized search approach with the decentralized search approach.

[0:24:19.1] BH: Sure. A really good analogy is the P2P file sharing that we've seen over the last 10 or more years. Originally we had Napster and LimeWire, which were much more centralized peer-to-peer networks, where you could get on them, you could search for things right in the app, find the items you wanted and then you click on it, download it and it was easy.

But then, those guys got shut down. It was not good. Then BitTorrent came along. Most people realized that there's not a awesome search feature inside of BitTorrent itself natively. You have to – people say go to Pirate Bay or whatever, find a listing, then it opens up a magnet link or whatever and then it opens up your BitTorrent app and it's always been that way.

The reason is because it's just so much harder to build a good search engine on a decentralized technology, and it's the same for OpenBazaar. The reason is because a peer-to-peer network is full of a bunch of really diverse peers. In our case, we have people running OpenBazaar in over a 180 different countries, on different internet connections, some really, really horrible, some really, really great. They are in different geographic locations, so there's different latencies and how you connect to people.

Not to mention that, but people are turning off their app and turning it on and turning it off and turning it on. You can already see the difference between trying to find. If I'm trying to find a comic book that someone is selling, I have to crawl all over that really, really unstable network of peers going in and out and ask each one of them somehow if they've got this content I need, and then I want it returned instantly and I want it to be sorted and searchable.

I mean, the demand is really high in relation to what you can provide. The opposite is like Google which has already done all that crawling. They're constantly crawling with massive machines, data centers. They're cataloguing it, they're optimizing it, indexing it, and then they're caching it and sending it back to you instantly.

You're only asking one really, really fast data center to give you results. The centralized approach is so much better than decentralized way. I mean, that's why Google is so great. I mean, it took a decentralized internet and made it fast.

In our case, we realize that that central point of failures is not great. In 1.0, we did not do a centralized search, we just made – we cobbled together a decentralized search, which was really rudimentary to see how well it would work. It basically stunk. It's really bad. It just was super slow, didn't return results very well. It basically worked about as well as you think it would after I explain that.

In 2.0, we took a different approach to it and we said, "Look, we realized that the technology and engineering is not there yet to really build a great decentralized search engine, like no one has done that yet." Rather than create one central database, one central index, search index, we're going to let anybody create a search engine and we'll integrate those in.

If somebody wants to build a search engine that focuses primarily on real estate properties, they could do that. If we have one that's like super strict and doesn't want to allow any kind of sketchy products or services in there, fine; whatever the niche is.

In a new one, we have three search engines right now, different search engines and you can choose which one you want as your default, or you could browse between them. They have different indexes. I mean, some have different rules, restrictions. OB1, my company we run one, which we operate out of the US, so we follow US laws. Anything illegal in our jurisdiction we remove from the index, which may make people happy or unhappy depending on who you are.

There are two other options and they have different rules and operate out of different areas. You could even create a separate one on behind Tor or something that is just anything goes. It's up to the users. While they are central points of failure, the experience is just so much better that we decided that this is an okay compromise, it was an okay enough compromise. It's not truly a decentralized search, but at least it works. It's just one example of a compromise we've had to make so far, because we just know the technology is not there yet.

[0:28:58.9] JM: This is a great time to acknowledge that OpenBazaar is a protocol. This is not a centralized store where everything is the same no matter where you – well, I guess if you go to Amazon in China, it's different than the Amazon that you see in America. Even that is balkanized world.

It's a protocol. There are transactions that occur over OpenBazaar that are for illicit items. But there are conversations that happen over TCP/IP that are elicit, that are illicit, that are illegal, and we don't blame TCP/IP for that. Similarly, we're not going to blame OpenBazaar for the sale of heroin under certain situations.

Let's get in to talking a little bit more about this protocol. Describe the trade protocol, the trade protocol that describes how trades proceed.

[0:30:04.6] BH: Sure. The first thing is like the entire mechanics of the network operate using something called Ricardian contracts. Really early on – I mean, we started in 2014. At that point, I believe ethereum was still being built. There really weren't any other truly smart contract platforms out there.

Bitcoin has a scripting system within it. You can do pretty basic smart contracts, like the escrow one I describe. But nothing really elaborate, like nothing that you could create this complex protocol in top of.

We said, "Okay, look. We know that some of these things are coming out and there are going to be all these different options and we don't know which one is going to win. Let's create something that's a little bit more agnostic, something more neutral." We found something called Ricardian contract.

My co-founder Washington Sanchez pitched this idea to us. Basically, the idea is that you have a contract which is machine readable and human readable at the same time. Basically, in our case it's a JSON structure. We define what the contract structure is supposed to look like. There is a listing structure, which would be you have to have a title and it has this many characters at most. It has pricing and it's going to be priced in Satoshis or Bitcoin.

It basically defines the scheme of what a listing should be. That's the beginning of the contract. But then also, we define in our protocol what are the phases that the contract can go through. There is the initial offer, which is like this is what I'm selling. Then there is a bid basically, so the buyer comes along and says, "I want this contract so I'm going to offer this to you."

Then there is the acceptance, then there is a bunch of different phases within OpenBazaar that it goes through. If the vendor rejects it, or if he issues a refund, or there is a dispute, there is all these different – there's a whole flow that OpenBazaar goes through. That's the definition of the trade protocol. How does that work? What do the peers actually expect in each of those states in order to be a valid contract?

Then we use digital signatures throughout that process to make sure that the contracts are valid and that the right people are actually participating. That's all written into the code. It's not necessarily a smart contract so to say, so to speak. But it is a contracting system and there is a protocol for how those proceed.

[0:32:50.3] JM: Would you contrast the smart contract versus the OpenBazaar contract as being less smart, because there is a more narrowly defined set of features that you can put into a contract?

[0:33:02.9] BH: I think smart contracts for the most part, I think they lean on more automation and kind of – For instance, like a truly smart contract for a marketplace like ours might be like when the software would look to UPS's API and when it sees that this package ID was delivered, it would instantly release the money to the merchant and everything would just go on.

In our case, the buyer would have to go back into the software and say, "Yeah, I got it." Hit a button, and then that would initiate the next phase of the contract. We don't have the ability to do a lot of those automated things, like natively as part of the cryptocurrency. But it does similar things.

[0:33:50.3] JM: That's a cool aspirational future to look towards, because there is no reason why we couldn't have that eventually.

[0:33:59.6] BH: Yeah, that's true. The biggest compromise here I think is when it comes to smart contracts, you have to commit to one platform, because if I choose ethereum for instance as my smart contract platform, I have to write all of my code in solidity, the language. There is the certain nuances of that language and ethereum that you have to code around and do all that.

What if you want to move to a new platform? It's a really hard process. What we've done is we just tried to look at it from the perspective that there are going to be a ton of these currencies out there. We've already seen Bitcoin's dominance go down, because there's all these other new tokens and things out there.

We want everybody to be able to use OpenBazaar. It's not a Bitcoin protocol per se. It's really just a decentralized protocol and so Bitcoin happens to be the first option that we leverage, but we want everybody to build and use in. We've tried to build like a very agnostic contracting language that can work on all those platforms.

You're right, as far as aspirational – yeah, sorry to cut you off, but just to finish the thought, I think using Oracle and hitting outside APIs to automate those process, you're exactly right. That's coming and we're just trying to really nail down the experience to make sure that it's really, really good, and then we slowly roll those things in as it makes more sense, rather than just try to do too much, like get the whole kitchen sink in there from day one.

[SPONSOR MESSAGE]

[0:35:39.2] JM: At Software Engineering Daily, we need to keep our metrics reliable. If a botnet started listening to all of our episodes and we have nothing to stop it, our statistics would be corrupted. We would have no way to know whether a listen came from a bot or a real user. That's why we use Incapsula, to stop attackers and improve performance.

When a listener makes a request to play an episode of Software Engineering Daily, Incapsula checks that request before it reaches our servers and it filters the bot traffic preventing it from ever reaching us. Botnets and DDoS attacks are not just a threat to podcasts, they can impact your application too. Incapsula can protect API servers and micro-services from responding to unwanted requests.

To try Incapsula for yourself, go to Incapsula.com/2017podcasts and get a free enterprise trial of Incapsula. Incapsula's API gives you control over the security and performance of your application and that's true whether you have a complex micro-services architecture or a Wordpress site, like Software Engineering Daily.

Incapsula has a global network of over 30 data centers that optimize routing and cashier content. The same network of data centers are filtering your content for attackers and they're operating as a CDN and they're speeding up your application, but doing all of these for you and you can try it today for free by going to incapsula.com/2017podcasts and you can get that free enterprise trial of Incapsula. That's Incapsula.com/2017podcasts. Check it out. Thanks again, Incapsula.

[INTERVIEW CONTINUED]

[0:37:28.8] JM: Central to OpenBazaar's protocol is the idea of an escrow. An escrow is a neutral party that two people can't – if two people want to make a transaction, if I am going to send you a t-shirt, you put money in an escrow account so that when the t-shirt makes it to you, the money will make it out of the escrow account to me. Because if we didn't have an escrow, I would have to send you the t-shirt and I would have to trust that you're going to send me the money eventually.

Escrow is fundamental to how OpenBazaar works. Describe how the escrow services implemented.

[0:38:11.5] BH: Sure. You're exactly right in how that works. First thing, OpenBazaar supports both options. A merchant can choose to operate under an escrow business, or just accept direct payments and make the users trust them.

Some vendors opt for that, because the escrow actually adds a little bit more complexity to the situation. If they're a well-known brand they may just say, "Hey, look. Our users, our buyers, they know us well enough. They know where to find us. They can trust us." That's their choice. But if you're a nobody and you're running a small business, most users are going to opt not to buy from you, because it's too high a risk, so they look for the escrow.

The way that escrow works is a merchant has a public key, like you mentioned earlier in the show and the buyer has a public key, you know their identities for OpenBazaar. What happens is you take those two keys and you can craft a special type of Bitcoin wallet, or address that is a mixture of those that basically in order to send money out of the wallet, you have to have both people sign a transaction before it's valid.

You have this ability to create an escrow type wallet and when money goes into it, they have to agree on what to do with that. In our case, we use that capability, so when a merchant or when a buyer wants to purchase something, he'll get – the nodes will get together and they'll create this address, and the buyer will send money into that address rather than send it directly to the merchant.

The merchant, since he owns the address, he'll be able to see that money went into it and got confirmed in the blockchain. So okay, the money is definitely in the escrow account. He'll feel secure enough to deliver the goods. Once the goods are delivered, the buyer will actually sign a transaction saying, "Yes, I want to move all that money out of the escrow account and give it to the merchant's wallet that he owns by himself."

Then he'll send that transaction to the merchant and the merchant will sign it as well, and he'll send it to the blockchain. Then the blockchain will say, "Okay, both people that own the escrow account want to move this money out of here. Let's do it." Then it confirms and that's it. The merchant will get the money.

Now we also have a backup. If the buyer forgets to release the money to the merchant, or refuses to, after 45 days that transaction will just happen. The money will go to the merchant. They're encourage to resolve the transaction before that time period goes out. But this is a result of we've seen a lot of cases.

When you buy something off at Amazon, you give them the money, you get the goods and you forget about it. You don't go back into Amazon and say, "Yeah, yeah. I got the goods. He can have his money now." That whole concept doesn't translate or exist.

You see a lot of times the buyers will just abandon and they will forget to give the merchant the money and the merchant is really upset. In this case, it's just an extra protection for the merchant to be able to still get that money.

[0:41:18.5] JM: Explain more how disputes can arise and how those disputes can be resolved. I know you touched on it there, but go into that in a little more detail.

[0:41:29.3] BH: Okay. I explained the happiest trail, easiest case. But sometimes that doesn't always work out. Somebody is unhappy, either the merchant or the buyer. We have a concept of a third person, a third type of user called the moderator.

What the moderator does is you can think of them as customer support. In Amazon, if you have a problem, the guy didn't send you the right product, or it was broken or something, you contact Amazon and ask them to resolve the issue.

In OpenBazaar there is no company to call. Well, we want to exist but we don't – that we don't run the network ad we don't have visibility of the transaction, so there's nothing we can really do. But we have a third type of user called a moderator, and they're who you call when you have a problem.

Within OpenBazaar interface, you can open up your order and you have a problem you hit this – I have a dispute, file a dispute. What happens is that third type of user will get notified and say, "Hey, we have a dispute. We need your help to resolve this." Now to back up, how did that guy even show up – how did he get involved at all?

Merchants can choose from a list of people who are on the network that serve as these dispute people, and that's an opt-in thing. Anybody can be a dispute resolution person and advertise their services.

You add them to your store. You can pick a couple of them. They have different costs associated with them. Like if you want to be a dispute person, you can say, “Hey, I’ll help you resolve your disputes. I charge 2% of the transaction if you need me.” You hire these guys out of the network to help you out if you have disputes.

When you purchase a good, you will select the moderator you want to use or trust for that transaction that the merchant suggested, and they’ll be there just in case there’s a problem. You’ve gone back to your order, you filed a dispute, the person you chose in the purchase process comes in to the picture. The three of you have a joint chat session. You can explain to them what’s going on, what the problem is, you both get to give your sides.

The moderator can then decide how to resolve the dispute if you guys can’t figure it out yourself. Basically they have the option to either refund all the money back to the buyer, give all the money to the merchant or any combination thereof, so they could split it down the middle if they can’t decide. They could give a bigger portion to the merchant and a little portion to the buyer. It’s up to them, then they get their cut out of that.

The way that this works is that it’s an even more complex version of the escrow address. It’s a two of three address. What that means is that two of the three people involved have to agree to sign a transaction before the money can move.

It breaks the deadlock between a buyer and a merchant if they can’t agree on what to do. The moderator will sign a transaction saying, “Here is the refund or whatever.” He’ll send it to whoever needs it, then they would sign it. If it’s a case of a refund to a buyer, the moderator would say, “Okay, here is a transaction where we returned all the money out of the escrow back to the buyer. He signs it, he sends it to the buyer, the buyer would sign it and submit it and he got his money back.” Or it could go the other way. It’s a little bit more complex version of a smart contract within Bitcoin, which is like two of three.

As like a super complex way, it’s hard to explain it. It makes more sense when you’re actually using it. But it creates a marketplace for dispute resolution, which is also kind of interesting. It’s crowd sourcing customer support. When your network is not run by a company, you can’t hire a helpdesk or customer support team necessarily. Like we're scaling it out to the whole network, and people can earn money to help others.

[0:45:23.0] JM: Makes sense. To go along with the crowd-sourced narrative, OpenBazaar is an open source project. This is a tremendously complicated project as you've articulated. You've got this complicated peer-to-peer process, you've got payments, you've got incentives between lots of different parties that you have to keep aligned.

Managing this across an open source project and making sure that everybody who's working on the open source project understands the different parts of it has got to be a complicated management challenge. Let's talk about the open source a little bit. First of all, what are the parts of the project?

I was looking at the open source repo and their several different projects. How is it broken up? What are the different projects that are in different repos?

[0:46:18.3] BH: We have a bunch of different repost, but the two biggest and most important ones are the backend and the frontend. The backend server, which is OpenBazaar-go, which we wrote it in golang, it basically is the node software basically, the server software. It is what complies to the protocol. It's what handles the Bitcoin transactions. It does all the heavy lifting.

The other one, the desktop repo is basically the client, which just talks to the server through an API, through a rest API. I mean, it makes the user experience shows what the marketplace could look like. In our case, we thought of the client as being as a reference implementation.

Anybody can run the backend code and write their own custom frontend to talk to it and that's their view of OpenBazaar. This is just our example of what it could or should look like. Those are the two repos that we work out of mostly. Those two teams have to work together to make sure that they're in-sync on what's expected, because if the backend changes the way that transactions work, the client is not going to understand how to send or purchase a good or whatever.

Yeah, there is a lot of coordination between that. I mean, luckily we have a pretty small and dedicated team of devs and a lot of them work for my company, so we can coordinate really well. But it is a really huge challenge to so many moving parts.

We run into a lot of problems all the time, where there's a misunderstanding of how something might work. But the cool thing about open source is that it's all out there, and so people that come along and are interested in knowing more about it or have a knowledge in a certain area, perhaps search engines or Bitcoin transactions or something like that will find stuff for us and make suggestions or help us fix things.

It's like a huge mass of team effort, which is the best part about open source is like anybody can collaborate with it and contribute. It's a beautiful meritocracy. We're really lucky to have a lot of people helping out.

[0:48:36.8] JM: How do you manage the open source community? What are the challenges that you've had to overcome as you've been learning to delegate, or maybe you can't delegate because people are just contributing of their own accord. What piece of advice do you have for people out there who are trying to manage open source communities?

[0:48:58.8] BH: I think there's all kinds of unique challenges. In technology, I mean everybody has an opinion about how things should be built, or what languages you should use or how it should be done, or what it should look like.

Really the hardest management task is getting people to come together on a certain vision, in a certain approach and follow that all the time. You constantly get new people that come onto to the project that maybe unintentionally try to hijack what's going on, like, "Oh, what did you use golang? You should use this." Or just submit code to do things in a different way, which has pretty big ramifications.

It may seem like it's a useful feature, but it screws up everything else you're trying to do. How do you encourage people to contribute when you don't necessarily want to take all their stuff? That's a big challenge. There is different skill levels of people that come and help and don't know where to start. How do you get people involved in a really complex project? Like where can they dive in and help out?

Other challenges are just human challenges; people get in arguments and people that are critical to the project decided don't want to work on it anymore. We've had that happen before. I mean, there's just all kinds of different challenges. It's not much different than a normal closed team, except that maybe people feel compelled to be a little bit more brazen and outspoken because they're not necessarily being paid in a lot of cases. It's a volunteer thing. You have to understand that.

[0:50:40.8] JM: We've seen that the brazenness or the acrimony, we've seen the extreme of that in the Bitcoin community. We've also seen the more positive atmosphere that can happen in the ethereum community when you have a benevolent dictator that is really tuned into the different incentives and the different arguments for either side.

I think Vitalik has done such a great job as leader of the ethereum community. I don't know much about the OpenBazaar community. Maybe the stakes are not exactly the same, because people don't have like an OpenBazaar currency, but can you talk about maybe some of the more vitriolic situations, or have you been able to avoid vitriol? Could you go there?

[0:51:36.3] BH: Yeah, sure. Obviously, a project like Bitcoin or ethereum is going to have way more issues, because A, like you said it's a currency and it's got value and anything with money is usually pretty contentious once it gets large.

You're talking about millions of people being involved with that and like we're not there yet with OpenBazaar. You have way more diverse stakeholders. But the thing is we have a huge overlap with that community as well. Almost all our users are Bitcoin-savvy. In a lot of cases they have a lot of Bitcoin. Some of our users are millionaires in cryptocurrency.

If you have screw you money, and that changes how you act with people a lot of times. It's sad to say, but if you feel like you have a lot at stake and you have a lot with control and you don't have a lot to lose, you're just going to be super honest with people and make claims. We get that a lot.

Bitcoin has that same problem too. They're making million dollar bets over certain things will happen and this is insane. But that comes with the territory, so we have to deal with that. In our case, in OpenBazaar like we said, we still have a pretty small development team, but we do run into issues.

A lot of it is what is the direction – where should we go? Which direction? Because you only have so much bandwidth to build things. You only have so many people working on it. If we say we're going to turn – if one person wants to make sure we build a super secure anonymous wallet into the app, that could take the whole team and that could keep up from building some other important feature that we think we need.

A lot of the contention is really around where do we go? There's so many different angles we could take this. Right now, because we're about to launch 2.0 probably later this week, the full version, and then we're going to be thinking about what's next for OpenBazaar.

We have a whole slew of ideas to put on the roadmap, and that will have to go into that forum and make our case for what we think is next and we do that in an open source way. Yes, I am the benevolent dictator of OpenBazaar in a lot of ways, but I try to make sure that it's a broader consensus. Like I don't just say, "Hey, we're going to do this from now on."

I'm usually used as like more of a tie-breaker type of situation where if we literally can't break through a log jam, I will help out. I think that so far that it creates some confusion sometimes, because that we have to work it out, you had to figure out what you're going to do and there's no one to just say, "Hey, we're doing this." I think it's created like a really interesting and creative platform. When you look at it, it does some things that are super unique, I think.

[0:54:40.7] JM: What kinds of transactions are most popular on OpenBazaar? Tell me about the culture and the types of people that are selling and buying stuff.

[0:54:52.3] BH: Yeah. I mean, this is one of the – more challenging questions to answer, because we don't really have a deep insight into exactly what people are doing. We can't just look in our database and say, "Ah, a bunch of comic books sold."

We can see what's on the network, like what are people currently offering. Right now, a lot of it is like collectibles, clothing, kind of small business type stuff. There is some drop-shippers that are selling all kinds of electronics and things like that.

If you think about it, in Bitcoin – I mean, Bitcoin is a deflationary currency, which means it's gaining value basically as time goes on. If you have 5 Bitcoin today, you may be worth a $100 we'll say just for conversation speed. But next week, maybe it's worth $500.

There is this really huge incentive for people to acquire Bitcoin, but maybe not spend Bitcoin. We see a lot of people offering up things that like, "Oh, I have this in my house and I want to get Bitcoin somehow, so I'm going to put this on there and see if people will give me some Bitcoin for it."

You have this weird collecting mix of like small businesses and garage sale type stuff right now. You also have a situation where tools not quite advanced enough to tie into other types of systems that serious merchants need. Shipping integrations, fulfillment systems, things like that, like a Shopify might have or an eBay.

We're not quite attracting those types of merchants yet, but we're working on it. In terms of buying, you can go into the search engines and see like what products have ratings. I'm looking right, there is technical books, clothing, comic books, Steam games, things like that seem to be the top items that are being rated.

That ratings are tied to transactions, so it is one unique way of seeing what has actually been purchased on the network, but we don't know how many. For sure, we don't know who's buying it, things like that.

[0:57:05.5] JM: OB1 is your company that leads the development of OpenBazaar. What are the goals of OB1?

[0:57:15.0] BH: OB1 didn’t exist from anything. We went for about a year, a little over a year building the software just in our spare time. It’s a side project. Then we raised venture capital and started OB1.

The goal of OB1 was to basically build a business on top of the platform. Our hypothesis was, “Look, we’re going to build this open protocol and there is going to be all kinds of different things on top of it to improve it that we wouldn’t want to bacon to the protocol or make open source.” Bu someone is going to need to offer it to the users.

We want to be the first company that capitalizes on that, because we build it, we understand it, we have a really great advantage there. OB1, the goal was to contribute to building the protocol, but also eventually offer services to users.

We haven’t gotten there yet. We haven’t gotten to the point where we’re offering services to people yet, because we’ve been focused primarily on just getting the product out in a state where people can use it well.

We’re in that transition period between delivering the product and actually starting to build services that are useful on top of it. I mean, you need users/customers before you can sell them something. That’s really still our primary focus.

[0:58:32.3] JM: Yeah. You think it will be like the Wordpress business model?

[0:58:36.5] BH: I don’t think it will be that, because I think – I think more likely is that we’re going to try and find ways within Bitcoin or the protocol or some other cryptocurrency to generate a revenue model.

It’s more interesting to us to stick with the blockchain paradigms, rather than use the Wordpress model. Also Wordpress is like – I think for instance, in their case there is a much clearer way to charge their users. For instance, like there’s a server software. You need servers and you need people to run the software and manage it and maintain it. You either have to do it yourself, or you need someone that’s an expert. That’s a great revenue model for us.

OpenBazaar, we want it to be easy enough for anybody to run on their own computer, their device. They don't really need hosting for instance. I mean, not to mention we don't really want to be in control of hosting it, because then we're a central point of failure and it goes against the decentralization model.

We have to look at ways of creating revenue that are a little bit different. For instance, maybe we offer some kind of insurance model. Maybe the escrow model is not great and they're having problems and they want to use some kind of fire protection. Maybe they buy a buyer protection insurance through us, we offer that.

Or maybe we have a reputation service, like we've got merchants and vouch for them. These are just a few ideas, but those are types of services that wouldn't be part of the core protocol, but still would provide value to users and it would be an opt-in option.

[1:00:22.0] JM: Yeah. Well, it's a more – certainly a longer term point of view than saying, "Let's figure out a way to ICO."

[1:00:29.5] BH: I mean, ICO – I think ICO, the whole concept of ICOs is craziness wrapped around a nugget of an idea that could be good. It could be good. I think I still haven't seen someone do it right. We have a lot of –

[1:00:47.9] JM: Not even IPFS?

[1:00:49.3] BH: Well, so IPFS I think – I mean, obviously they haven't delivered yet, so I don't know for sure if they're going to meet their demand. I really love the team. I mean, Wan's a good friend and I think that they're great. If anybody is going to do it, I definitely believe in them.

But we just still haven't seen that happen. The idea of Filecoin is good, and we just need to see it executed. That's what I think is so scary is that now we have something like 1,900 different tokens out there, and we still don't have like one example other than ethereum itself as being super successful. Ethereum's biggest success you could say is in creating more coins.

The smart contract reality hasn’t hit us yet. Or it hasn’t been completely fulfilled, other than for crowd funding. Who knows? Is it a big bubble and it’s going to blow up and none of those things are ever going to happen, or are we just not there yet?

I tend to think that we’re probably not there yet, and that there are a few that are going to do it right and they’re going to actually come up with something cool that’s useful. Most of it is going to be garbage. The way that we’re looking at is we rode a huge block post about like why we wouldn’t never do a token, or why we’re not thinking of a token at the moment, but we always left the door open.

If there was a way that we could really be assured that this is something that would benefit our community and make a difference and it could be done in a way that was right for everybody, then we would. I mean, we made that compromise when we took venture capital funding, which was a huge thing.

There were a lot of people that were like, “Oh, we’re not going to work on this anymore, because you guys raised millions of dollars and you can just pay for it.” The change in dynamics of our project dramatically. But we wanted to see this thing happen and we wanted to make sure we accomplish our goal.

In the same way, I mean if it comes down to it there may be a day where an ICO or some kind of crowd fund is the only way we can move forward. Maybe VCs decide, you know blockchain companies are just not going to return on our investment and we’re out. How do you fund your project? They become the only option.

Never say never, but ultimately we haven’t really seen a model that works perfectly, or that works well enough.

[1:03:12.4] JM: All right. Well, Brian we didn’t get to talking about the IPFS refactoring, but maybe, I don’t know, somebody else on the team, or we can do a different show about that. Because it seems like a very interesting topic. That seems like a complicated migration, but unfortunately we’re out of time.

Thanks for coming on Software Engineering Daily. I know you're a busy guy and I am watching the OpenBazaar project closely. It's really fascinating.

[1:03:36.9] BH: Thanks for having me. I love talking about it, so it's never a problem.

[END OF INTERVIEW]

[1:03:42.9] JM: Thanks to Symphono for sponsoring Software Engineering Daily. Symphono is a custom engineering shop where senior engineers tackle big tech challenges while learning from each other. Check it out at symphono.com/sedaily. That's symphono.com/sedaily.

Thanks again to Symphono for being a sponsor of Software Engineering Daily for almost a year now. Your continued support allows us to deliver this content to the listeners on a regular basis.

[END]