TALK NOTES

The Lightning Conference
October 20th 2019

Many of you may have noticed that my voice sounds like shit. That's not because I'm using a bad voice modulator (I wish). I wasn't able to talk at all yesterday morning. Warning in advance – I may have to default to whispering. If you don't understand me, don't worry; my slides and a transcript will be made available tomorrow.

Hello and welcome to "Lightning for Journalism." My name is Janine, and I will be talking about how the capabilities of the Lightning Network could enable sustainable journalism. I am an independent investigative journalist. This talk will be a high-level view of the technology and ecosystem. If there isn't time left over for Q&A at the end, feel free to talk to me at some other time during the event. In case the mask didn't make it obvious, this is a no-photography, no video session, but they will be recording the slides and audio.

I don't think one needs to particularly observant to notice that journalism all around the world has some severe issues. Some are old, others are new. Journalists and their sources still have to navigate jurisdictions in which they have inconsistent legal protection, and even when they are protected, they may be subject to extra-judicial censorship and self-censorship.

In terms of economics, journalists and media organizations often struggle with under-funding, misaligned incentives related to the dominant ad-driven surveillance system and so-called "benevolent" billionaires. They face a variety of security threats, tend to be heavily reliant on centralized infrastructure that makes them easy targets, and are led astray – willingly or unwillingly – by disinformation campaigns.

Censorship can come in many shapes and sizes. Many of you probably know about the banking blockade put in place against WikiLeaks since December 2010. More recently, there's been outrage about Apple and the NBA taking steps to limit the flow of information about controversial actions and events in Hong Kong due to fears that they would lose access to the Chinese markets. In South America, the Venezuelan news outlet TeleSUR was recently blocked by broadcasters in Ecuador, under pressure from the Moreno government, which is trying to cover up unrest and police brutality in their capital of Quito. What these three examples show us is, whether we like it or not, it is often the case that liabilities can easily cross borders, while rights usually don't, and nationalized infrastructure is especially weak against disturbances in the power dynamics of the state.

Countries that are relatively weak on the geo-political stage end up being fighting grounds for media imperialism by other states, which can suppress localised independent reporting if it does not become beholden to those powers. This is a really interesting article about how media organizations in Africa have become dependent on foreign aid and economic development projects by the United States and China, which in turn influences the worldview underpinning their journalism, and results in narrative clashes.

Oh boy – in come the tech-bros and brahs to tell us all about how "blockchain" will save journalism. Not Bitcoin, not a particular blockchain, just "blockchain." It is almost as if they are proposing a plan that they don't understand at any level. So before I go into how Bitcoin and the Lightning Network can be used by journalists for better sustainable journalism, I want to make clear that I don't share that perspective. At best, in the next five to ten years, I predict that majority of those who will benefit from these tools will be western, English-speaking, niche, technologically sophisticated journalists (in case you didn't know, there aren't that many). Even that will be a huge challenge.

First, I want to go over some case studies where the mindset of "blockchains solve everything" merely resulted in replicating and even worsening existing issues. I assume most of you have heard of Steemit before, but if you haven't, it is a blogging and social media platform using a dedicated blockchain as a content storage database that has been around since 2016. I bet fewer of you have heard of Civil Media, which is a ConsenSys-backed company that developed a supposedly "self-governing" marketplace of newsrooms. But they didn't want to go through all the heavy engineering of creating their own blockchain, so they decided to dump all of their word salads on the Ethereum network, and created an ERC-20 token for the governance mechanisms.

Now I know what many of you are probably thinking – "Ethereum already has a bloating problem. Storing every single article written by multiple media organizations is going to make it worse." But fear not! One of the Civil Media partners clarified that they are not doing storage, they are doing... decentralized archiving. Good to know... really dodged a bullet there! If you want to know more about the problems I see with Civil, technically, organizationally, etc. you can check out this very long thread about it on Twitter.

Unsurprisingly, after a mere 2.5 years or so, Steemit is buckling under the weight of all the word salad, and Civil's token sale failed because most of the people who tried to get involved had trouble migrating through the multi-step, multi-app, KYCed process of acquiring the tokens. ConsenSys ended up holding about 80% of them, which meant they had a solid majority position in terms of the governance process and could propose or veto any changes they wanted. But who needs the tokens when you run the infrastructure? ConsenSys owns Infura, which runs Civil's Ethereum and IPFS nodes. If you wanted to, say, write an article that is critical of their partnership with the Saudi government and their business operations guy saying that Khashoggi's murder is mere conjecture, they can just pull the plug on your access.

Another "blockchain for X" project fails. Once again, nobody involved really understood what a blockchain is. They think that the properties of decentralization, security, immutability, and censorship resistance come automatically with the software. Which is not the case at all. These are emergent properties based on the number of people involved, the design of the infrastructure that is deployed, and the convictions and principles that are broadly held within the community. Of course, I don't really expect some Brooklyn hipsters to have a great understanding of how to thwart actual censorship, so it doesn't surprise me that they are proud of themselves for building a more inefficient content management system.

In conclusion: stop abusing blockchains as content management systems! And for goodness' sake, use OpenTimestamps.

After that healthy dose of reflection and skepticism, let's look at what Bitcoin and the Lightning Network will do. The combination of Bitcoin and Lightning offers three main things: censorship resistance, privacy, and micropayments, or the ability to implement "streaming money."

The benefits of censorship resistance for journalism should have been evident to anyone who read the whitepaper, because Satoshi wrote in numerous places about timestamping. 'The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.' Furthermore, 'the timestamp proves that the data must have existed at the time, obviously, in order to get the hash.'

When it was announced last October that Forbes would be using the Civil platform, a marketing puff piece claimed that Civil was "the first major media company to experiment with publishing stories to the blockchain." Which is nonsense. That I know of, if there is any journalist or publishing organization who should get credit for being first to experiment with blockchains, that's WikiLeaks, because since June 2011 they have officially not only used Bitcoin to accept donations, but on a number of occasions they have also used it for timestamping. The most prominent example is where they actually embedded a whole Cablegate file across a whole bunch of transactions (like I said, I don't generally recommend that as a practice). Since then, they have taken a much more minimalist approach. Obviously, if they had tried to "decentralized archive" the millions of files they have, Bitcoin could not handle that.

In 2017, Assange still brought up an interesting counter-point about the value of timestamping or using the latest block hash as a "proof-of-life" or some other similar proof. 'The problem is, it is very complicated. Experts might be able to do it, but does the average person understand the significance? Will we still default to social proofs?'

In a nutshell, why is Bitcoin censorship resistant? Because not only is blocking the broadcast of transactions difficult, because there are so many ways to transmit it to the network, but reversing a transaction or block is computationally expensive. In addition, Lightning has censorship-resistant properties. It is really hard for intermediate nodes to block payments because with sufficient interconnections between nodes and bridge nodes and private channels etc., 'the network treats censorship as routing failure and goes around it.' In combination with onion routing, intermediate nodes can't determine the originator of any payment, because they only have visibility one hop in either direction.

I am over-simplifying this for brevity. I'm sure that are still attack vectors that need to be accounted for. But this is the design intention.

As Eric Hughes wrote in the Cypherpunk Manifesto, "privacy in an open society requires anonymous transaction systems," so it's very important that privacy is a priority when choosing what applications and systems you bring into your work. I mentioned private channels, they're also called non-advertised channels, where you can only see them if you know specific "routing hints." And I've already mentioned onion routing, which has privacy benefits because the routed payment is passed along with each node only stripping one layer of encryption around the "message" away at a time. If you want to know more, there is a great blog post from Lightning Labs with an overview of routing as it currently stands.

It's also important that we be vigilant about the ways in which wallet developers and operators could be threats to privacy on the Lightning Network, because within the first year or so of Lightning on mainnet being live, I suspect that we have already seen a subtle attempt at this. Earlier this year, myself and my co-hosts were interviewed about Lightning Peach by Colin Harper at Bitcoin Magazine because we noticed that there were a number of red flags in their Terms of Service and Privacy Policy, which explicitly said that they were collecting a ton of revealing user information.

Initially they fought us on that allegation, but the discrepancies were so obvious that they couldn't maintain their position, and they have since added a so-called "privacy mode" into their wallet.

If you want to know more about privacy practices and tools for Bitcoin in general, I gave a talk almost two months ago titled "Bitcoin Privacy: On- and Off-Chain," which you can find on my website.

Andreas Antonopoulos introduced the term 'streaming money' in a talk from 2016. "If we can do payments that are on a millisecond frequency, as low as a satoshi, why not get your salary paid every minute?" Within the next five to ten years, I think we will be opening up more internet-based services to streaming money applications. In the context of journalism, you could be paid by the article, which would be so much easier and even cheaper per reader due to the lower threshold for payment size. But you could find more creative ways to measure and value your output, such as pay-per-word or pay-per-minute or second. Not your minutes and seconds necessarily, but how much time your readers spend engaging with your writing. Apps like that already exist for Bitcoin, like ProTip.

We don't necessarily need to get rid of chunky payments altogether, because re-building an economy entirely on micropayments and streaming money will still have drawbacks, especially in the first five to ten years of implementation and adoption. Micropayments could significantly lower the barrier to entry, especially in terms of having a more global audience, but chunky money could remain a viable option to have some stability, and be less cognitively taxing.

Since I've been working on researching what I've termed "revision-controlled journalism," using version control and open-source intelligence, I've been looking out for new tools coming on to the scene. And the three main Lapps that I've come across so far are Yalls, the oldest proof-of-concept in the area by Alex Bosworth, Lightning Publisher for Wordpress from the Elements Project at Blockstream, and LibrePatron, a Bitcoin-based alternative to Patreon by Jeff Vandrew.

Yalls is probably the most familiar to people, though as Alex Bosworth himself says, it is just a proof-of-concept that is supposed to illustrate the basics of what is possible with micropayments and blogging. This is the most centralized option of the three, obviously, because you don't necessarily need to self-host anything.

The Lightning Publisher was released early last year. It allows you to add Lightning payment buttons into WordPress-based pages. When the reader comes across one of these articles, it gives a brief preview (which you can modulate the length of entirely to your liking), and the option to read more by sending a Lightning payment. This is an application within the BTCPay Server suite, and you can find a video for how to set it up on the BTCPay Server YouTube channel.

Finally, there is the mostly chunky money application LibrePatron, a Bitcoin-based Patreon alternative. It also works with BTCPay Server, and has many of the same features that you would find as a creator or patron on Patreon – minus the censorship, of course. Since it's self-hosted, you have even more customization options for your page and how you can interact with your supporters. On Block Digest, we've interviewed Jeff Vandrew twice now. The first time was to discuss LibrePatron back in February, and more recently the new (mis)guidance from the IRS about tax obligations with cryptocurrencies, since Jeff is a CPA in addition to being a developer.

In terms of usability, I think everyone here knows that we still have a long way to go before there is a robust and sustainable economy that will support content creation and journalism using micropayments, in a way that respects principles like censorship resistance, privacy, and decentralization.

I suspect that one of the largest pools of potential early adopters for Lightning applications that cater to journalists would be ones who are already involved in reporting on this technology and have some level of familiarity with it, maybe even get paid in it, but are dissatisfied with the shenanigans and power dynamics of "crypto-news" organizations like CoinDesk, Decrypt, and even Civil. These are not the only three, but what they share in common is this vestigial reliance on traditional corporate and editorial structures that I think can be summarized as "benevolent billionaire mode," where capital rich companies and individuals agree to fund what is often a failing and unsustainable venture, hopefully out of a genuine desire to benefit the public but not always. Millionaire, billionaire, you get the point.

I'm not saying there shouldn't be any philanthropy or that it is naturally evil in some way, but when you are funded by someone who can absorb your failure without much consequence to themselves, you as a journalist, you as a media organization, won't see the cracks, won't be motivated to see the cracks as quickly, when they start to form. The advertising surveillance model is actually very similar: it is just another "benevolent" billionaire situation where *they* have an unsustainable and corrosive revenue model too. When your incentive is not to maximize the amount of time people spend reading and absorbing your article, but to maximize the attention and consumer spends of your readers to advertisers, there is a problem.

As Julian Assange said many years ago while discussing Bitcoin and internet economics, "where you put your money is where you put your power." Where you source your money also influences how and why you wield your power. So in the next couple of years, I hope that we can start re-routing around the damage that weak and broken practices have caused, and start building more sustainable models for journalism.

Thank you!

Janine (J9Roem)