Hi everyone.

I've been a long-time lurker in this forum, and finally created an account. My background was originally in decentralizing social networking, through my company Qbix. Since 2011, we built an open source operating system for the Web, with reusable components that can be used by any site as an alternative to hosting closed-source community features Facebook, LinkedIn, Telegram etc. In fact, recently we have been inspired by Ethereum to build the QBUX token to move the Web from feudalism to a Free Market. QBUX is an application on Ethereum, to power the Web micropayment economy, I will post about it some other time. This post is about a new crypto currency protocol that I think may be relevant to the community here.

Having launched Qbix, we reached 7 million users in nearly 100 countries. (Here is avisualization of our users from back in 2016 when we passed the 4 million mark). People use the Qbix Platform to create a social network for their own community. And as time went on, we wanted to help them launch a payment network and communities to issue their own currency to their own members, for everyday payments.

The state of crypto

When we looked around in 2016 and 2017, we saw Bitcoin, Ethereum, Ripple, and a few others. Unfortunately, none of them were suitable for our purposes – namely, powering everyday transactions by millions of people in thousands of communities. The main problem was that there was a global consensus about every transaction in the world. Full Nodes had to store every transaction ever made, going back to the beginning. It wouldn't be able to power payments, and payments is what would make this whole crypto thing "mainstream", as mainstream as Facebook / LinkedIn etc.

We saw that since 2013, the payments processing space was slowly moving from banks to social networks, such as WeChat, Facebook Messenger, iMessage, and so on. This year in 2020, we see announcements by Facebook that they will launch Calibra in WhatsApp, and Telegram will launch Grams inside its messenger.

So basically, unless decentralized crypto gets its act together (with Ethereum 2.0 etc.

) the payments space will belong to Facebook, Amazon, and the Chinese government, etc. Just like the social networks belonged to them. Calibra may not be terrible, but that network of banks will be intermediaries in all transactions, similar to Ripple, etc. Not exactly decentralized.

Furthermore, innovation on these platforms may be restricted, or at least have the sense of "sharecroppers" working for feudal lords again, as we had with the Facebook Platform for developers, or LinkedIn, or anyone else. They can change the APIs at any time. They can disconnect you or charge cartel-style rents, and so on.

We need a new Architecture

There is a reason that no one is paying for everyday services with Bitcoin or with Ethereum-based tokens. Both projects have had great success in adoption by investors and speculators and DeFi innovators. But when it comes to actually using

the currency as money (medium of exchange), the network starts to get clogged and the fees go up. It's like renting time on a mainframe in the 50s. At the risk of posting a self-serving link, this presentation drives the point home

.

I am glad to see that Ethereum 2.0 is proceeding apace, and I really hope this will change soon. We need the crypto space to finally power payments

or it will never go mainstream, and the cypherpunks will lose to big corporations again.

Eliminate All Bottlenecks

Back in 2017, we didn't see a light at the end of the tunnel, so we started our own

project. Like Qbix it had to be totally open source, and work everywhere. In addition, it had to be scalable to an unlimited number of transactions, by being embarrassingly parallel, with no bottlenecks.

The problem with having one monolithic blockchain is that you need to obtain a global consensus about every transaction in the world, that goes into the next block. That is the source of all the problems. Consensus is expensive, and ultimately the PoW miner (or PoS voter, etc.) is the bottleneck. Sure, you can increase the block size, but that doesn't solve the core topological problem of having one central computer pack all the transactions in the world into a block. Not only that, but due to how things are stored in Bitcoin and Ethereum, every full node has to keep the entire history of every transaction ever, to be sure that its view of the world computer / ledger didn't get corrupted.

The Internet and Money

To make an analogy with other Internet protocols that have been around since the 1980s. Imagine if people were talking about "how many emails a second can the Internet support". Or if they required everyone to set up a tier-1 peering connection to be sure they are receiving their emails correctly. The reason this doesn't happen is that the Internet is a network of networks. It can support tons of stuff happening at the same time, and route messages between networks once

in a while.

Now, I agree that the Internet is federated. Email, the Web, etc. currently rely on DNS, which has some central authority like ICANN. But within each network, things can happen lightning-fast, and between networks, things can get routed quickly too. Money works similarly: it has value inside a certain community (e.g. casino chips in a casino) and no one really carries tons of it outside the community, without exchanging it for something else, because it becomes worthless. The value of money is only in whether someone else will accept it in return for something you want to obtain. If almost no one is around, the money is worthless and needs to be exchanged (perhaps via some global bridge currency, like XRP is in its ecosystem).

Also, there is a tug-of-war between communities who want to retain money inside the community, and people who may want the freedom to make a "run on the bank" and cash everything out, bringing the community's economy to zero. Governments are wary of people circumventing capital controls, and startups don't want their investors to reverse their transactions tomorrow. These kind of conflicting interests should be documented in some sort of language, that's open and enforced. Ideally, it should be not per-wallet, but per-coin.

Governments and Securities

Finally, you have the idea of securities. Many governments have passed laws that regulate sales of assets which are currently worth near $0 but have a chance to be worth 2-1000x more. The entire startup industry is funded in this way (I should know). The intent of the laws is to protect investors, and require at least extensive disclosures, etc. But the laws have also prevented legitimate innovation and chilled the ICO market. The dream of crypto-currency was that the network participants would own the network. I remember seeing Fred Wilson and many VCs express great enthusiasm

for this disruption of their own industry. Contrast that to[what they say now in 2019]():

If you had programmable rules that are per-coin, then you also can do basic things like keep securities locked up for 40 days under regulation S, and then let them be sold back into the US. You could have one bridge coin be the security, and the community coins would be pegged to USD, EUR or whatever fiat currency of the federation the startup community is located in. So they wouldn't be securities. People could actually spend the money, while the communities themselves would pass KYC / AML – so governments wouldn't let, say, the Sinaloa cartel open up a barber shop as a front to launder money. The US government doesn't require this kind of stuff for transactions under $10K. In fact, there is currently a bill in US Congress to exempt transactions under $200 from taxes!

Intercoin

I should state my bona-fides up front. I am a huge

fan of what Ethereum has done and the ecosystem it has built. The idea of programmable money is needed, and now ETH, DAI and the rest have become actual money

that you can use to fund new DeFi projects. That is amazing. You can factor your cash flows and raise money without your buyers worrying that you're going to call and redirect the cash flows back to yourself. You can benefit from innovations in lending, fundraising, and much more that are possible because of a general-purpose turing-complete language for writing smart contracts.

But, back in 2017, we went for a completely different approach. As I describe it below in bullet points, I think you will see how it might lead to a new, complementary project that has a chance to make crypto go mainstream and be used for everyday payments:

1. Each coin is not divisible.

So unlike Bitcoin there is no growing set of UTXOs. If you want to do exact change, we have denominations of 1/2, 1/4, etc. and you transact with a seller, or with a "change bot" who gives you exact change.

1. Each coin is on its own blockchain.

This is the key difference between Intercoin and Ethereum. Intercoin's architecture is closer to projects like[MaidSAFE]().
There are [mathematical results]() that show the probability of a double-spend goes down exponentially with diminishing returns after 30 or so notaries. You don't need the whole network watching every transaction. And by having smaller sets of notaries participate in consensus, you essentially get the benefits of locally "permissioned" consensus, including lightning-fast resolution.

1. Coins, not balances.

Each coin lives on its own "shard". In Ethereum, a smart contract could attract a lot of money, making it an attractive target for hacking the consensus, so you need a large network to secure it and all the balances. But if each coin in Intercoin is worth 5 cents, or whatever, the effort it takes to find all those computers and hack their consensus far exceeds the reward. And the more value you want to steal, the more notaries you have to hack. The economics make it not an attractive proposition. And when the network is large, it's essentially infeasible to hack a large amount of it because of the [Permissionless Timestamping Network]() recording everything in a scalable way.

1. Coins are the unit of general-purpose computation

Intercoins can be thought of as files in BitTorrent. But they evolve over time, kind of like a Merkle DAG in Git repositories. The coins don't have to be coins, they can be chatrooms, documents that you collaborate on, etc.

1. Community Money Apps

On the Intercoin platform, DeFi developers don't think in terms of smart contracts. They think in terms of making apps for community currencies, that are implemented on the level of a coin. Things like: UBI, Local Consumer Price Index, and so on. For example, you can have a township issue its own currency, have people buy in and out of it, but also issue slightly more every day and airdrop it to all citizens as a form of UBI. The amount could be determined democratically by having each citizen vote to increase or decrease the UBI. The local CPI would measure the median spending on food every day, and the community could vote to cover 80% of that for everyone, ending food insecurity overnight. Intercoin could also be used to donating to a community after a disaster, or to students of a university, and seeing how the money is used. Investors could see statistics on how the startups are spending their money. A decentralized Netflix could be implemented with micropayments for every minute of movies watched. And so on.

1. No centralization

Whether it's user data, votes, or money, gathering too much in one place makes it an attractive place to hack (or for "trusted intermediaries" to dip into or rent-seek). Intercoin was designed to have no miners, no PoW, no PoS, no DPoS, nothing but fully decentralized architecture. It can eventually be used for general-purpose applications like voting in elections, not just money. But in every case, its focus is on facilitating the small transactions first (small payments, individual votes, etc.) and anything larger involves more validators. One side-effect of this is that you have transaction fees as a percentage of the transaction size

, unlike Bitcoin and Ethereum where you can send large sums of money once in a while for a small fixed fee. If Bitcoin/Ethereum are for large, once-in-a-while transactions, Intercoin is for the opposite, the long tail of transactions. So we think it might be more ok by regulators for that reason.

1. Economics

A payment network needs to be launched on top of an existing social network. Even PayPal got a huge boost from facilitating eBay payments. Social networking companies get this. The main reason we started

Intercoin project is because we already had

a large social network and infrastructure to secure the validations. Money is a community phenomenon and benefits from network effects. And Intercoin took the unusual step of requiring every community to hold it on full reserve, thereby creating demand for Intercoin but also creating liquidity between every currency pair. It also allows us to implement our native stablecoin solution (although other stablecoin solutions are possible by changing the denominator instead of the numerator).

Basically to get from the Web to Intercoin, you would do it in three steps:

1. Replace centralized domains / DNS with a hashes / distributed hash table
2. Replace servers with a local consensus about every coin / activity
3. Crypto signatures for all actions and (optional) end to end encryption of everything

Join the discussion

So I realize that Intercoin is an alternative architecture to Ethereum, but the crypto space could definitely use more than one approach. If the above sounds interesting, I invite you to pop onto our forum and give us your feedback, help shape Intercoin. There are many things we need to refine and probably a lot of things we missed. We can benefit from a variety of views both from the tech point of view as well as legal, token-economic, etc.

Intercoin

Intercoin

Meet, talk, discuss, invest, and invite others to the Intercoin project.

Here is an example of a recent post. It has to do specifically with the consensus:

Intercoin – 16 Feb 20

Overview and Implications of Intercoin Consensus

When Intercoin begun architecting its ledger, we started with the premise that it must be fast and scalable in order to handle everyday payments. That required challenging the prevailing architecture of the day, including Bitcoin, Ethereum, Ripple,...

Hopefully now that I have made an account here I will participate more in the discussions about Ethereum 2.0 . At the moment we are just all-hands-on-deck when it comes to the ITR launch.

PS: We are launching ITR tokens on Ethereum March 1st. These are used to fund the development of Intercoin. I was mostly posting about joining the forum, but if you want to visit intercoin.org and fill out the form to set up a video chat with our team, you're more than welcome to. We are open to all developers (especially if you know Node.js / JS ES6 / Web Crypto). Everything is open source.