

*Orgens Network: An inclusive, Decentralized
Blockchain Analytics Solution for Bitcoin, Built on Cardano*

I. The Problem

From April 15th to May 18th, 2021, Bitcoin's market capitalization declined by around 53%. And during this time the entire cryptocurrency market lost around \$1.5 trillion in value.

A number of factors contributed to this crash, but two events were central to its severity:

- 1) On April 17th there was a 60% drop in the Bitcoin network's hashing power, which was quickly attributed to a coal mining disaster in Xinjiang, China, and government-imposed blackouts on data centers in that province following this disaster.
- 2) Following many negative news stories stemming from this mining accident and subsequent blackouts, Tesla CEO Elon Musk stated that Tesla would no longer be accepting bitcoin as payment until bitcoin "mining transitions to sustainable energy."

These events highlighted two alarming realities that have been voiced for years by both critics and champions of Bitcoin:

- 1) The majority of hashing power that secures and validates Bitcoin's network is controlled by just a handful of mining companies – making the network susceptible to sabotage, and leaving Bitcoin markets (and cryptocurrency markets generally) open to attack and dramatic price manipulation.
- 2) Bitcoin's legitimacy and utility as a financial asset will be limited if buyers cannot verify the provenance of specific satoshis to ensure both the provenance of satoshis, and the energy used to mine them are consistent with buyers' regulatory obligations, and ethics and sustainability objectives.

II. Background: Problems with Proposed AML, ESG and CTF Solutions

Even prior to the above events, powerful institutions and individuals were establishing the relationships and infrastructure needed to support a stratified Bitcoin market. This system would ostensibly satisfy some of investors' Environmental, Social and Governance (ESG), Anti-Money-Laundering (AML), Sanction compliance and Combating-Terrorist-Financing (CTF) objectives, but it would also erect a firewall of financial exclusion to prevent the average Bitcoin holder from utilizing their satoshis as collateral in the legacy financial system.

In this system, the only ones with access to provably "clean" bitcoin would be investors with the clout to secure purchases of newly mined bitcoin directly from miners with politically acceptable practices, and possibly also entities able to pay for the services of private, blockchain analytics firms such as Coinfirm and Elliptic. And once Bitcoin gains widespread institutional and state-level adoption, this "clean coin" of proven provenance would likely be the only kind of bitcoin accepted by institutional investors and financial institutions. It would thus be the only kind of bitcoin that would be acceptable as collateral in

doing business with mainstream financial institutions. And it would be the only kind of bitcoin that would be seen as a legitimate asset for accounting purposes.

Essentially, this would establish a system whereby Bitcoin is divided into two assets with two separate values and use cases: Depending on its holder and their proof of provenance or lack thereof, it would be seen by the legacy financial system as a “clean coin” and legitimate store of value, or a “blood coin” associated with pollution, climate crisis, and rogue and sanctioned states guilty of human rights abuses. This may seem outlandish to those of us with some knowledge of the Bitcoin network, its history and genesis: We realize Bitcoin can fundamentally change the economics of energy in an environmentally beneficial way because it introduces a highly profitable use of electricity that’s location independent. And we realize that socially, Bitcoin has the power to liberate people and even nations from the consequences of chronic, high inflation, hyperinflation and banking discrimination. But these truths won’t stop financial elites from pushing dubious narratives to cement the status of their satoshis as pristine collateral while undermining the value of most bitcoin as collateral. For example, in April of 2021, Canadian businessman Kevin O’ Leary, who is now praising Bitcoin after calling it “garbage” as recently as 2019, said the following in a CNBC interview:

“Institutions will not buy coin mined in China, coin mined in countries with sanctions on them, and all of a sudden there’s this huge demand for virgin coin with the provenance known ... And I see over the next year or two, two kinds of coin: blood coin from China; clean coin mined sustainably in countries that use hydroelectricity, not coal.”

This framing of Bitcoin by elites into two assets – clean coin and blood coin – is already, quietly constructing a system where elites can use sound money (satoshis) as collateral to borrow and spend unsound money (fiat currency) for other assets, while non-elites will eventually be forced to spend their satoshis to realize its value, thus diminishing their long-term holdings of satoshis relative to elites. In the long term, this will amass more and more of Bitcoin’s total supply into fewer and fewer hands.

Given the apparent lack of appetite for “blood coin” among the global financial elite, along with the rise of carbon credit markets and the emergence of ESG as a central corporate concern, it’s not altogether surprising Elon Musk and others took the Xinjiang blackouts as an opportunity to criticize Bitcoin’s mining network. What’s surprising is Musk (the CEO of a publicly traded company that’s a large player in carbon trading markets and a huge recipient of government green energy subsidies) didn’t address these concerns in a solutions-oriented way *before* driving up, then driving down, the price of Bitcoin with brief and enigmatic public comments. Corporates have been discussing and strategizing regarding ESG, AML and CTF concerns involved in Bitcoin asset allocation for years, so it’s curious Musk was silent on them for so long, then suddenly became such a vociferous critic.

That being the case, many holders of Bitcoin have understandable misgivings about the prospect of Elon Musk holding a prominent role in the Bitcoin Mining Council proposed by Michael Saylor. There are many unsettling questions that remain unanswered about the form this Council will take: Who will ultimately control it? How will it mesh with the plans of financial elites to divide Bitcoin into “clean” coin and “blood” coin? Will it actually diminish centralized control of Bitcoin’s mining network, or just shift some of that control from one power center to another – and from one potentially unfriendly jurisdiction to other potentially unfriendly jurisdictions?

Furthermore, as Bitcoin inevitably grows in geopolitical consequence, couldn't the decisions of a centralized body like a Bitcoin Mining Council undermine the inclusive and unfettered adoption of Bitcoin? Before the ink was even dry on El Salvador's landmark law to accept bitcoin as legal tender, current and former officials from the U.S. claimed the law could be designed to help "the criminal element" get their hands on U.S. dollars via bitcoin, and that it could end up collapsing El Salvador's economy. That being the case, if El Salvador and other nations that follow its lead are to remain unwavering in their resolutions to adopt Bitcoin, they will need to implement a blockchain analytics (AML/ESG/CTF) solution that's accessible and affordable to their citizens, and not controlled by a centralized, governing authority that could use its influence to delegitimize the growth of Bitcoin-centered economics in these countries.

Finally, many champions of Bitcoin have welcomed the reality of Chinese bitcoin miners moving their operations out of China. But while the end of Chinese mining dominance would no doubt be a healthy development for the Bitcoin network, the current exodus of Chinese mining operations doesn't appear to be the liberation from CCP influence some BTC champions are making it out to be. So long as these companies remain Chinese-owned, it's likely some operations of Chinese miners and mining pools will still coordinate some or all of their activities from within China, and in any case these companies will continue to remit taxes to the Chinese government. Given recent geopolitical tensions and China's history of human rights abuses, it's possible this fact could become more problematic for the Bitcoin network in the future. Furthermore, if Chinese mining companies operating abroad are influenced by the Chinese government, the tax base these miners generate for local jurisdictions abroad could become a leverage point by which the Chinese government could influence the politicians and politics of jurisdictions where Chinese miners are operating.

Of course, these concerns about negative influence – both influence over the Bitcoin network and negative influence stemming from it – are by no means just an issue when it comes to the Chinese government. Bitcoin's disproportionate control by any great power center needs to be carefully monitored if Bitcoin is to avoid falling prey to a central evil of all major fiat currencies – namely, that they've become a tool for enforcing hegemonic power structures and furthering the goals of corrupt institutions. And the basic reality is that well-intentioned institutions, organizations and investors who want to accumulate satoshis will want to get as clear a perspective as possible on where their Bitcoin comes from, ideally who mined it, and what entities benefited from its minting.

In sum, it's impossible to predict the particular threats that will arise for the Bitcoin mining network and markets in the future. But as "clean" Bitcoin inevitably rises to the level of pristine collateral in the eyes of institutions, the legacy financial system will have certain AML, ESG and CTF requirements Bitcoin holders will need to comply with in order to use bitcoin as collateral. And based on the AML and ESG solutions currently available and proposed, these requirements will almost certainly lead to the stratification of Bitcoin into two functionally different assets, the nature of which will in turn concentrate the holdings of Bitcoin over time, and ultimately jeopardize the decentralization and security of the Network over the long term.

For these reasons, a new blockchain analytics solution is needed that satisfies the following conditions:

- 1) It must be accessible and affordable for the majority of Bitcoin network participants, not just to a small minority of whales and the financial elite.
- 2) Its governance must be democratic, decentralized, and driven by free market forces.

- 3) In order to be adopted as an acceptable AML, ESG, and CTF standard, it must provide assurances to institutions and regulators which match or exceed assurances provided by the problematic ESG solutions being proposed, and the current AML and CTF solutions being provided by private companies like Elliptic and Coinfirm.

To satisfy these conditions, we propose the development of Orgens Network – a decentralized, smart contract-based AML, ESG and CTF solution.

III. Orgens Network's Value Proposition

Orgens Network will provide bitcoin holders and buyers with three, synergistic value propositions:

- 1) It will provide Bitcoin holders with a level of transparency into the provenance of the satoshis they own – showing them key features about noteworthy network actors they've transacted with either directly or via some degrees of separation: They'll be informed about: 1) whether they've received bitcoin directly from a miner or mining pool and the practices and physical location(s) of said miners and mining pools; 2) whether they've received bitcoin directly from centralized exchange or exchanges practicing KYC protocol(s); and 3) whether they've received bitcoin from a problem address associated with criminal activity, a sanctioned or otherwise undesirable location, or other activity that's problematic with regard to the centralization of hash power, environmental sustainability, sanction compliance, etc.
- 2) If Bitcoin holders would like to generate proof of the provenance of their satoshis, Orgens Network will provide the option to 1) generate an Orgens Non-Fungible Token (ONFT) linked to a unique, secure url displaying the Network's findings – both a detailed breakdown of the bitcoin's provenance including key information outlined above, and AML and ESG ratings based on these findings; And 2) if they choose, the protocol will "color" their bitcoin via a color aware Bitcoin wallet so their satoshis will remain easily identifiable by Orgens Protocol and linked to their ONFT (and secure url) in the future. (NOTE: If a Bitcoin holder would not like to generate proof of the provenance of their satoshis, no record of this provenance will be saved by the protocol, on IPFS, or elsewhere, as Orgens Protocol will by no means come to be utilized for involuntary blockchain surveillance.)
- 3) Lastly, Orgens Network will provide markets (both OTC and order book) to trade satoshis along with the ONFT attached to these satoshis: First, the Orgens UI will provide a decentralized escrow for OTC trades of satoshis along with the ONFTs linked to them. Second, satoshis queried by the protocol will be assigned desirability (ESG, AML, CTF) ratings based on their provenance, and these ratings will be indicated on the bitcoin's ONFT. Users whose bitcoin receives a high enough rating based on desirability of their bitcoin's provenance will have the option of unlocking special exchanges reserved for satoshis of like rating. For example, the highest exchange tier may be open only to satoshis that were derived directly from a mining operation known to use exclusively renewable energy. And another exchange tier could be accessible only to bitcoin obtained through mining by a decentralized pool member. In this way, premiums paid for bitcoin of desirable provenance would financially incentivize increasing the environmental sustainability and decentralization of the bitcoin network, while providing more liquid markets (i.e. a broader base of buyers) for "premium" satoshis.

To draw a comparison to the current, U.S. credit system, these features of Orgens Network will make it the Credit Karma of Bitcoin once Bitcoin-backed lending is embraced by regulated lending institutions.

It's possible the network effect and crowdsourcing of the Network's development could make it technically superior to centralized blockchain analytics firms and make it the protocol of choice for some lending institutions in satisfying their ESG, AML, CTF and sanction compliance. And one would think the open and auditable nature of Orgens Network protocols would be preferable to the confidential trade secrets other blockchain analytics firms rely upon. However, it's likely many regulated lending institutions seeking to provide crypto-backed loans will open accounts with centralized, blockchain analytics firms in the way they currently have accounts with credit agencies to ascertain the creditworthiness of prospective borrowers, and that Orgens Protocol will operate principally as the People's blockchain analytics protocol.

In the future landscape of cryptocurrency-backed lending, blockchain analytics leaders like Coinfirm and Elliptic will supply AML and CTF risk scores and KYT reports to lenders in the same way credit scores and reports are issued today by Transunion, Equifax and Experian. And Orgens Network will empower bitcoin holders with knowledge of their satoshis' creditworthiness, similar to how services like Credit Karma empower individuals with information pertaining to their creditworthiness. Apart from satisfying their (personal or institutional) ethical objectives, Orgens Network users will use the network 1) because they want to use their satoshis as collateral with regulated lenders in the future, or 2) sell their satoshis for a premium to others who want the option of hypothecating these satoshis in the future. For prospective borrowers, attempting to hypothecate satoshis derived from suspect transactions could result in a lender being required to make Suspicious Activity Report to law enforcement, so there's an obvious value for would-be borrowers in querying their satoshis provenance prior to pledging them as collateral to a regulated lender. And for Bitcoin buyers, the financial reason for paying a premium for satoshis on Orgens Network is obvious: These buyers are essentially paying a premium to gain some assurance their satoshis have a good "credit score" should they ever want to hypothecate them in the future.

IV. Network Architecture

The Orgens Network will be composed of two main components:

- 1) A decentralized indexing /querying layer for organizing and quickly retrieving Bitcoin transaction data and real-world data that's associated it. The size of Bitcoin's blockchain makes a query of a specific address and its interactions with other addresses of interest very costly in both time and computing power. However, by building a decentralized database of addresses of interest, and building out indexes of these addresses' interactions with other addresses in a decentralized, community-maintained ingestion service, Orgens Protocol will allow users to quickly and cost effectively trace their transactional relationships to addresses of interest, mapping the provenance of their satoshis in relation to addresses that could affect their value from an AML, ESG, and/or CTF perspective.
- 2) A consumer-facing, decentralized super-dApp enabling network users to:
 - a. query salient facts about the provenance of their satoshis and generate AML and ESG ratings for their Bitcoin address;

- b. digitally document these facts and ratings and their personal ownership of their satoshis;
- c. and exchange their satoshis via a “listing page” and decentralized OTC trading desk with escrow, or via an orderbook exchange market (most likely a CEX or KYC-capable DEX).

To explicate the structure of Orgens Network, its easiest to discuss the roles of the network’s different participants and their relationships to one another.

Users:

Users connect to the Orgens Network, which must be able to communicate with wallets that support both Bitcoin and the layer one (smart contract) blockchain Orgens Network is built on. Once connected, users are given the option to query Orgens Network’s indexes of Bitcoin transaction history to inform them about the provenance of their satoshis (in exchange for a query fee).

When a query is conducted by Orgens Network, a secure, IPFS-based URL is generated which displays salient facts about the user’s satoshis: which Addresses of Interest (AOIs), the user has interacted with, and when.

An “Address of Interest” is one which has been identified by the Orgens Network as connected to an Entity of Interest (EOI). And EOIs may be Bitcoin miners, mining pools, mining pool members, centralized exchanges with mandatory AML and KYC policies, Bitcoin mixers, anonymity wallets, entities known to have utilized Bitcoin in the commission of crimes, or any other network participants whose transactions with the consumers of Orgens Network may affect the value of the user’s satoshis – either positively or negatively.

In addition to displaying some salient facts about a user’s satoshis, their secure URL will display an AML ESG rating (or ratings) of the satoshis based on the Orgens protocol’s analysis of the user’s transaction history from an AML and ESG perspective. Based on this rating and the displayed transaction history, a user may choose to do one or more of the following.

- Enable a decentralized identification protocol integrated with Orgens Protocol (e.g. Atala Prism) to enable their secure URL display that their satoshis in fact belong to them personally.
- Generate an Orgens Non-Fungible Token (ONFT) establishing ownership of the secure URL featuring the user’s transaction history.
- Enable a Bitcoin color-aware wallet to mark their satoshis for easy identification by the Orgens Protocol in the future, even if their satoshis have been exchanged or sent to another Bitcoin address (so long as no mixing and layering takes place to effectively remove the “color” from their satoshis).
- Exchange their satoshis (and their associated ONFT) via the Orgens Network’s non-custodial, escrowed over-the-counter exchange. This OTC exchange may feature a “listing page” where sellers can list deals (satoshis + linked ONFT for spot price + premium), and potential buyers can fulfill the terms of listings to execute OTC trades.

- Exchange their satoshis on an Orgens Protocol Exchange market. These markets will be broken into tiers and will be accessible based on the AML and ESG ratings presented by the user, which will be evidenced by their ONFT (and BTC color).
- Alternatively, a user may not currently hold satoshis whose provenance they want to query with the Orgens Network, but instead want to purchase satoshis that have already been queried by the Orgens Protocol and received acceptably high desirability ratings. Such users could be smaller companies or NGOs without access to currently available, blockchain analytics services, a customer of a participating financial institution, or any individual that may want to use satoshis as collateral with a participating financial institution in the future.

Sentinels:

Sentinels compile real-world data and documentation linking EOIs and their AOIs. We'll term these presentations of evidence "packages of proof" (PoPs). Additionally, in most cases these PoPs will present documentation showing that a transactional relationship to the EOI could affect a Bitcoin address' AML and/or ESG rating. For example, a sentinel may post evidence of the EOI's energy usage in mining Bitcoin, or its connection to a money laundering scheme to present the EOI's relevance to Orgens Network's AML/ESG rating protocol.

After compiling what they believe to be a compelling PoP, a sentinel posts this PoP of a specific AOI on the network indexing bulletin along with an amount of staked OR token (the native token of the Orgens Network).

For this service, the sentinel will be awarded a portion of any query fees when 1) a query discovers the AOI posted by the Sentinel in one or more indexes, and 2) this AOI has a material effect on the user's AML/ESG rating.

The share of a Sentinel's fees collected for a query will depend in part on the amount of OR the Sentinel has staked to back the validity of their PoP, as well as the amount of OR staked by curators to this same PoP. (The network role of curators will be discussed below.)

The other main factor in determining a Sentinel's share of fees for a given query will be the primacy of the posted AOI and PoP in determining the AML/ESG ratings of the bitcoin whose provenance is being queried. Put differently, the Orgens Network will algorithmically rate the (AML and ESG) desirability of an end user's satoshis based on the user's transaction history with a number of AOIs. These rating algorithms will weight a specific AOI depending upon time signature(s) and other transaction metrics of the user's transaction(s) with this AOI. And the share of fees rewarded to a sentinel for posting this AOI (and its associated PoP), will be proportional to this rank of importance given by the algorithms.

To clarify by way of example, let's imagine a query that shows an end user's satoshis were transferred to the user's address directly from the address of a mining pool member, and that previously this mining pool member's address received an equivalent amount of satoshis incrementally from an address linked to said mining pool. In this case, the addresses of both the mining pool member and mining pool would be the preponderant factors in the AML/ESG ratings of the end user's satoshis, and the sentinel(s) who posted these two addresses would be rewarded a share of the query fee proportionate to the

significance of these addresses in determining the AML/ESG ratings. By contrast, consider another end user whose satoshis can also be traced back to a coinbase rewarded to this same mining pool. But in this case, the end user did not receive their satoshis directly from a mining pool member, but received them by way of numerous other transactions, including transactions linked to an address that has been identified by the Oorgens Network as having utilized Bitcoin in a money laundering scheme. In this second example, the address associated with the money laundering scheme would be of primary importance in determining the AML rating of the end user's bitcoin, so the sentinel who posted this AOI and PoP associated with the money laundering scheme would receive more of the query fee relative to the sentinels who posted addresses and PoPs linking these satoshis to the mining pool.

This last aspect of the query fee sharing scheme is important for incentivizing sentinels to post AOIs and PoPs associated with "undesirable" entities (i.e. "tainting" EOIs). Because the Oorgens Network will feature exchanges where Bitcoin holders like mining pool members will be able to sell their satoshis at a premium if they're rated at an AML and ESG premium by the network, mining pool members, pool operators, and any other network participant with documentation evidencing connection to a "desirable" or "clean" Bitcoin address have financial incentive to post that documentation as a sentinel, or provide that documentation for someone else to post. However, the query fee sharing scheme must also incentivize sentinels to identify and post tainting counterparties and their AOIs if the indexing protocol is to have true value as an AML/ESG solution. Doing this will cost sentinels significant time and resources, as they'll need to rely on extensive research, Bitcoin analysis software, education and training, along with documentation from government regulators, centralized exchanges, law enforcement, etc. That said, it's essential that the network fees – which will be comprised of query fees, NFT and Colored Coin minting fees, and exchange fees – are shared in a way that incentivizes the exhaustive indexing of as many desirable and undesirable AOIs as possible. Of course, eventually this fee structure will be determined by the Oorgens Network DOA (which will be further described below).

A final note about sentinel incentives: Because query fees collected by sentinels will depend first and foremost on AOIs being transactionally related to end users' Bitcoin addresses, sentinels will be incentivized to post AOIs and POPs with the greatest network reach – those AOIs that most frequently transact the largest amount of satoshis which reach the greatest numbers of network participants.

Indexers:

Indexers are the node operators on the Oorgens Network. They're principally responsible for four main functions:

- 1) Translating data and documentation from PoPs into uniform data points that feed into Oorgens Network's AML and ESG ratings algorithms when users query the network.
- 2) Implement upgrades to transaction mapping, query and rating protocols adopted by the Oorgens Network DAO.
- 3) Dedicate computer power to running the Oorgens Network protocol, which uses a set of APIs to build out "transaction trees" of transactional relationships between AOIs identified by sentinels, and other Bitcoin addresses. The initial set of APIs making up this protocol will be developed by Oorgens Network's core development team. And APIs will be added to the protocol or improved through a democratic

process of protocol improvement proposals, voting on these proposals, and awarding grants for the implementation of ratified proposals. This grant proposal process will

4) Dedicating computer power to run queries on the Orgiens Network, which .

5) Running a node of the Bitcoin blockchain (or obtaining updated Bitcoin data from a provider of an endpoint provider (i.e. Bitcoin node as a service provider) such as Blockdaemon so that Orgens Network data can continually be made current.

Curators:

Curators stake OR to a posted PoP to signal to indexers the relative importance of mapping and charting transactions stemming from this PoP's AOI. In exchange for this staked OR, curators receive a portion of query (and possibly NFT and colored coin minting) fees when 1) the query discovers the AOI posted by the Sentinel in one or more indexes, and 2) this AOI has a material effect on the user's AML/ESG rating. The fees sharing scheme awarded to curators staking to AOIs will mirror the fee sharing schemes for Sentinels, and via a bonding curve, disproportionately reward curators who post earlier to PoPs rather than later. Because the role of a curator is commensurate with an investor speculating on the importance and future utilization of an AOI within the Network, this bonding curve could potentially be designed in such a way that curators staking OR to AOIs that don't end up being queried frequently would have a negative return of OR. This would incentivize research into the importance of specific AOIs, and disincentivize frivolous staking of OR by curators, which would create a false signal and possible misallocation of indexer/network resources.

Challengers:

Challengers challenge the accuracy of data provided and/or ratings assigned by sentinels and indexers. Their claims are reviewed by arbitrators, and if their challenges stand, they earn slashing fees from the indexer or sentinel whose data or conclusions they challenged.

In order to prevent frivolous claims from being made on the Network, challengers will need to stake an arbitration fee in order to make a challenge. Following arbitration, if the challenge is upheld, the challenger will receive slashed stake from the indexer or sentinel who posted inaccurate information to the Network, and the challenger will get back their arbitration fee. However, if their claim is denied by the arbitrators, the challenger will not receive any slashed stake or receive back their arbitration fee.

Arbitrators:

Arbitrators review claims made by challengers and make decisions regarding their challenges. Initially, challenges will need to be reviewed by a committee appointed by Orgens Network's development team, but as soon as possible the arbitration of challenges will be integrated into the Network DOA's democratic decision-making process. Every 6 – 8 weeks, decisions will be rendered by the DOA on outstanding challenges, in the same voting rounds that address proposed protocol upgrades and grant proposals.

Voters:

Network participants will have voting power on Network Proposals proportionate to the amount of OR they have staked on the network (as Sentinels, Indexers, Curators, or Delegators). These proposals will be comprised of improvement proposals on Network protocols and modifications of fee sharing agreements, along with claims made by challengers.

V. Candidates for Layer One Blockchains**Ethereum & The Graph?:**

Those familiar with The Graph Protocol will have noticed much of the proposed network architecture for Orgens Network's indexing protocol is taken from the design of The Graph Protocol. The reason for this is obvious to those familiar with The Graph: The Graph is the only working, decentralized indexing protocol, and thus provides a good model for the staking and game theory dynamics needed to build and maintain this kind of protocol.

Given that the core protocol of Orgens Network closely mirrors that of The Graph, we should first consider whether the indexing protocol of Orgens Network could be developed as a subgraph or series of subgraphs on The Graph. Graph Community members seem to be in agreement that it's a matter of time before The Graph supports indexing of the Bitcoin blockchain. And while high, fluctuating, and indeterminate gas fees on Ethereum would make Orgens Protocol unusable on the present state of Ethereum, if Ethereum 2.0 is rolled out prior to Orgens Network's launch, network fees could likely be brought down enough to make an Orgens Network's on-chain components feasible on Ethereum.

That being said, the APIs to be utilized in Orgens Network's indexing protocol are very different from APIs currently being created on The Graph's subgraphs, so more investigation would need to be done into whether it would be technically feasible to locate the Network's indexing protocol on The Graph (assuming the Bitcoin network is even supported in time for Orgens Network development). For example, how would the system of Sentinels and Curators be dovetailed with The Graph's internal economy of indexers, curators and delegators? And even if these design issues were overcome, outsourcing the querying and delegation to The Graph network and its native GRT token would eliminate most of use cases of the OR token, could dramatically affect the project's network effect and also lower the bar considerably for competing projects who could utilize Orgens Network subgraphs, linking them to their own front-end dApps to mimic Orgens Protocol. Finally, there are a number of features of Ethereum which may make it less than ideal for Orgens Protocol, relative to other, emergent smart contract blockchains, notwithstanding Ethereum's first mover advantage.

Cardano:

For many reasons, Cardano is probably the optimal layer one blockchain on which to build Orgens Network. Of course, this would entail building the Network in a programming language that very few developers are familiar with. However, if this challenge of discovering sufficient technical talent is overcome, Plutus and Cardano offer a number of advantages over Ethereum and Solidity:

1. Plutus is a functional programming language which is more provable and offers a higher level of assurance than imperative languages like Solidity. Functional languages are not without their downsides: they can be very difficult to build with, even for experienced developers. However, once Plutus is thoroughly tested and attains a sizable network effect with developers, the advantages of building with higher assurance code will likely outstrip other considerations and draw a disproportionate amount of decentralized finance development to Cardano.
2. Plutus is essentially a smart-contract-specific library based on the programming language Haskell. And Haskell and functional languages like it are the languages of choice for software development in much of the traditional finance world. This, combined with the fact that Plutus is highly focused on mathematical and computational programming, and the large amount of liquidity in the Cardano Ecosystem, will likely make Cardano one of the top layer one blockchains for decentralized finance, and lend more accessibility to Orgens Protocol than can be found on most other POS protocols.
3. Input Output Global and the Cardano Foundation – the principle, founding entities of Cardano – have the most robust commercial initiatives for pursuing relationships in the developing world. Because Orgens Network's first and most critical relationships outside the Orgens Protocol community will be with financial institutions in emerging markets, the commercial inroads and government level adoption Cardano is working on may bolster the efforts of Orgens Network.
4. A number of factors make Cardano the optimal ecosystem on which to raise money for Orgens Protocol's development:
 - a. Project Catalyst offers a way to not only vet interest in the project at little cost. It also provides a means of obtaining early seed funding without becoming heavily indebted to or beholden to a small group of early investors who could negatively affect the project's development through a short-sighted fixation on ROI. Furthermore, Project Catalyst is a great platform on which to crowd-source ideas and develop enthusiasm in the project among the future Orgens Network community from the project's earliest stages.
 - b. Projects like Sundae Swap are pioneering the method of using a Stake Pool Offering (SPO) as means of raising development funds, and there is a higher percentage of liquidity staked on Cardano than any other ecosystem.
 - c. The low number of defi projects currently building on Cardano (relative to ecosystems like Ethereum, Solana, Polygon, etc.) results in a great deal of liquidity looking for viable, lower cap, higher growth potential projects in the Cardano ecosystem.
5. Cardano leadership has stated their intent to make available their developments of governance systems in Voltaire to projects built on the Cardano ecosystem, and this could reduce the cost and complexity of developing Orgens Network in a truly decentralized and democratic way.

VI. Tokenomics

As the work token of the Orgens Protocol, the OR token will power the internal economy of Orgens Protocol in the following ways:

1. Users will use it to pay transaction fees for ...
 - Ordering queries of their satoshis
 - Minting ONFTs and/or Colored coins
 - Exchanging satoshis (and ONFTs) on Orgens Network exchanges
2. Sentinels will be required to stake OR along with AOs they post, and will earn a portion of Network transaction fees in part proportionate to the amount of OR they stake.
3. Indexers will be required to stake OR along with AOs they post, and will earn a portion of Network transaction fees in part proportionate to the amount of OR they stake.
4. Curators will be required to stake OR along with AOs they post, and will earn a portion of Network transaction fees in part proportionate to the amount of OR they stake.
5. Challengers will need to stake an arbitration fee in order to make a challenge. Following arbitration, if the challenge is upheld, the challenger will receive slashed stake from the indexer or sentinel (and curators) who posted inaccurate information to the Network, and the challenger will get back their arbitration fee. However, if their claim is denied by the arbitrators, the challenger will not receive any slashed stake or receive back their arbitration fee.
6. Voters will earn a small percentage of OR they have staked within the network for voting on challenges. A small percentage of transaction fees will go into a treasury that funds both winning grant proposals and voter rewards for voters who vote on challenges and proposals.

VII Potential Future Developments

Support of Additional Blockchains:

The most obvious, eventual outgrowth of this project would be to develop support for other blockchains beyond Bitcoin, as The Graph has done with its indexing protocol. But there are several reasons for optimizing the indexing protocol as much as possible for Bitcoin before moving on to other blockchains:

1. Bitcoin's maintains a high level of market cap dominance and has a special, perceived standing as collateral in the eyes of most investors.
2. Most institutional interest in cryptocurrency at this point is focused on Bitcoin.
3. Bitcoin will soon be the only dominant proof-of-work protocol (as Ethereum is transitioning to proof-of-stake). And although PoW has its advantages over other consensus mechanisms, its relatively high electricity usage makes Bitcoin a lightning rod for ESG concerns. Based on recent trends and assertions by the likes of SEC Chairman Gary Gensler, it appears that in the emerging, financial regulatory order ESG concerns may be an even bigger issue than AML concerns, so Orgens Protocol has a kind of double application for Bitcoin relative to its application for other, large blockchains.

That being said, if Orgens Protocol is designed similarly to the way (I've been told) The Graph is designed, the indexing part of the protocol will be built off-chain, with only the transactional components of the network – i.e. staking, depositing, and exchanging coins and tokens – being built on-chain. So it's not as if the entire network would have to be rebuilt to support an additional blockchain.

And eventually developing a decentralized, AML and CTF solution for Cardano could have definite benefits for the network: It could provide a competitive edge for the institutional adoption of Cardano relative to other smart contract blockchains. And aside from the potentials of quantum computing, probably the biggest, existential threat to large cap PoS blockchains going forward would be state-level sabotage through the monopolization of validator control. \$100 billion is literally nothing for a central bank to generate to stage a 51% attack, so a tool that could track real (as opposed to apparent) decentralization (via analyzing address associations) could be of great value to Cardano and other blockchains in the future. Granted, it's hard to imagine a central bank flagrantly attacking a cryptocurrency or the cryptocurrency industry, but we are about to enter an era of central bank digital currencies, and just a few months ago few of us could've imagined the CCP would shut down China's soon-to-be trillion dollar BTC mining industry, and the U.S. congress would legally classify stake pool operators and Bitcoin miners as crypto brokers for tax reporting purposes.

Collateral Custody:

Because a central use case of Orgens Protocol will be to empower BTC holders to hypothecate their BTC as collateral for loans from traditional financial institutions, this begs the question: Who will custody this collateral? The obvious answer would be the financial institution servicing the loan. However, if financial institutions express reticence at this prospect, an alternative could be to develop a third leg of Orgens Protocol, whereby:

- 1) Lenders could mint a lien NFT to facilitate the decentralized custody of collateral on Orgens Protocol.
- 2) Borrowers could lock their satoshis as collateral in a special wallet by depositing it along with an NFT that is linked to a url that displays the Loan Agreement, including terms of the loan. From the time a borrower locks in their collateral, to the time the loan terms are fulfilled or the loan is canceled and the lien is released, only the lender would be able to withdraw the collateral with their private keys.
- 3) Upon fulfillment of the loan terms, the lender would release the lien with their private keys. At this point the borrower could withdraw the BTC using their own private keys. Essentially, this dApp would work like a multi-sig wallet where one party (the lender) is required to sign first before the other party (the borrower) signs, and the wallet contract is initiated by the borrower depositing an NFT (the Loan Agreement) along with a corresponding amount of satoshis specified in the NFT.

While the prospect of collecting more fees for the custody of loan collateral may appear attractive, this kind of application should be approached with extreme caution. Apart from regulatory complications that would arise in custodying bank collateral, storing large volumes of other people's crypto is always risky and has been the downfall of many protocols and exchanges with solid teams behind them. That being the case, in its system architecture Orgens Network should investigate novel alternatives to staking pools developed by projects like Hex.com (which feature minting and burning mechanisms in their staking systems to eliminate the need for large pools of tokens being held in network contracts) to

see whether such approaches might offer enhanced security without unacceptable downsides. And if financial institutions do not have the means to custody loan collateral, it would probably make most sense to partner with a project or company whose main focus is crypto custody, and it definitely makes sense to identify a project or company prior to approaching financial institutions in case this is a concern and something they need time to work on from a regulatory and share-holder perspective.

VIII Conclusion

The inescapable complexity of Orgens Network will no doubt make its development a difficult and lengthy undertaking. However, if the success of The Graph's distributed approach to indexing-protocol-as-a-service is any indication, it's very possible that Orgens Protocol could grow to be as good or better than centralized, blockchain analytics services. And if the Network can attain a level of functionality comparable to blockchain analytics services now available to large institutional investors and billionaires, and can do so at a cost that makes it accessible to Bitcoin holders with relatively small holdings, its value to the Bitcoin community and the global economy in general will be immense, especially in Emerging Markets (EMs):

EMs suffer from chronically unstable access to USD and other major fiat liquidity, and EM liquidity tends to dry up during global, economic downturns, leaving EMs with no option but to print high levels of currency to keep their economies afloat, debasing their currencies relative to USD denominated debts that must continually be repaid to keep their economies from collapsing. This situation makes basing a growing portion of economic activity on Bitcoin (a sound money and store of value) and less on USD denominated debts an incredibly attractive proposition for EMs. However, EMs will need to maintain access to the global banking system and fiat liquidity. If forced to choose between the USD on one hand, and Bitcoin on the other, EMs will necessarily choose the former, without question.

This means EM financial institutions that want to base lending on Bitcoin will need solutions in place to satisfy the global banking system's Bitcoin AML, ESG and CTF requirements. And if Orgens Network is able to achieve this by providing superior, continually upgrading analytics that are widely accessible, it will have a solution EM financial institutions will be hugely motivated to adopt and promote – a solution that could one day unlock hundreds of billions or even trillions of dollars in lending capacity, while incentivizing more clean energy mining, more decentralization and less illicit activity on the Bitcoin network – all while also bringing a great and unique value proposition to Cardano.

To discuss this project further, please don't hesitate to reach out to –

Anthony Capitan
Brerrabbit3@protonmail.com
1(510)833-5027