CROWN STERLING

ORION

EMPOWERING DECENTRALIZED COMMUNITIES & DATA SOVEREIGNTY

Built on quantum security, freedom, assembly, and choice.

Litepaper

March 2024

Notice

NOTHING IN THIS WHITEPAPER CONSTITUTES LEGAL, FINANCIAL, BUSINESS, OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISER BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER CROWN STERLING LIMITED LLC ("CROWN STERLING"), ANY OF THE PROJECT TEAM MEMBERS WHO HAVE WORKED ON THE ORION MESSENGER PROJECT IN ANY WAY WHATSOEVER (THE "CROWN STERLING TEAM") NOR ANY THIRD PARTY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS LITEPAPER, MATERIALS PRODUCED BY CROWN STERLING, OR ACCESSING THE WEBSITES AT [HTTPS://WWW.CROWNSTERLING.IO/] OR [HTTPS://WWW.ORIONMESSENGER.IO] OR ANY OTHER MATERIALS PUBLISHED BY CROWN STERLING.

Crown Sterling and the Crown Sterling team do not and do not purport to make, and hereby disclaim, all representations, warranties or undertakings to any entity or person. All statements contained in this litepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by Crown Sterling and/or the Crown Sterling team may constitute forward looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward looking statements. These forward-looking statements are applicable only as of the date of this litepaper and Crown Sterling and the Crown Sterling team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date. You understand that the Orion Messenger Project involves significant risks, including but not limited to, the risk that (i) the technology associated with the Orion Messenger Project may not function as intended, and (ii) the Orion Messenger Project may fail to attract interest or adoption, either from key stakeholders or the broader community.

Preamble

Personal Data Sovereignty & Data Bill of Rights

Personal Data Sovereignty refers to the concept that individuals should have full control over their personal data, including how it is collected, used, and shared. To understand its importance, picture this: you are a customer of a popular social media platform, and you regularly share personal information about yourself, including your interests, location, and online behavior. At some point, you start to notice that this platform is using your data in ways that you feel you did not consent to, such as selling it to advertisers or using it to manipulate your online experience. Sound familiar?

This is where Personal Data Sovereignty comes in – it empowers individuals to take ownership of their data and protect their privacy. And while privacy can be challenging to protect, original ownership is something that can be protected as an intrinsic right, which is why we established the Data Bill of Rights on the Genesis Block of our chain:

*"We believe that digital assets are the **intangible personal property of the original producer and therefore are protected** by the United States Constitution, including the 4th and 5th Amendments, and the United Nations Universal Declaration of Human Rights, including Articles 12 and 17."*

Freedom of speech as the basis of the Bill of Rights seems to have been an intentional declaration by the Founding Fathers of the United States. We believe freedom of speech to be a fundamental tenet of any successful governance and democratic system, which is why the First Amendment of our Data Bill of Rights declares:

*"**Freedom of speech**, in all of its forms, is a **foundational pillar of human liberty**; and therefore, an **unequivocal human right** that must be upheld regardless of race, color, gender, religion or national origin."*

You don't have to be an "influencer" or content creator to be an original producer of data. You're creating data every day when you do just about anything on your digital devices, and in some cases just by having the device near you when you are speaking. Data has become the world's most valuable asset. You might think, if we're creating more data every day, how could its value continue to increase if there is no scarcity associated with it? It is the control of data that generates its value. Our goal is to decentralize that control and put it back in the hands of original producers. Controlling your data today is controlling your identity, and perhaps even your behavior, tomorrow. We believe that the key to sovereignty is maintaining your proof of self through encryption and blockchain technology.

The Quantum Threat

While there is a constant debate about quantum computing, the ifs have now become whens. In May of 2022, the White House issued a memorandum requiring agencies to inventory their IT systems' cryptography and set milestones accordingly, “the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography with the goal of mitigating as much of the quantum risk as is feasible by 2035.” That decision and announcement says a lot about the vulnerability of today’s encryption.

It’s also worth noting since the National Institute of Standards and Technology (NIST) announced the selection of four encryption algorithms to become part of the post-quantum cryptographic standard in July 2022, one by one, these algorithms are being cracked by teams around the world. Everyone is a runner in the race to post-quantum cryptography, as the very real risk coined “harvest now, decrypt later,” represents the threat that a bad actor maintains a copy of your [encrypted] data until quantum computing power becomes available, and then it’s time to harvest. While the exact when remains unknown, it’s clear that the solution is beyond any number-theory based encryption protocols, which are vulnerable to brute force attack as computational capabilities advance.

There is a solution – and it is geometric. Crown Sterling’s journey began with Founder Robert Edward Grant’s discovery of a prime number prediction pattern published alongside colleague Talal Ghannam, PhD in 2018. This led Grant to take a closer look into the risk of quantum computing, as well as the geometric approaches to face it head on. This paper was just the beginning of his work exploring information-theory solutions related to challenges like cryptography and compression.

Orion’s Inception

Blockchain answers a fundamental question, “what is value?” and it has proven value is not simply fiat currency that a government says is worth value. It can be many things. Value is found in the content and data of an original producer. So the question remains, how to protect that value?

An original producer cannot maintain Data Sovereignty without sufficient protection, and in the digital realm, the solution is encryption. Encryption underlies the very ability to extract value from original data. Not only do we believe that this encryption must be quantum-secure, but we’ve also spent the last five years researching and developing its cryptographic protocols and integrating it into solutions, including the Orion™ Messenger.

Our “Founding Father,” was inspired to create Orion after a series of personal experiences as a content creator himself. One day, he was shadow-banned on a popular social media platform after a bot mistakenly flagged a post featuring “Isis” (as in Isis and Osiris, ancient Egyptian deities) erroneously flagging it as a reference to the “Isis” terrorist group. This error caused a steep decline in his account activity and exposure, causing him to reflect on the possibility of being deplatformed. He realized how his social media accounts serve as a chronological archive and

storage mechanism for thousands of posts and how easily it could all be erased by a third party. This led him to consider what kind of platform and features he would want: a decentralized communication platform with quantum-secure encryption, free from shadow-banning and data harvesting - a platform where sovereign communities can thrive.

Most commonly used private and group messaging apps, at best, rely on the same route encryption protocols. Most large group chats specifically, are not even encrypted. Furthermore, many of these companies are the world's leading data miners. Siphoning, consolidating, and monetizing their user's data for corporate gain.

The looming threat of quantum computing creates an immediate need for a new and stronger encryption protocol built on a platform that values user rights and privacy. Combined with the slow erosion of our most fundamental freedoms of speech, assembly, and ownership, discerning, rights and privacy-oriented community leaders need Orion.

Orion Commitment

Before our era, knowledge was guarded by the privileged few who wielded it to maintain an iron grasp on positions of influence. The inception of the internet (Web 1.0) represented a commendable endeavor to establish a more equitable world by democratizing access to a vast array of information. This provided opportunities for individuals to attain considerable influence. Web 2.0, however, was a corruption: mega platforms took ownership of the data and used it to exert power and control, ultimately monetizing your data.

We are committed to the digital transformation represented by Web3, which embodies key principles of data sovereignty and the protection of our fundamental and inalienable rights. Data belongs solely to its creator, and they alone maintain the right to its value. Decentralization, security, and blockchain technologies denote the humble beginnings of Web3. These are the critical means to end the era of Web 1.0. A world in which the parasitic, ad-driven, personal data-mining scheme of Web 2.0 is shunned by the people. Instead, data represents knowledge, and thus power, to be democratized and harnessed by the human collective.

Proof vs Trust

Though information technology is a branch of computer science, the players dominating the industry have not earned their place through the meritocratic process of the scientific method. Instead, the hard science aspects underlying the industry have been overshadowed by political and financial interests. The largest software providers on Earth did not rise to the top by creating battle hardened software that has not been properly and publicly peer-reviewed. Such a process would have weeded out those whose intentions were not aligned with their user base. To our detriment, the opposite has occurred. Through efficient promotional campaigns, monopolistic tendencies and other strategies designed to maintain market share, the winners of Web 2.0 enjoy a high degree of trust from their users despite demonstrable evidence of their adverse actions and interests.

We’re building a trustless system. One in which your data is provably encrypted, provably decentralized and definitively your own. The collective will be our auditors, the decentralized system will be our safety, and encryption our security.

We recognize that building and launching three distinct products - Bellatrix, Betelgeuse, and Orion's Belt - will take time. Our philosophy and core values demand our commitment to precision in the development of next-generation technology. We invite you to join us on this journey.

Data Exploitation

The term "Cloud" evokes a gentle and secure environment. However, this perception is misleading. In the past twenty years, the swift expansion of highly sophisticated social media platforms and user-friendly cloud storage systems has engendered a collective lack of awareness regarding the hazards associated with entrusting our entire online activity to cloud-based infrastructures. Before we knew it, it was too late. Most of humanity became—in the best case—addicted and—in the worst case—financially and professionally dependent upon low cost and free cloud based services. With the personal data of millions of users, platforms can transfer, process, upregulate, modify and sell this data as they see fit. There’s nothing free or freeing about this scheme. We’ve all been deluded and charmed by the concept of free but the painful truth is that if you aren’t paying for a product, you are the product. It doesn’t stop there, as advancements in Big Data and artificial intelligence capitalizes on the reduced hardware costs attributable to Moore's Law, the decision to employ algorithmic analysis of this data has become a straightforward technical choice. Consequently, these algorithms have managed to capture our attention and manipulate our cognitive processes, transforming us into predictable consumers of superfluous products and sensational content.

Within the span of a few short years, algorithms leveraged our data to influence elections, predict stock prices and influence the behavior of billions of people. The technologies employing these algorithms then competed to be the first private entities with Trillion-dollar market caps. As this situation reached global systemic proportions, no laws existed to sufficiently regulate and control these entities.

Security

The growth of a centralized software solution scales linearly with the internal list of known, unresolved security vulnerabilities. As platforms are closed and employees contractually obligated to protect company secrets and incentivized through equity and option plans to protect the company's future, these vulnerabilities remain unaddressed until it is too late. Cyberattacks. Data leaks. And yet, we continue to willingly hand our private data over to these centralized platforms for lack of a better choice. The fact is that our privacy is not their priority.

Additionally, well known security issues currently threaten entire industries, yet are difficult to rectify without rebuilding critical infrastructure from the ground up. The scientific research into

cryptographic algorithms has led to the creation of new protocols, however deploying these new protocols at a global scale comes with huge costs for tech giants. Due to this, the financial interests drive the narrative and security issues are misrepresented or downplayed. After all, the entire system is based on encouraging user adoption through blind trust.

Our team looks to take a different approach. We have implemented modern security best practices while focusing our research and development efforts toward building flexible solutions that can quickly incorporate tomorrow's tools.

Orion

Orion aims to solve each of these pervasive issues one at a time, systematically and thoughtfully implementing the software as three distinct phases:

1. Bellatrix: Orion's revolutionary messenger application, supporting [autonomous/sovereign] communities through quantum-secure end-to-end encrypted messaging.
2. Betelgeuse: Orion's decentralized storage solution facilitating data sovereignty for all.
3. Orion's Belt: Orion's migration onto a post-quantum blockchain optimized for decentralized value transmission into the quantum age.

ORION

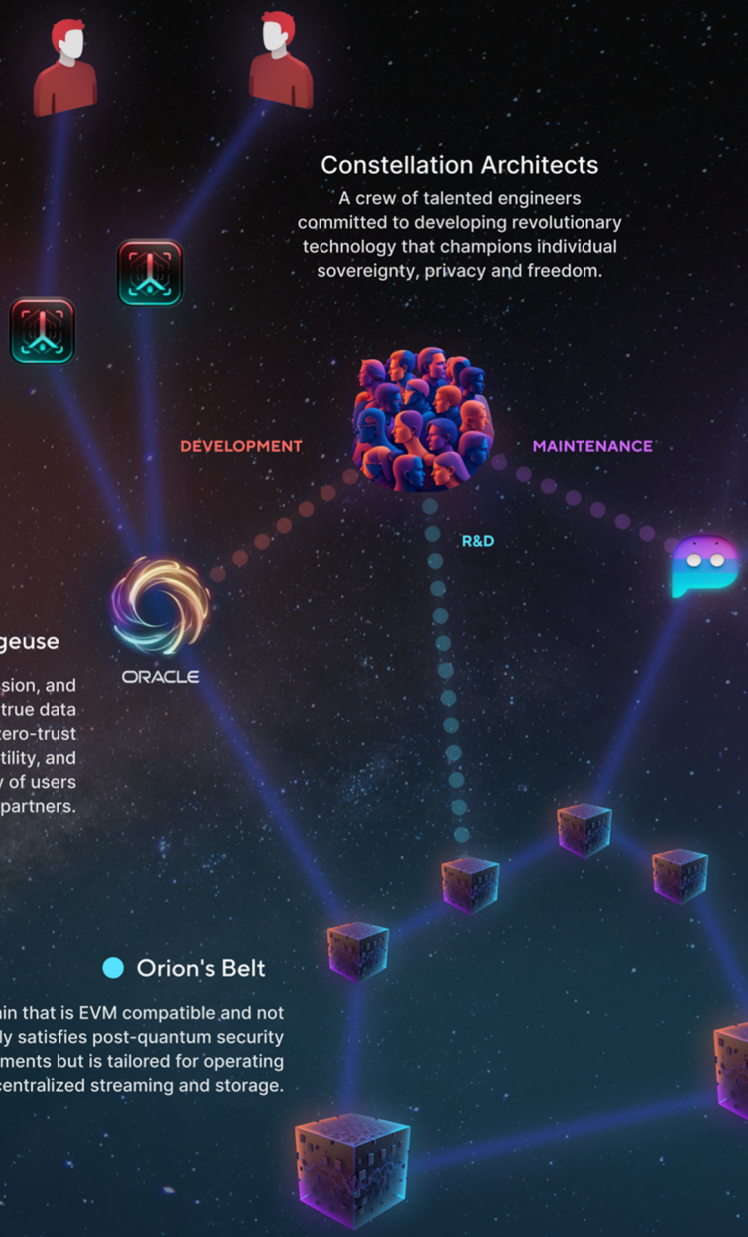
We are building a trustless system.

One in which your data is provably encrypted, provably decentralized, and distinctly your own. Orion gives you power over your data.

Ecosystem

Limitless expansion is key for successful decentralized data streaming and storage initiatives. As more applications are developed and integrated, the ecosystem thrives as a hub for fostering collaborative learning and growth, driving greater value for all involved.

Thus, another objective of our mission is to empower organizations to effortlessly scale their projects and delivery by using Orion's solutions to address both common and challenging product needs.



Constellation Architects

A crew of talented engineers committed to developing revolutionary technology that champions individual sovereignty, privacy and freedom.

Community

Community is the heart and soul of Orion. That's why we're dedicated to educating the rapidly growing number of people who value security, privacy, and personal data sovereignty.

We know that ease of use is key to keeping our community engaged, which is why we've designed Orion to be as user-friendly as possible. With quantum-secure end-to-end encryption, members can interact with each other just like any other messenger app, but with unparalleled security.

For creators, we've developed enhanced engagement and moderation tools to help them grow and nurture their fan base, making it easier than ever to build a thriving online sovereign community.

We understand the importance of building a platform and tools that are developer-friendly. We're committed to building a robust, accessible, and scalable platform that can be easily integrated into other inspiring projects.

Bellatrix

Is an easy-to-use social messaging platform that incorporates end-to-end quantum-secure encryption.

Betelgeuse

A decentralized data storage, compression, and streaming solution that ensures true data sovereignty. Its chain-agnostic and zero-trust design delivers exceptional services, utility, and unrivaled security for our community of users and our growing network of partners.

Orion's Belt

A blockchain that is EVM compatible and not only satisfies post-quantum security requirements but is tailored for operating decentralized streaming and storage.

Network

Partners can seamlessly run their custom apps on our EVM-compatible network and fully utilize our next-generation quantum-secure encryption. When launched, our validator network and enrollment will be open to all. Furthermore, we anticipate that as the network matures, it will grow significantly and, ultimately, rely heavily on outside nodes.

First Epoch - Bellatrix

The first stage in achieving secure personal data sovereignty is Bellatrix, an end-to-end encrypted chat application, protected with post-quantum algorithms and integrated with Ethereum-compatible wallets. The app supports the creation of sovereign communities and gives managers the necessary tools to administer their community as they see fit. Core efforts within this stage center around encryption and, secondarily, creating a modern and customizable interface with a smooth user experience–whether through desktop or mobile devices.

Quantum-Secure Encryption

With privacy concerns on the rise, software solutions that provide heightened levels of security are gaining significant traction as individuals seek to safeguard their personal information.

As part of our approach, we have created a flexible and agile software architecture that allows us to easily switch between encryption protocols. This gives us a unique edge, as our modern coding practices allow us a degree of flexibility that is not available to legacy solutions, which have already committed to a direction, before defining the correct architecture. We are focused on delivering the application to an educated group of users that understand the importance of security and have designed the entire solution for this purpose. Additionally, this allows us to stay up to date with all advances in cryptography, and to outmaneuver new threats as they arise. As part of the initial phase of the project, we have invested significant time and resources researching, testing and integrating modern post-quantum algorithms, including Kyber, Dilithium, NTRU, XMSS, OTP and QuEME, an iteration on AES EME which increases its quantum security.

IT departments worldwide are striving to integrate post-quantum encryption into their infrastructure; however, they still have a long and expensive way to go. We, on the other hand, strive to incorporate encryption that is future-proofed and not merely a combination of RSA or Ed25519 for asymmetric cryptography and AES for symmetric cryptography. To do this, our encryption leverages the in-house knowledge of cryptography specialists and a dedicated development team focused on the low-level details of quantum-secure best practices, alongside a robust IP portfolio.

We believe that the owner of the platform should never be able to covertly eavesdrop on what users are sending each other. Therefore, we currently utilize AES256 to encrypt communication and NTRU cryptography to exchange secrets and we are working on adding OTP and QuEME for the communication and Kyber and Dilithium for key exchange. Users own their data by locally securing their secrets on their devices–not servers. Thus, they are given absolute ownership and responsibility of their own cryptographic secrets.

We ensure the unwavering strength of our security measures by mandating the use of end-to-end encryption for all communications, including group chats. This approach cultivates a culture of robust security that users cannot opt out of, which underscores our steadfast commitment to protecting user data.

We use two independent cryptographic systems–on for identity, and another for communication. This makes the system thoroughly resilient against damage from the theft of user secrets.

And finally, it is necessary to ensure that the application incorporates the benefits of Web3 without overcomplicating the interface. For those who may find Web3 unwieldy, we provide a legacy authentication option: username password login.

File sharing

Offering a high degree of security only for messaging is not enough, as most users want to share other types of sensitive data, including documents, images, audio and videos. All data transferred through the Orion messenger application is end-to-end encrypted, whether a direct message, group chat, or attachment.

We leverage a microservice architecture that offers easy expansion and regular implementation of new features. All services are stateless and can be easily scaled horizontally, which allows service at a global scale. We also benefit from using well defined interfaces, protocol buffers for service to service communication, and swagger for client-server interactions.

To accelerate the system, we added a websocket signaling system to deliver instant notifications to users, which allows the application to fetch data faster and ensure a better experience.

The data authenticity is protected by our cryptographic identification system. Our Web3 vision and long-term goals, driven by decentralization and industry best practices regarding tokenization and fee distribution, protects us against malicious actors, as it disincentivizes their most common attack patterns.

Community

As proponents of free speech, both in communications and in the assembly of communities, Bellatrix offers a modern set of tools for leaders and content creators to organize groups of people, schedule events and create connections with other communities, forming a federated web of independent organizations.

Second Epoch - Betelgeuse

The second product of Orion, Betelgeuse, consists of a decentralized storage node network which offers the streaming and storage of encrypted data. The release of this product marks the beginning of a new epoch in the history of Orion when users will be able to directly participate in the protection and conservation of their data. The nodes in the network will guarantee the quality of their service through escrow mechanics, and will achieve a consensus that validates the quality of all participants by consistently verifying the Proofs created by each node.

Decentralized Data Streaming

When creating a global service offering storage and social media features, performance is a major concern for Web2.0 projects. The conventional approach is to outsource the data transfer to cloud providers that offer PubSub services. To bring this level of user experience into the Web3 era, similar performance must be achieved through a decentralized system. We have designed and tested a decentralized PubSub, that welcomes anyone to participate and incentivizes them to offer highly efficient data streams.

A decentralized version has other advantages over its Web2.0 counterpart. With decentralization, a mesh network of independent contributors will be working hard to deliver the data from content creators directly to the consumers. This ensures that there is no such thing as a single owner of the platform; thus, no one will have the capability to cut you off from your data.

Decentralized Data Storage

Similar to the data transfer, the storage network must be decentralized. This way the data can be randomly replicated across multiple independent participants. This increases security, thus reducing the ability of hackers to breach the system and steal private data. Furthermore, a Web3 native storage network provides users better control over who is able to access their data. To ensure data persistence, storage providers will be able to contribute their storage to a storage liquidity pool of the network and will be properly incentivized for long-term retention.

Ecosystem

Betelgeuse, our decentralized encrypted storage solution, presents other developers with an opportunity to use our system to deploy their own applications. They can leave centralized Web2.0 storage behind. This will create an ecosystem of applications that will increase the volume of the network, incentivizing additional nodes, and thereby strengthen long term stability. At this juncture, content creators may prefer to make the transition to Web3 identities or maintain a Web2.0 authentication.

Apart from enabling software providers to consume the network, this stage also includes the development and migration of all Orion-related services (including communication systems, data protection services, password managers, wallets and other security and privacy services) to the Betelgeuse network.

Third Epoch - Orion’s Belt

The third phase, Orion’s Belt, is our migration of Bellatrix and Betelgeuse onto a decentralized Layer-1 blockchain that meets post-quantum security requirements and is optimized for supporting the streaming and storage of data. The blockchain selected will be EVM enabled to allow consumers to run custom applications on a familiar interface that still leverages best-in-class post-quantum security.

Post-Quantum Blockchain

The importance of having a decentralized blockchain that can't be broken–even if the attacker possesses quantum computers–should not be underestimated. With the inevitable march of technology, the threat of quantum computers will only increase until classical encryption algorithms can no longer promise "unbreakable" security.

To mitigate this, we must embed post-quantum cryptography not only into our messenger but also into the underlying ledger. There are two reasons why accounting and messaging must be supported by outstanding security:

1. The data must be publicly available
2. The data must be kept for a lifetime

Combination of these two traits guarantees that attackers will have sufficient time to crack any encryption. Thus, we must not only take advantage of today's most secure post-quantum algorithms, but also ensure that the security of the system is easily upgradeable.

A secondary, but equally crucial aspect of selecting a blockchain specialized to supporting data streaming is that it must be extremely fast. To ensure we select a chain that is as fast as possible, we've researched the best consensus protocols in the industry for a solution that will easily allow for latency sensitive functions. The low-level implementation of the protocol must be optimized to further accelerate functions, for example by giving them direct access to the transactions pool.

Migrating Bellatrix and Betelgeuse onto a post-quantum blockchain is the final step to ensure network resiliency and user sovereignty. By the third epoch, the entire software stack–from messaging through storage and right down into value transmission–will be decentralized and quantum encrypted.

It's at this stage that our true vision will be realized, and we have raised the collective consciousness and the bar for decentralized quantum security. Additionally, we will build and nurture a new generation of trustless platforms, security conscious norms and the next evolution of Web3 security developers by offering our platform to anyone who wishes to innovate atop Orion's Belt.

As you can see from our genesis story, our motivation is clear, and the threats are real. Our vision and technology are groundbreaking while our competitors have proliferated a dangerous and misleading illusion. They've done it well; however, they've gotten greedy, and their true character is showing. We're all getting wiser and realizing *free isn't value* - that it actually comes at a significant cost. The world is slowing but surely learning that ***if you aren't paying for a product, you are the product***. Below you will discover there are millions of powerful creative thinkers, influencers and fellow humans that will be freed and thrive with Orion.

Target Markets

Our go-to-market strategy is based on numerous business factors driving the immediate need for Orion. We've identified several potential audiences with a strong affinity for privacy, anti-censorship, verified identities, free speech and community engagement. Below we outline some of the prospective audiences we're actively pursuing:

Influencers and Content Creators

In addition to the concerns defined throughout this paper surrounding the slow decline of our fundamental rights, we believe content creators face several more growing concerns spreading across social media and messaging apps severely impacting their brand, reach, and audiences.

Algorithmic Manipulation

The algorithms used by social media platforms are deliberately crafted to keep users engaged for as long as possible. This often results in a prioritization of sensationalism, clickbait, and emotional manipulation over substantive content. These algorithms exploit content creators by forcing them to produce material that adheres to these superficial standards, thus stifling their creative expression.

Platform ownership of communities

When social media platforms exert control over the communities built and nurtured by influencers, it can have several negative consequences for both the creators and their audiences. In essence, their followers are loaned to them by the company. Some of the key issues arising from this power imbalance include a loss of creative control, vulnerability to platform changes, platform lock-in, monetization constraints, censorship, and content removal, and data ownership and privacy concerns.

Monetization challenges

Influencers and content creators often struggle to monetize their work on social media platforms. These companies take a significant cut of any revenue generated, and stringent guidelines can result in demonetization or removal of content altogether. The ever-changing monetization policies create an unstable income stream for creators while the platforms continue to profit from their labor.

Follower Exploitation

Social media platforms are known to employ psychological tactics that prey on users' innate desires for validation and social approval. Influencers, by virtue of their large followings, are particularly susceptible to this exploitation. They are incentivized to prioritize the growth of their audience and engagement metrics above all else, which can lead to a focus on shallow content, ultimately doing a disservice to their followers.

Fake Followers and Bot Accounts

The proliferation of fake followers and bot accounts on social media platforms is a concerning issue that skews the perception of engagement and success for influencers, followers, and any external parties viewing the content. These inauthentic accounts not only inflate engagement metrics but also foster a false sense of popularity, leading creators to make misguided decisions about their content and brand partnerships. This deception can also result in inflated advertising costs for companies that rely on accurate engagement data for their marketing campaigns. Furthermore, fake followers erode trust in the influencer ecosystem, making it increasingly difficult to discern genuine engagement and organic growth from artificially manipulated numbers.

Influencer Copycats and Financial Scams

The rise of influencer copycats and the promotion of financial scams have detrimental effects on both the original content creators and their audiences. Copycats, who mimic the style, content, or persona of successful influencers, dilute the creator's unique brand identity and divert attention from their original work. This can result in lost income, reduced growth, and diminished credibility for the genuine influencer. Moreover, when these copycats promote financial scams, such as fraudulent investment schemes or counterfeit products, they exploit the trust that audiences have placed in the original influencer. Unsuspecting followers may fall prey to these scams, losing money and suffering from a sense of betrayal. This tarnishes the reputation of the authentic influencer and erodes the trust that is so crucial to the influencer-follower relationship. Furthermore, the financial scams themselves contribute to a negative perception of influencer marketing as a whole, casting doubt on the legitimacy and ethics of creators operating in the space.

Data Collection and Privacy Breaches

Social media platforms collect massive amounts of personal data from users, including influencers and their followers. This data is used to create targeted advertising, which generates revenue for the platform. Users rarely have control over how their data is used, and these practices are often veiled in obscure terms of service agreements, leaving both influencers and their followers vulnerable to privacy infringements. It is essential for influencers and their communities to be aware of how their data is being scrapped, packaged, and resold.

Exploitation

In conclusion, social media and messaging platforms are designed to maximize profits for the companies that own them, often at the expense of content creators and their followers. The exploitation of influencers and the commodification of their work should not be taken lightly. It is vital to push for increased transparency, fair compensation, and greatly improved encryption and data protection rights within these digital spaces to ensure the well-being and creative freedom of those who rely on them for their livelihoods.

We’re reaching influencers by developing a compelling incentive program and offering exclusive features (including a robust loyalty and engagement point system, promotional tools, and monetary rewards) to motivate influencers to actively promote and use Orion. We also collaborate with influencers on content creation, events, and campaigns to enhance community engagement.

Web3 Early Adopters & Practitioners

This audience is already familiar with decentralization, Web3, and tokenization concepts. They are early adopters of new technologies and can quickly understand Orion's innovation, benefits, and timelines. They inherently value their privacy and fundamental rights and support the numerous benefits of decentralized frameworks such as DeFi, DeSci, and DeComm.

We’re reaching them by engaging with the crypto and blockchain communities through social media, forums, and discussion platforms. We also attend, and sponsor industry conferences, meetups, and events to build relationships and exchange thought leadership around improving security, privacy, and protecting our rights as free thinkers.

Privacy, Rights, and Security Advocates

This audience is a direct reflection of our core values and beliefs. We collectively are very concerned about data privacy, security, censorship, and government surveillance. This audience, like us, has experience using privacy-oriented messaging apps and we appreciate the added benefits of Orion’s quantum security and Crown Sterling's strong ethos in data sovereignty and our inalienable human rights.

We’re reaching more of them by sharing informative content and highlighting the importance of privacy, security, and later decentralization. We also connect with privacy and security influencers, experts, and thought leaders.

Along with the core audiences above, we also align strongly with digital nomads, remote workers, activists, and journalists.

To serve and nurture the Orion community, it is crucial to provide these communities with increased security through advocating and building robust verification processes and a seamless integration of novel encryption technologies. Moreover, we will provide compelling incentive structures to honor the influencers, their creative work, and the integrity of their own communities. Our team and Orion will do that. We, too, are creators, privacy and rights advocates, and world-class cryptographers, building a platform for our fellow creators and their audiences. We believe it’s crucial to advocate for a more equitable distribution of power, revenue and control between platforms and influencers, enabling creators to speak and assemble freely while maintaining their autonomy and protecting the interests of their communities.

We will not sell your data
We will not censor protected free speech
Algorithms will not up or down regulate your content
No spam bots and copycat accounts
Your platform, your community, your content
By creators for creators

Conclusion

We're living in a world where our data is an extension of who we are, so it must be protected and its value reclaimed by you, its rightful owner. The evolution of boundary conditions and borders is happening at a rapid pace, primarily due to the accelerated evolution of the digital space. We believe that boundary conditions for new sovereign communities will be based on quantum-secure encryption. Within those communities, new economies will emerge; and within those economies will be money systems - barter, trade, collective bargaining - everything we see in functioning economic systems.

We see content creators and influencers as pioneers - leaders of microeconomics, and we envision Orion as the platform that will support these decentralized sovereign communities in creating their own mechanisms of economy, able to interact with each other and not have to worry about censorship from a centralized function. We've built and continue to develop solutions and applications driven by our mission of Personal Data Sovereignty rooted in our Data Bill of Rights and will continue to advance with new features and tools to meet the demands of the evolving digital world.