Outlier Ventures presents

The Post Web

PRIVACY ENHANCING TECHNOLOGIES IN THE POST WEB

CO-AUTHORED BY

JAMIE BURKE
Founder & Chairman, Outlier Ventures

JASPER DE MAERE
Head of Research, Outlier Ventures

Residual Centralisation for Specific Needs

Even with decentralised systems, some wallet functions may remain centralised due to unique performance requirements, such as ultra-low latency or high-throughput applications. While the majority of infrastructure should decentralise to safeguard critical assets and interactions, **retaining centralised components for specific use cases could be an acceptable tradeoff for enhanced usability.**

Let's unpack 'personhood' and 'assets', two components that the wallet will host in The Post Web.

Personhood

Personhood is the comprehensive representation and management of a user's identity, reputation, data, and privacy.

TL;DR

- **Personhood:** Encompasses identity, reputation, personal data, and privacy, forming the user's unique personhood.
- **Dynamic Management:** Wallets must manage personhood elements dynamically, balancing control, consent, and secure interactions.
- **Privacy:** Privacy-enhancing technologies (PETs) like ZK proofs enable secure and private interactions, but due to cost considerations, they will be applied selectively.
- **Human-in-the-Loop:** Until universal regulatory frameworks exist, human oversight will remain critical to ensure accountability and manage personhood within wallets.
- **Personal data:** Serves as the foundation for enabling automated, agent-driven services while addressing risks like algorithmic biases.

Personhood within wallets in The Post Web includes a user's identity, reputation, personal data, and privacy, forming the basis of their digital presence and interactions. This allows users to control their digital footprint, manage consent and permissions, and engage securely and privately with AI agents and decentralised services. In order for personhood to have a meaningful impact and be accounted for in **economic, on-chain activity, a comprehensive, universally accepted regulatory framework** needs to be in place to govern identity, data, and privacy across the ecosystem. Until then, we believe that humans will need to be **involved (human-in-the-loop approach)** to ensure oversight and accountability in respective jurisdictions in managing personhood and teaching character and social function to better represent a person. Nonetheless, this is critical in enabling agents to function with a **high degree of autonomy** on behalf of individual users or entities.

EXHIBIT 21:

The Layers of Personhood in Post Web Wallets

Source: Outlier Ventures

Exhibit 21 illustrates the dynamic layers of personhood within wallets in The Post Web.

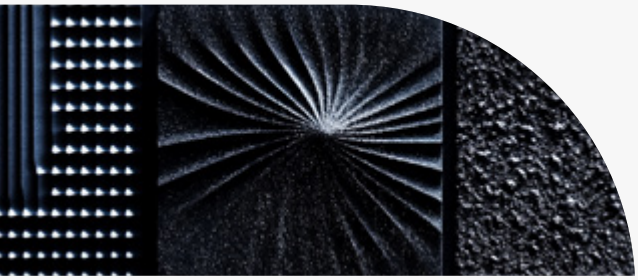
→ At the core is **Personal Data**, the foundation that powers all other elements.

→ Surrounding it is **Identity & Reputation**, derived from data to establish trust and credibility.

→ **Consent & Permission** acts as the gatekeeper, dynamically controlling access to personal data and identity based on user preferences.

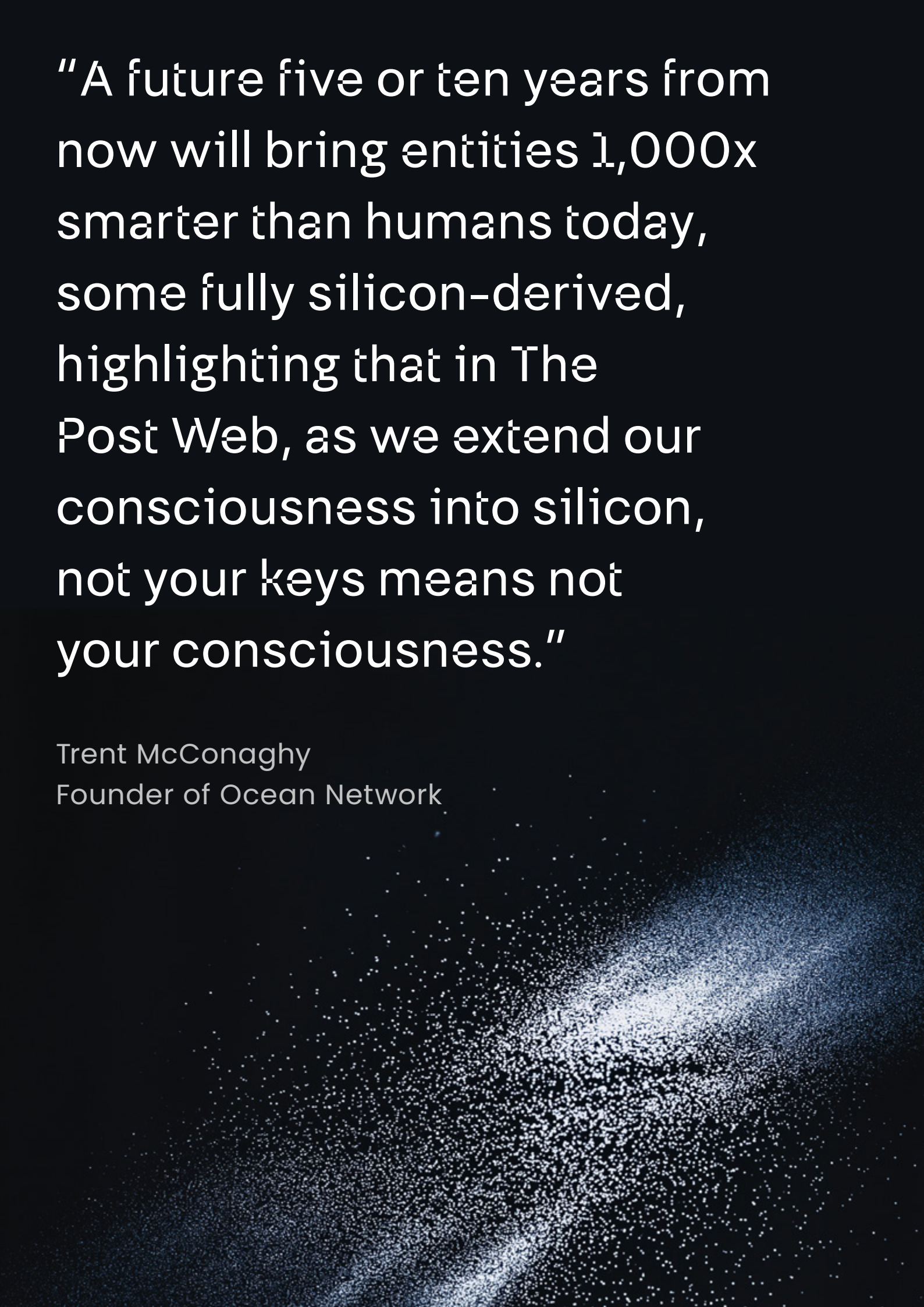
→ Encompassing everything is **Privacy**, the protective layer that regulates the flow of information and ensures sensitive data remains secure. Together, these layers create a cohesive framework, enabling secure, controlled, and trust-rich interactions in The Post Web ecosystem.

Let's unpack the different elements of personhood within wallets.



“A future five or ten years from now will bring entities 1,000x smarter than humans today, some fully silicon-derived, highlighting that in The Post Web, as we extend our consciousness into silicon, not your keys means not your consciousness.”

Trent McConaghy
Founder of Ocean Network



Personal Data

Today, personal data is often stored in silos on Web2 platforms, outside the user's control. Much of the information is duplicated and outdated. Furthermore, this data remains inaccessible to the user, undermining their sovereignty.

As discussed above, **personal context, and therefore data, is the foundation for powering personhood in The Post Web wallet.** In this vision, personal data will be treated as a bearer asset, securely stored within wallets. As more economic activity moves on-chain, wallets will increasingly house transactional and behavioural data, evolving from basic information to complex user profiles. This enriched data will enable highly personalised services while being safeguarded through robust privacy measures and granular, automated consent mechanisms.

Managed by consent and privacy layers, The Post Web will enable agents to use dynamic and portable data enriched by contextual information to optimise information distribution in real-time based on changing user preferences, locations, and circumstances. At the same time, agents will preserve necessary levels of privacy by unlocking private verifiability through the use of privacy-enhancing technologies (PETs).

Identity & Reputation

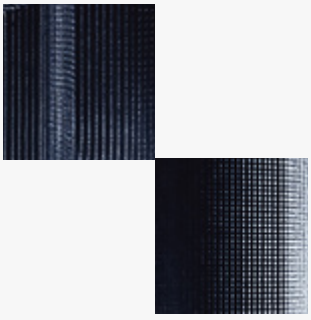
Identity and reputation (I&R) are built on top of personal data, which is extracted and synthesised into actionable metrics that form the foundation of trust in The Post Web. Identity provides static verification, acting as a reliable anchor, while reputation serves as a dynamic and cumulative credibility metric, evolving with users' actions and interactions over time. However, the interplay between static identity and dynamic reputation introduces challenges in ensuring both can coexist seamlessly, especially as decentralised systems aim to balance verifiability with pseudonymity.

As they are the enablers for trust-based, economic transactions, the economic importance of I&R in The Post Web cannot be overstated. **Identity is a static trust layer, while reputation reflects real-time reliability within specific socio-economic contexts.** Together, I&R empower users to leverage their digital presence for economic gain, fostering a more equitable and trust-rich internet. However, the reliance on pseudonymity in many Web3 contexts creates tension with the growing demand for verifiable identity, particularly in regulated industries and agent-based systems.

Identity and reputation in The Post Web will extend beyond individual users, becoming **contextualised within their social graph as social dynamics increasingly move onto DLT through trends like SocialFi**. By incorporating relationships and interactions within a user's network, these systems can create more nuanced and context-specific trust metrics, enhancing credibility and fostering trust in social and economic interactions.

In Web3 today, efforts for on-chain reputation are ongoing but have yet to see much traction, largely due to the lack of viable on-chain economic use cases where reputation is critical. **Reputation's dynamic nature** and need for real-time updates further limit its development, leaving users with little incentive to build this dataset. Moreover, as reputation is highly context-specific, designing systems that accurately reflect credibility across diverse socio-economic interactions remains a significant challenge. In contrast, identity has seen greater success, especially as regulated industries such as finance, healthcare, and insurance adopt DLT and, by extension, AI agents. **While identity challenges the pseudonymous ethos of early Web3, it will become increasingly important in enabling agents to operate in these regulated environments,** provided that safeguards are in place to protect user privacy and control.

In The Post Web, **as users empower agents, identity and reputation will be critical components, requiring robust management to unlock the full potential of trust-based interactions and economic activity.** Reputation systems will need to address existing limitations by integrating real-time updates and incentivising users to contribute to dynamic trust frameworks. Meanwhile, identity will need to evolve in a way that balances the demands of regulated systems with the decentralised principles of Web3, ensuring that both identity and reputation support a trust-rich, equitable, and adaptable internet.



Consent & Permission

Today, wallets are primarily focused on **authorisation**. By clicking "sign," users effectively **consent to execute a specified transaction.** This core aspect of wallets will remain essential in The Post Web, although the **nature of consent will become far more complex** than transaction signing in Web3. Authorisation of **consent and permission is crucial as the near-irreversible final step** that empowers agents to act on behalf of users.

Humans need to improve at managing consent, as demonstrated by the unwillingness of people to engage with cookie consent forms or navigate GDPR toggle menus. In recent years, we've also seen a rapid rise in **consent fatigue**, where repeated consent requirements lead to user disengagement and high drop off rates. Whilst we believe The Post Web has the opportunity to remove much of this poor UX, we foresee similar challenges with human in the loop consent and permissioning when delegating activity to agents unless regulators embrace its innovations.

Highly automated, granular consent solutions will be essential in The Post Web to ensure users authorise their intended actions. As more economical and meaningful activities are outsourced to agents, consent will become more complex and crucial. **When agents act as representatives of users**, they must also be able to identify themselves as authorised representatives to ensure trust and verifiability in their actions.

Today, consent fatigue is managed through intuitive consent UX/UI and easy language. Given how much activity will be delegated in The Post Web, we don't see this as a sustainable solution. **Instead, we believe that highly granular user profiles, created from large personal data and preferences compilations, will unlock the degree of automation needed** by enabling systems to act based on these preferences. However, this approach risks creating biases if the algorithms managing these profiles are centrally controlled, a challenge that must be carefully managed.

"Without advancements in users' ability to grant informed consent and authorise agents to act on their behalf, the full vision of a Post Web will be unnecessarily constrained."

As a consequence, founders have a significant, untapped opportunity to abstract and streamline consent and permission management as wallets evolve to hold users' reputations, identities, sensitive personal data, and more. This is a bottleneck which needs to be overcome before we can delegate large pockets of commoditised economic activity to agents.

Privacy

Privacy, similar to consent and permission, is about **information governance** and the ability to **obscure aspects of sensitive or proprietary information**. However, it is often mistaken for anonymity, which is a separate concept.

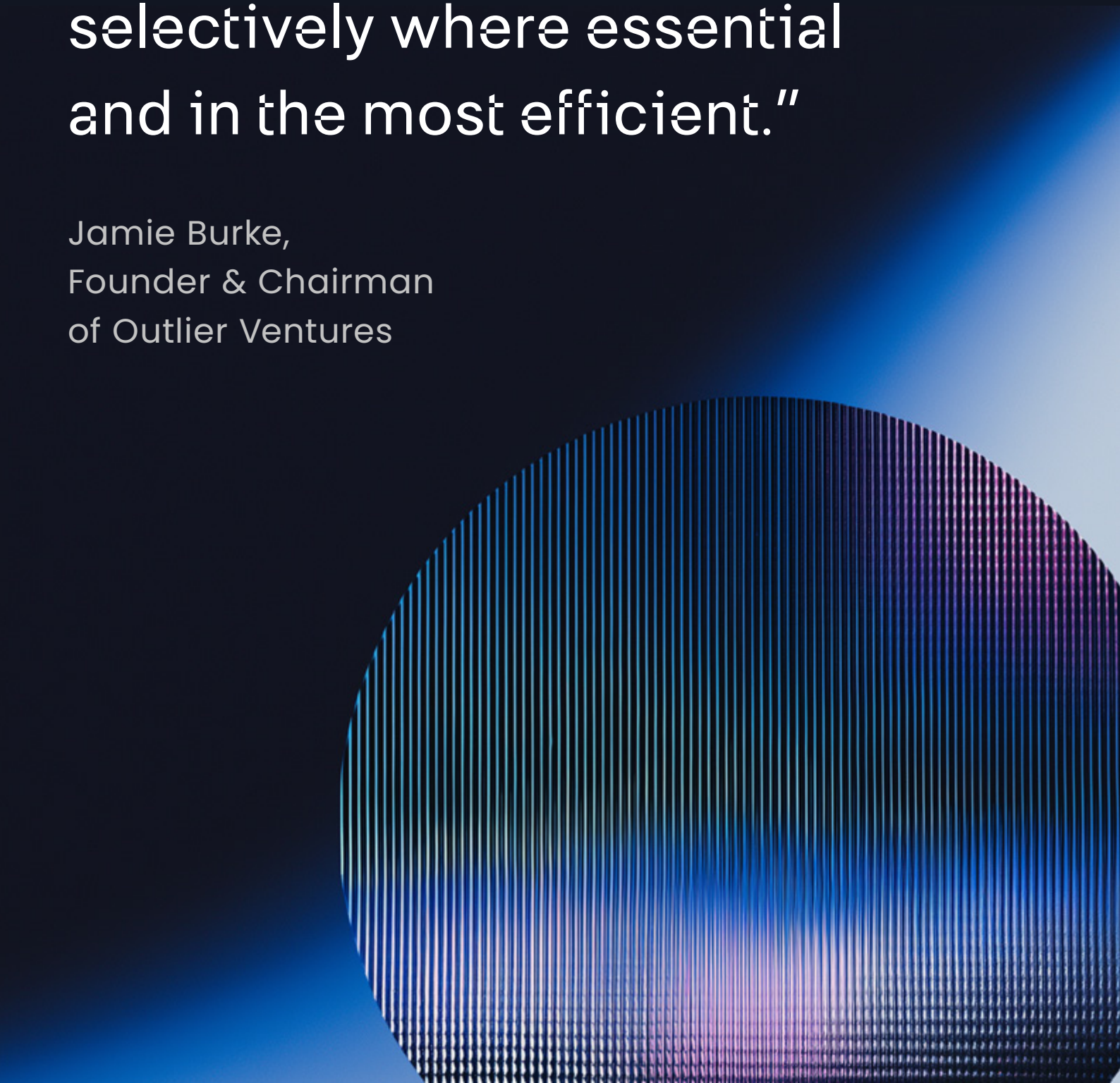
Privacy-enhancing technologies (PETs) such as; **zero-knowledge proofs, fully homomorphic encryption, trusted execution environments, and multi-party computation** are not exclusive to cryptocurrencies and blockchain. However, today, they are making rapid progress in areas like **cost, throughput, and capacity**, making many of these technologies **economically viable for the first time.**

Private verifiability, the ability to prove the authenticity and accuracy of information without revealing underlying data, is poised to **transform which types of economic activity can be hosted on-chain. The ability to specify levels of information asymmetry** between economic actors is critical for various use cases where competitors operate on the same permissionless blockchain.

That said, PETs are one of the **most underappreciated pieces of innovation in Web3 today** and will be critical in making The Post Web and the **computable economy possible**. That's why we have a dedicated section on privacy in Chapter 4 of The Post Web thesis.

“Given the costs of privacy-enhancing technologies (PETs), The Post Web will likely default to openness, using privacy selectively where essential and in the most efficient.”

Jamie Burke,
Founder & Chairman
of Outlier Ventures



Be part of The Post Web conversation

Listen to our podcast

Hear a weekly Web3 specialist in conversation with Jamie Burke

Follow us on LinkedIn

Be the first to hear about our announcements and launches

Follow us on X

Join the conversation and follow **@OVioHQ** on X

Sign up to our Newswire

A weekly round up from our ecosystem, straight to your inbox

postweb.io