The Crypto-Contrarian

The following casts a dark view on crypto as it stands today, but rest assured, I believe in public validating networks and the future of digital assets.

My crypto-journey began in 2013, where I was immediately hit by how greed before utility mattered most.

Ten years later, crypto hasn't progressed and there are no legally credible killer apps emerging from the viper's nest of anonymous transparent chains waiting for new victims.

I often listen to Pivot, with Kara Swisher and Scott Galloway, discussing how they know more about crypto than 99% of people, and they still don't understand it. Well, they have my sympathy.

For what it's worth, the fraudulent truth of crypto's inadequacies is hidden behind the double speak of intellectually gifted fraudsters that hide the truth to project network values, and crypto-influencers that sell a promised-land they do not understand."

Facts

Chains must be fast, compliant, and composed of authenticated and unique users. Asset management must be easy, fast, secure, and offer superior recovery compared to existing centralized incumbents. Privacy and compliance must be absolute, as businesses will only use decentralized services if their activities are confidential and deemed compliant.

Transitioning Ethereum-like monolith code and anonymous users to a compliant framework is delusional. Successful future network effects will come from working applications driving usage of a compliant ecosystem. Existing alt-coins cannot and will not become compliant and will rapidly fade as mainstream compliant apps become newsworthy.

Background

Why Layer 1 solutions matter, and why doubling down on Layer 2 is is flawed

Layer 1 - efficiencies

Compliant chains must enable encryption that can execute at machine speed because chains, not applications, must be compliant in order to ensure users cannot have more than one wallet, preventing wash trading and money laundering. Identity-embedded compliant chains require validators to execute optimal, encrypted transactions at machine speed. Optimal encryption is required for privacy, authenticated user lookups, compliance scanning, and ease-of-use crypto shielding. Compliant chains must enable self-regulation to protect a user's privacy. Mainstream platforms must enable authenticated recovery if they are to replace familiar centralized recovery methods.

Layer 2 - inefficiencies

Optimal validator encryption cannot be invoked using a Layer 2 chain, as excessive inefficient virtual machine bytecode would need to be encrypted and executed by validators. Layer 2 chains also cannot harness encrypted transaction efficient roll-ups because lost transaction data denies comparative analytics.