**Web3 Wallet Communication — Research**

As Web3 continues to decentralize in ways that scale, new products will be created without the need for centralized entities (duh) -- with permission-less communication tools now at the forefront of attention.

Before diving into a number of different products that are being created in this space, I think it’s worth mentioning the ways in which users have leveraged the Ethereum blockchain to communicate with one another.

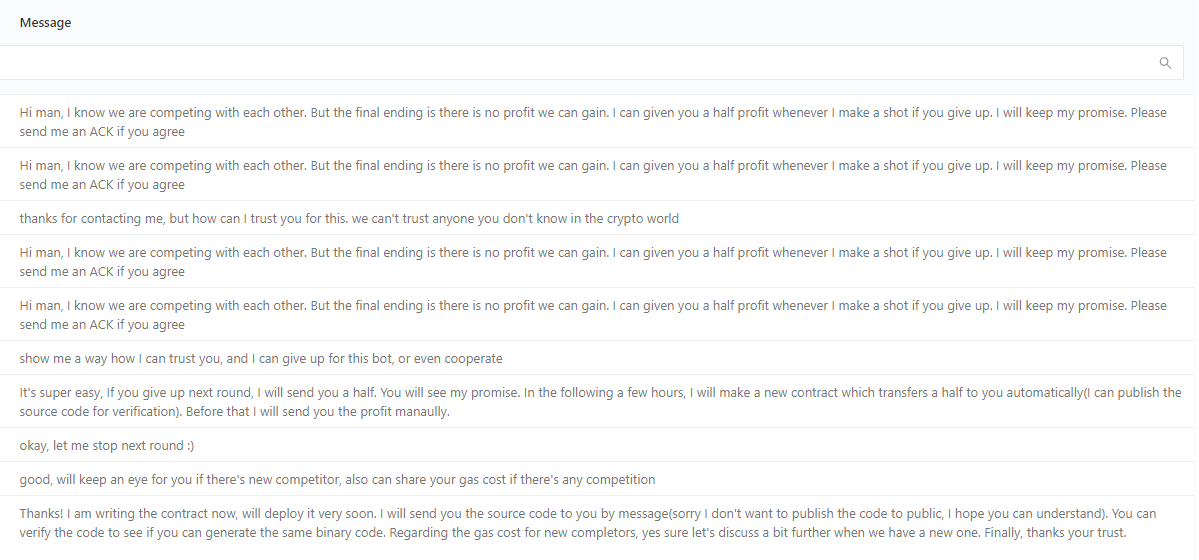
### **Input Data Messages (IDM)**

The input data field on an Ethereum transaction is typically used to update contract call information where …”Data is written in hexadecimal form which can be decoded to show the exact function being called. However, the same field could be used to enter hexadecimal data that — when converted to [UTF-8](https://en.wikipedia.org/wiki/UTF-8) encoding — is represented as text.” (Etherscan blog).

The Etherscan team has decoded and identified a number of these messages and boiled them down into different categories including:

1. Transaction receipts/notes
2. Description of properties (in JSON)
3. Crypto begging
4. Advertising
5. Conversations

Below is an exchange between two MEV bot operators who are communicating through IDM.



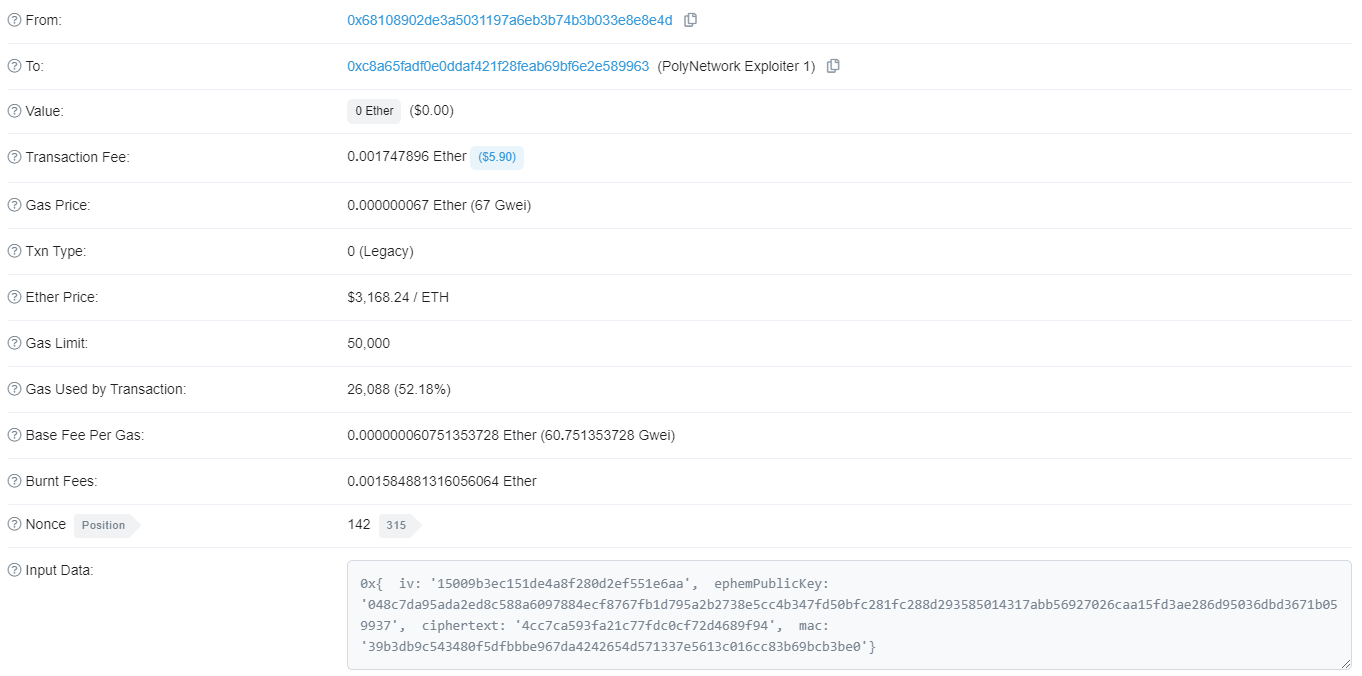
Two MEV bot operators in contact via IDM.

### **Non-Standard IDMs**

Any IDM that is not sent using standard text. Examples include:

1. Encrypted Messages
2. Event Logs
3. Bytes

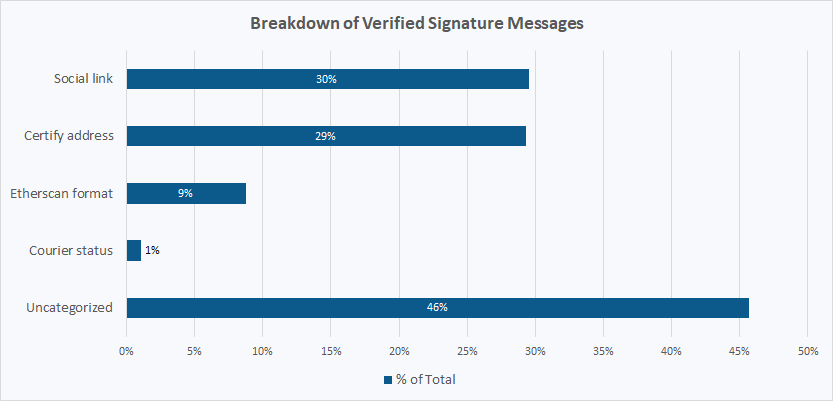
Below is an *encrypted* exchange sent to PolyNetwork Exploiter 1.



Encrypted IDM example

### **Verified Signatures**

Verified signatures are messages stored off-chain where a wallet owner can sign a message using their private keys to verify both their message and address. Since these signatures aren’t tied to an address, Etherscan ultimately built a message aggregator to allow users to view the signatures. It’s important to note that these messages don’t incur a transaction fee like IDMs and don’t require conversion from hexadecimal to UTF-8.



Signature breakdown

Even with seemingly archaic forms of wallet-to-wallet communication methods, there is a large number of people who use these tools for a number of different reasons. Since these communication methods have been used for some time, others have taken notice and have developed better interfaces for users to interact with.

### **Blockscan Chat**

Developed by the team behind Etherscan, Blockscan Chat allows users to instantly message any Ethereum compatible address through a web based application. This messaging tool also allows users to access chat messages across multiple devices, block addresses, and receive notifications upon message arrival. However, as convenient as this application is, Blockscan Chat faces issues related to decentralization and encryption. All data is stored on Blockscan’s servers and no messages are sent on the blockchain. While the messages are transmitted over SSL, they are not currently end-to-end encrypted. After reading through the applications TOS, Blockscan Chat also has the ability to suspend and/or terminate your access to the platform.

### **Ourspaces.xyz**

Ourspaces was developed by Chris Min, former engineer at Dharma Wallet, who launched the product back in November of 2021. Ourspaces, like Blockscan Chat, allows users to message an Ethereum compatible address but allows these users to create token gated group-chats, where creators input a ERC-20 / ERC-721 contract address and add requirements as shown below. The product appears to have the same problems as Blockscan Chat, including decentralization and encryption, although encryption appears to be on the roadmap going forward.

### **Status.im**

Status is a mobile wallet that allows users to buy and hold assets, discover dapps, chat with other Ethereum addresses, and post status updates to keep in touch with Etheruem contacts. Status uses Waku, a peer-to-peer protocol for private, secure and censorship-resistant communication, built by the [Vac Team](https://vac.dev/). Waku provides messaging with no dependence on centralized servers, data centers or service providers. Every message is end-to-end encrypted, and broadcast to every single peer in the network. However, messages are not stored on the blockchain and do not cost anything to send. By default, encrypted messages are cached on Status nodes for 30 days so that you can still receive messages even if your phone is offline. Currently, Status hosts a set of these special nodes in order to support its users, however, anyone is able to host a Status node with the proper hardware.

### **Inb0x.life**

Inb0x is an Ethereum wallet communication platform that provides end-to-end encryption services. Once users sign a message through MetaMask, the website prompts the user to then allow MetaMask to secure the user’s newly generated key pair used for encryption. While the service utilizes web3 encryption tools, the platform isn’t decentralized nor are the messages stored on-chain.

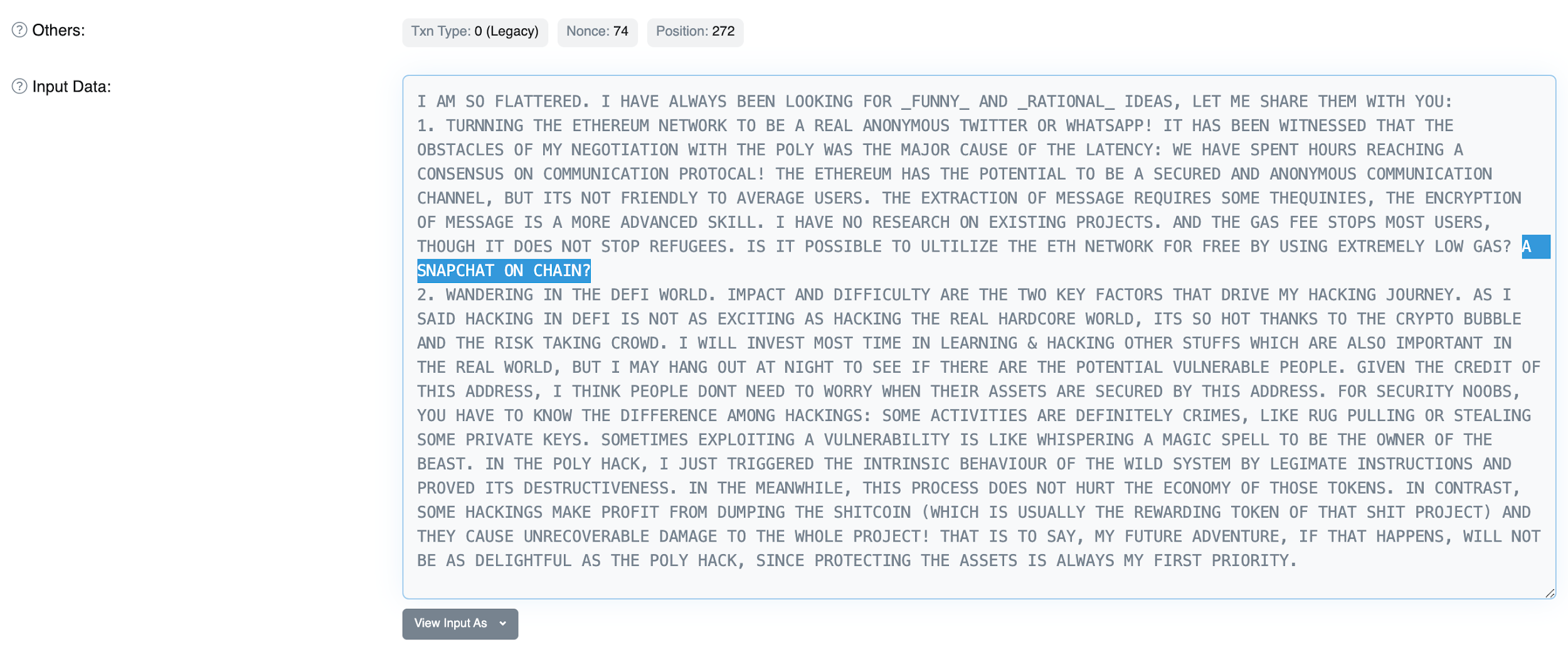
### **Summary**

There has been a growing number of platforms created that aim to offer solutions to the existing nature of wallet-to-wallet communication. As time progresses, this space will continue to become saturated, with rumors of mobile wallet apps entering the communication space. However, many of these platforms are not fully decentralized and/or not fully encrypted which poses risks to the users of said platforms. While there is an opportunity to improve on the shortcomings of these platforms with enhancements to the tech stack, there is also an endless amount of opportunity to build differentiated applications using wallet-to-wallet communication technology.

### **Opportunity**

Once encrypted, fully decentralized, scalable messaging technology can be deployed to Mainnet successfully, I suspect that product market fit will be achieved the fastest through consumer social dapps that leverage the chutzpah of their Web2 counterparts. Gm.xyz (Reddit), Orbis.club (Twitter) and Chingari (TikTok) have all found initial success by simply mirroring existing social applications. Although the level of encryption, decentralization and scalability (as well as success) varies greatly across platforms, it’s clear that social applications present a great deal of opportunity. Considering applications related to text and video have been built, Snapchat and Instagram present themselves as open opportunities.





Polygon Exploiter 1 references snapchat on-chain