近期爆火的Nostr是什麼？如何操作？是否能代替Twitter？Nostr全面解讀

原文：
https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-nostr-protocol

近期，一個名為 nostr 的去中心化社交協議大火，其社交產品 Damus 在短短數日裡用戶就已經突破 72 W。該產品上線後，甚至引來了 Twitter 現任 CEO Elon Musk 爭議性的封殺政策。

那麼，nostr 究竟是什麼？有什麼魔力？為什麼如此受到追捧呢？下文將一一進行探討。

Nostr 出現的原因——爆火的導火索

經歷了反壟斷之年的互聯網群眾們，即痛恨於中心化機構對數據的濫用與侵犯，又無力脫離優秀的應用體驗以及並無選擇性的市場，歸根究底在於社交產品背後是公司為機構在運營，是公司就有接受監管與審查的義務，他所有負責的對像是股東以及註冊地政府，本質上追求的是商業上的成功，而不是言論自由的理想。

此外，目前的社交軟體都或多或少存在著一些問題：

1、Twitter 的問題

- Twitter 有廣告；
- Twitter 使用奇怪的技巧讓你上癮；
- Twitter 不會顯示你關注的人的真實歷史動態；
- Twitter 會禁止某些人的帳戶；
- Twitter 會使用影子禁令（Shadowbans）.
- Twitter 有很多垃圾資訊；

2、Mastodon 和類似應用的問題

- 用戶身份附加在第三方控制的域名上；
- 伺服器所有者可以像 Twitter 一樣禁止你，伺服器所有者也可以阻止其他伺服器；
- 伺服器之間的遷移是事後才考慮的，只有在伺服器協作的情況下才能完成。它在對抗環境中不起作用（所有追隨者都會丟失）；
- 運行伺服器沒有明確的動機，因此它們往往由愛好者以及希望將自己的名字附加到一個很酷的域名上的人來運行的。然後，用戶受制於一個人的專制，這往往比 Twitter 這樣的大公司還要糟糕，他們無法遷移出去；
- 由於伺服器往往是業餘的，它們經常在一段時間後被拋棄 —— 這實際上等同於禁止所有人；
- 如果每台伺服器的更新都必須痛苦地推送（和保存！）到大量其他伺服器，那麼擁有大量伺服器就沒有意義了；這一點由於伺服器數量龐大而加劇，因此更多的數據必須更頻繁地傳遞到更多的地方；
- 對於影片共享的具體範例，ActivityPub 愛好者意識到完全不可能像文本註解那樣在伺服器之間傳輸影片；

3、SSB（Secure Scuttlebutt）的問題

- 它沒有太多問題，我認為這很棒。事實上，我打算以此為基礎，但是它的協議太複雜了，因為它根本就沒有被認為是一個開放的協議。它只是用 JavaScript 編寫的，可能是一種快速解決特定問題的方法，因此它有奇怪和不必要的怪癖，比如簽署一個 JSON 字符串，其必須嚴格遵守 ECMA-262 第 6 版規則；
- 它堅持從單個用戶那獲得一連串的更新，這對我來說是不必要的，而且會增加內容的臃腫和僵化程度 —— 每個伺服器 / 用戶都需要存儲所有的 Post 鏈，以確保新的 Post 是有效的。為什麼要這麼做？(也許他們有很好的理由)；
- 它不像 Nostr 那樣簡單，因為它主要是為 P2P 同步而設計的；
- 不過，可能值得考慮使用 SSB 而不是這種自定義協議，並僅使其適應客戶端中繼伺服器模型，因為重用標準總是比嘗試讓人們使用新標準更好。

4、其他要求運行伺服器方案的問題

- 他們要求每個人都運行自己的伺服器；有時人們仍然會在這些方面受到審查，因為域名可能會受到審查。

而反壟斷的終局古往今來更多是屠龍勇士終成惡龍，既然中心機構做不到，也沒有立場去做，那麼對自由

的嚮往便催生出使用代碼來保障自由的去中心化協議：Nostr。

Nostr 協議是什麼？——真正的去中心化社交

最近大火的 Damus，是建立在 Nostr 協議的一個應用，主要是以去中心化的社交場景（你把它理解為去中心化的 Twitter）即可。

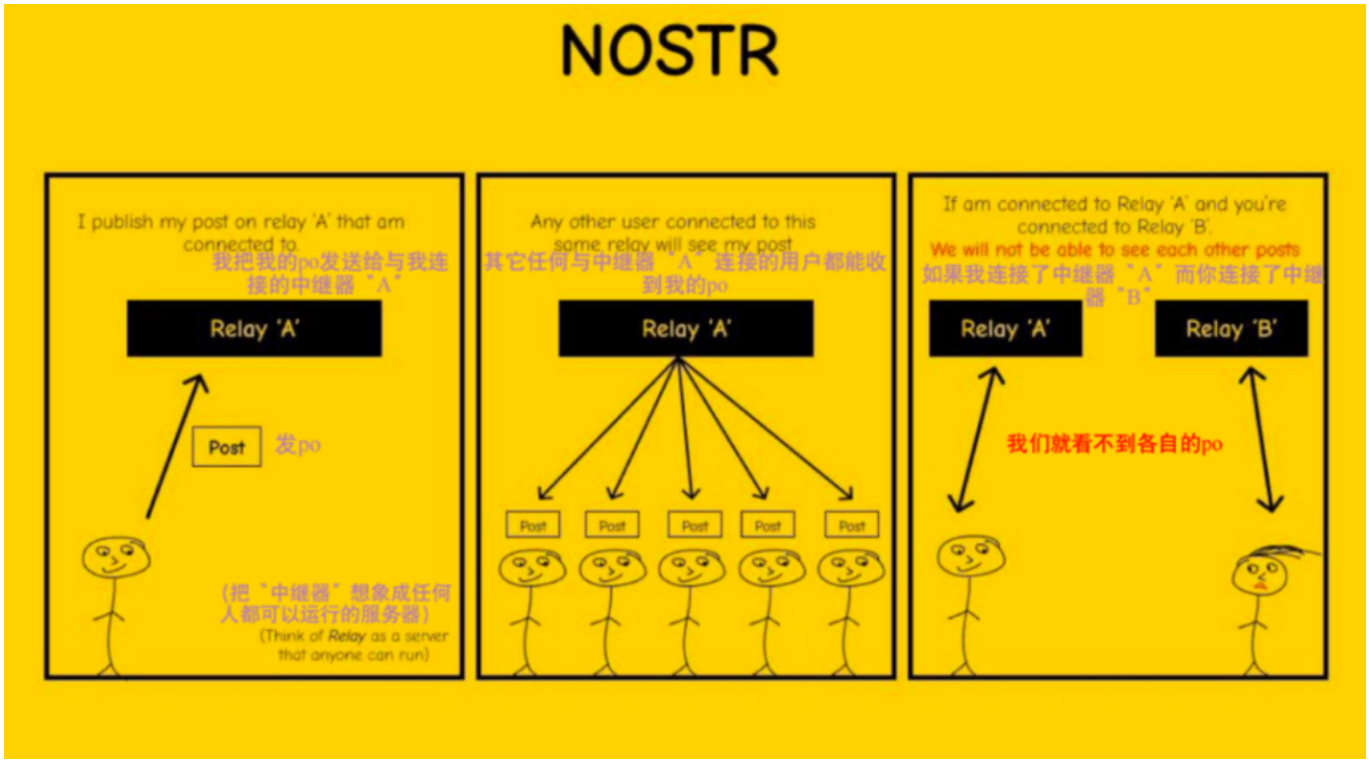
Nostr全稱是Notes and Other Stuff Transmitted by Relays，是一個於2020年啟動的去中心化社交網路開源協議。項目創始人fiatjaf也是比特幣和閃電網路的開發者。目前項目沒有公開融資，**推特創始人Jack Dorsey對該項目進行了14BTC的捐助** 。

透過 nostr 協議，你可以建立很多東西，這個協議相對輕量級的、簡單但可擴展的開放協議，在它上面可以建立真正去中心化的社交媒體平台。

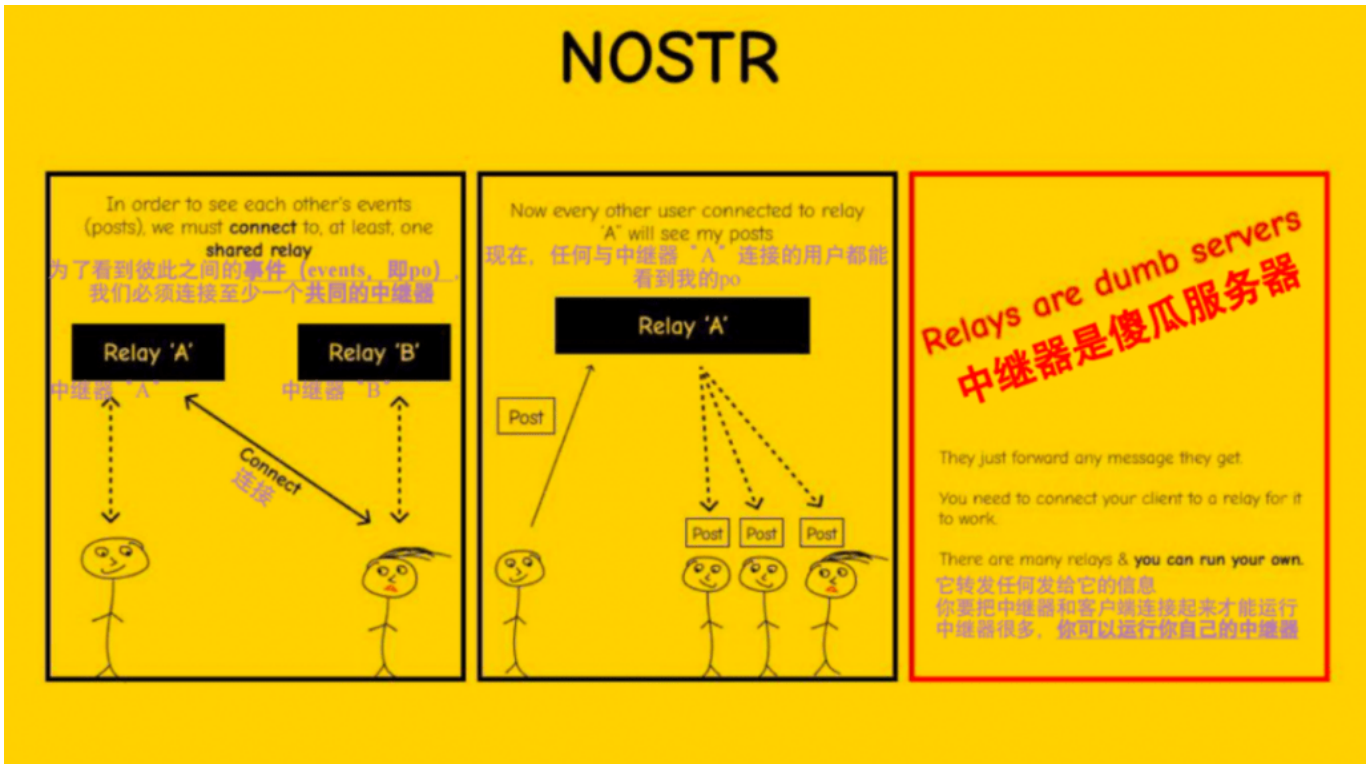
Nostr 協議的運行原理

Nostr協議中由兩部分組成，一個是客戶端Client，另一個是中繼端Relay。客戶端用於簽名、驗證信息，由用戶運行。中繼端可以抓取、存儲任何與它鏈接的客戶端的信息，並且轉發給其他客戶端。

任何人都可以運行中繼端，但中繼端和中繼端之間互不通信，這一點與區塊鏈節點有著本質區別。



另外，客戶端允許用戶與他們想要的任何數量中繼端相連，用戶還可以選擇是否想要從自己所連接的中繼端中讀取、寫入信息等等。這就意味著，我們可以連接某個中繼端來檢索內容，但是可以選擇不在那裡進行事件發布，或者反過來也成立。



如何在 nostr 上創建帳戶？

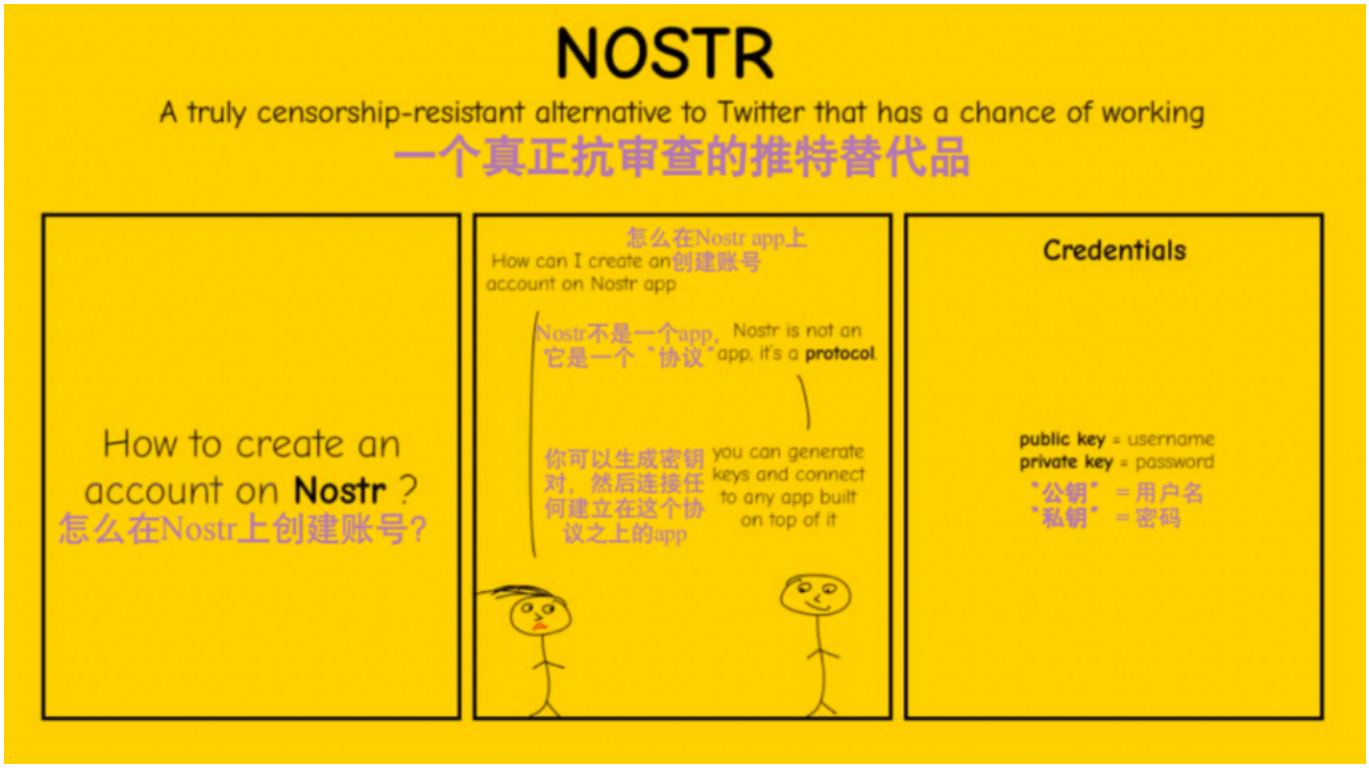
在 nostr 中，我們不需要通過使用個人數據來註冊一個帳戶（這就是它的優勢）。

像比特幣一樣，我們只需要一套鑰匙，也就是兩把鑰匙。

- 一個公鑰（Public Key）作為你的用戶名，這個密鑰可以共享，並對所有人公開（就像你的微博帳戶、微信 ID、銀行帳戶一樣，別人通過這個找到你）。

- 一個私鑰（Private Key)。這把鑰匙像你的密碼，需要對它進行保密，通過這個密鑰，你可以在任何由 nostr 支持的平台上訪問你的帳戶。只需要選擇一個 nostr 協議的客戶端，如 anigma、coracle 或 astral，它就會為你生成，這裡，為了增加安全性，建議使用外部簽名程序，如 Alby 瀏覽器擴展或 nos2x 擴展等等，也可以用 Rana 等工俱生成一個獨立的私鑰。

注意保存私鑰，因為它是將來恢復和重新登錄你的帳戶的唯一途徑。



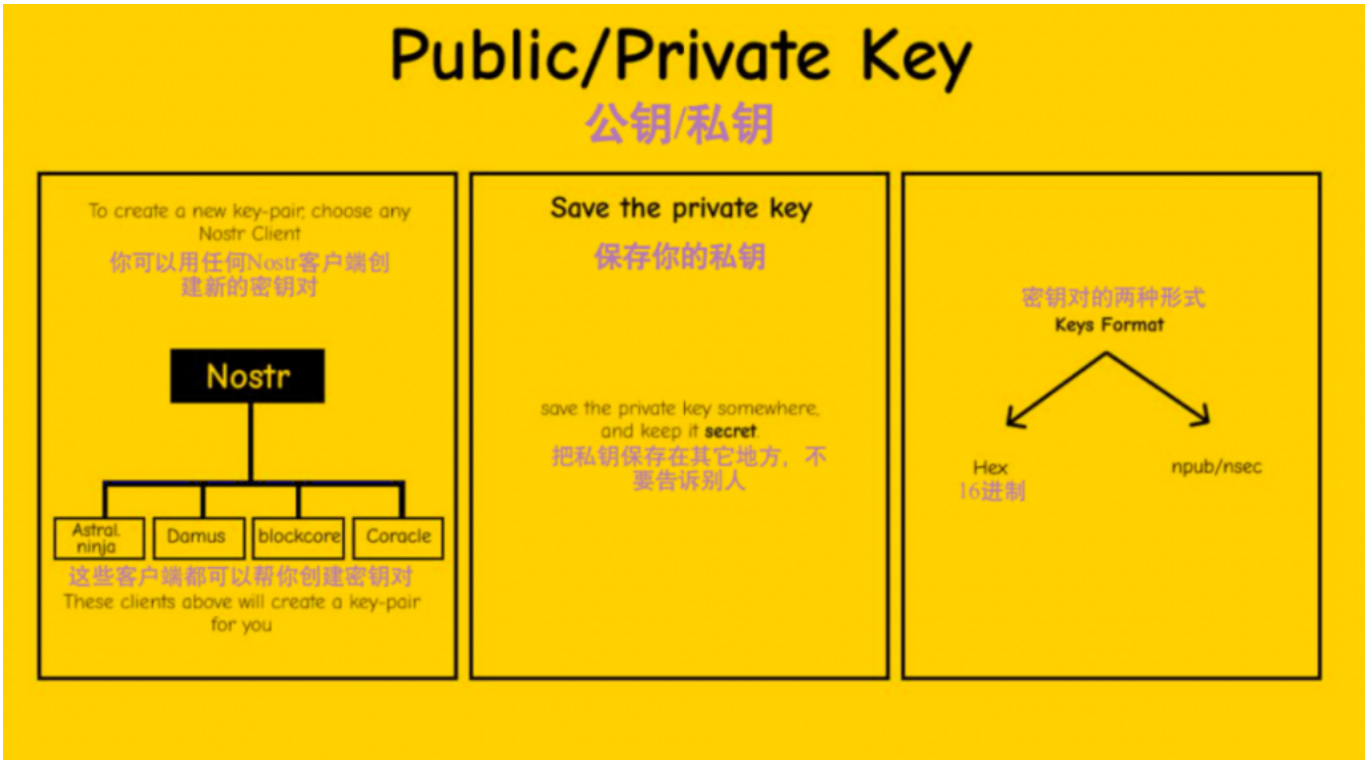
Nostr 協議的特點

Nostr 協議主要有以下 5 個特點：

1、簡單易注冊

任何用戶都可以創建一對公私鑰，無需通過域名或社交帳戶注冊。Nostr的簽名和驗簽算法不是常用

的ECDSA，而是schnorr signature算法，這意味著，如果用戶已經擁有比特幣以太坊的私鑰，那麼是可以用於Nostr網路的，但因為編碼形式的不同，私鑰在不同網路的顯示形式可能有所不同，這個需要做一次轉換。



2、信息傳遞存儲去中心化

不依賴於任何可信任的中心化服務器，且客戶端發布信息可選擇存儲至多個中繼端，因而對單一中繼端依賴更小，也更具有迅速恢複性。

3、降低信任風險

訊息都有公鑰標識，而訊息的驗證由客戶端驗證完成，中繼端只負責存儲、傳輸，用戶無需信任中繼端，這進一步降低了通過Web3錢包進行簽名帶來的信任風險。

4、處理應對垃圾信息

果在Nostr網路中不能刪號封人的話如何對抗那些不良信息呢？Nostr中繼端可以要求用戶為發布付費或其他形式的身份驗證，並將這些在內部與公鑰相關聯，以對抗垃圾信息。如果一個中繼端被用作垃圾信息載體，它很容易會被用戶丟棄，客戶端可以繼續從其他中繼端獲取更新。

5、 與閃電網路的結合：

Nostr的開發者fiatjaf同時也是比特幣和閃電網路的開發者，因而Nostr原生支援閃電網路。閃電網路速度非常快，性能非常強，能夠承載Nostr上的高並發應用。基於Nostr的客戶端Damus內置比特幣閃電網路功能，可以直接調用第三方閃電網路錢包支付。2023年2月3日，Damus表示將通過比特幣閃電網路隨機向用戶發放小額比特幣。

Nostr 協議如何進行操作？

Nostr 的**NIP 是一個雷同於以太坊EIP 提案的機制，而NIP-01 即說明了每個訊息的內容。**

從用戶客戶端的視角出發，可以進行下列操作：

操作1、簽名發布信息：EVENT

用戶想要發布信息時，則是用自己本地客戶端存儲的私鑰，對一串內容`content`做簽名，最終生成如下的`json`類型數據

{

“id”：<結構化數據的哈希值>

“pubkey”: <事件創建者的公鑰>,

“created_at”: <unix 時間戳>,

“kind”：<種類，可理解為頻道>，

“tags”：[

[“e”, <另一個事件的id>, <推薦的中繼器URL>],

[“p”, <推薦的中繼器 URL>],

… // 未來可能會包含其他類型的標籤

],

“content”：<任意字符串，如hello world>，

“sig”: <序列化事件數據的sha256 哈希的64 字節簽名，與”id”字段相同>

}

這裡的id 其實是基於當前內容`[pubkey,created_at,kind,tags,content]`組合後用哈希計算得出的，因為有時間戳的參與，所以正常情況下id 是不會重複的。

操作2、訂閱目標事件：REQ

作為信息傳輸，有來就有回，指令REQ 需要向中繼器發送一個隨機ID 作為訂閱ID，以及一個過濾器信息。目前協議可支持的設定如下，

{

“ids”: <事件ID 的列表>,

“authors”: <公鑰列表，必選項一>,

“kind”：<種類列表，可理解為頻道>，

“#e”：<“e”標籤中引用的事件的ID 列表>，

“#p”：<“p”標籤中引用的公鑰列表>，

“since”: <時間戳，篩選此時間之後的>,

“until”: <時間戳，篩選此時間之前的>,

“limit”: <要返回的最大事件數>

}

從篩選條件來看，基本等同於關注這個功能，既不需要對方許可也能拉取到對方發布的信息（事實上本質都是公開的），而過濾器也只是更好的定義，是誰在什麼時間段，發布的那一條

當然出於中繼器這樣的設計，有可能部分中繼器並沒有存儲目標用戶的信息，那麼用戶需要嘗試從不同的中繼器去拉取，一旦中繼器掛了，甚至全部相關聯的中繼器都掛了，那這塊信息也就損失了。

操作3、結束訂閱：CLOSE

最後一種客戶端能對中繼器發起的信息便是close 指令，即關閉訂閱，那客戶端便不會持續持續獲取到最新的事件信息了。

從技術角度看，此協議使用了訂閱ID 的模式這意味著中繼器會建立起持續的websocket鏈接，一旦此中繼器收到被關注用戶的信息，就會主動向訂閱方的客戶端發起請求來同步，這種模式雖然對中繼器而言負載更高，但同時也能得到實時被關注數這樣的數據，是一種能激勵用戶發布更有價值信息的方式。

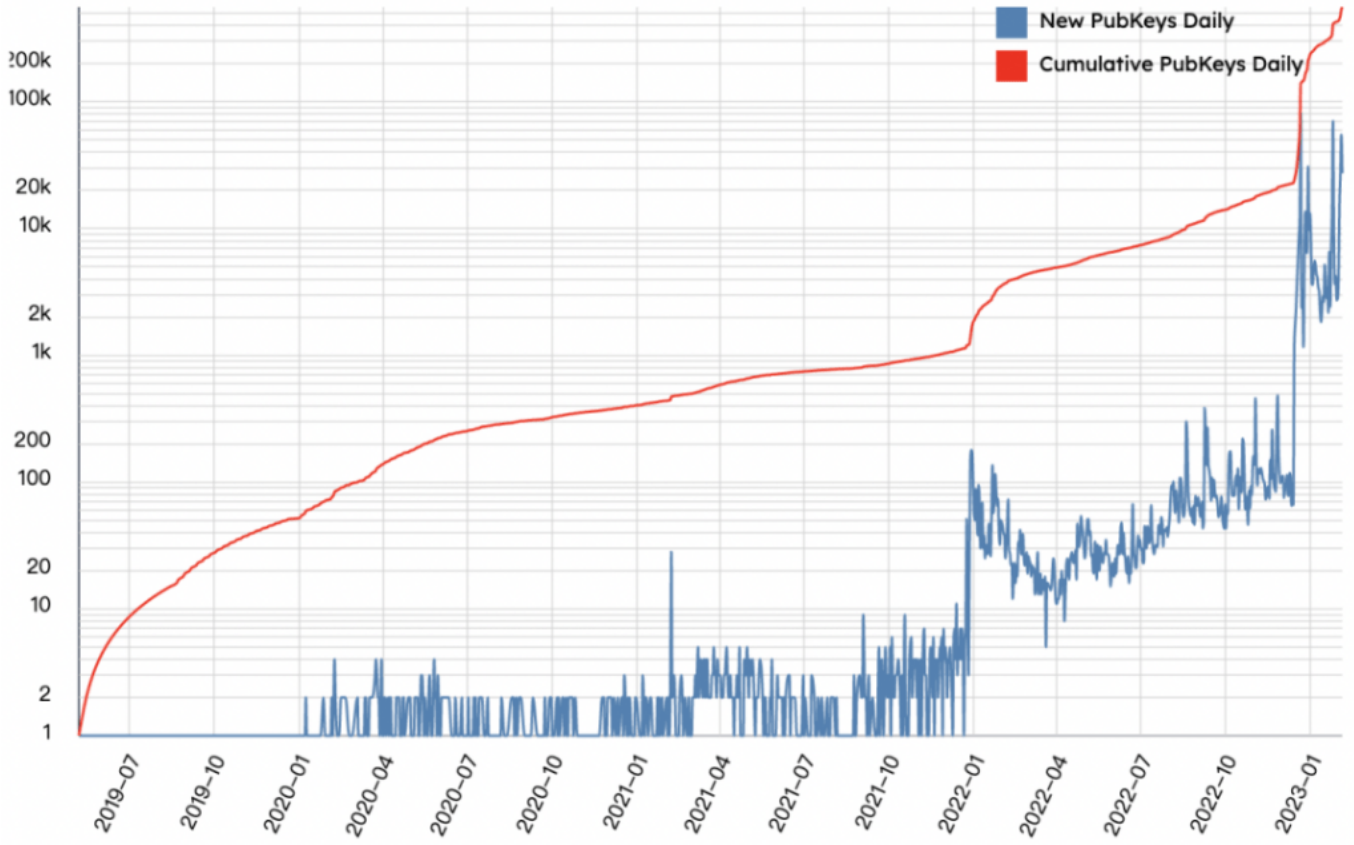
並且協議出現多個「e」、「p」，這類信息雖然並不是必選項，但他能讓各個中繼地址在客戶端之間裂變，傳播，是提升抗審查性的關鍵。

Nostr 協議的表現如何？

1、Nostr 的數據表現

根據nostr.io的數據顯示，截止至2023年2月5日，Nostr的公鑰數量為500, 463，擁有的中繼端為289個，事件（event）超過121萬。Nostr在最初的NIP 01中定義了三種不同的事件類型：

- 0：發送有關用戶的元數據，例如用戶名、圖片、簡介等；
- 1:發送短信和基本內容；
- 2:推薦中繼服務器供關注事件創建者的人連結。



2.Nostr 的生態應用

去中心化的推特是Nostr當前最大的用例，然而其運用遠不止社交產品這麼簡單。現在基於Nostr建立起了類似Telegram的Anigma.io、Reddit的替代品novote、端到端加密文本共享工具Sendtr、在線下棋小遊戲Jeste等等。

Name	Post	Reply	Mentions	Reactions	Delete post	Direct message	Direct message	Create channel	Create channel posts	Post in channel	Reply-in to channel	NIP5
Damus	✅	✅	✅	✅	❌	✅	✅	❌	✅	✅	✅	✅
Nostr console	✅	✅	Partly	✅	✅	✅	✅	✅	✅	✅	✅	✅
More-speech	✅	✅	✅	❌	❌	✅	✅	❌	❌	❌	❌	✅
Astral	✅	✅	✅	❌	❌	✅	✅	❌	❌	❌	❌	✅
Nostroid	✅	✅	✅	❌	❌	✅	✅	❌	❌	❌	❌	✅
Nostros	✅	✅	Not sure	Not sure	❌	❌	❌	❌	❌	❌	❌	Not sure
Anigma	✅	✅	✅	❌	❌	✅	✅	✅	✅	✅	✅	❌
Alphaama	❌	❌	✅	✅	❌	❌	❌	❌	❌	❌	❌	✅
Coracle	✅	✅	❌	✅	❌	❌	❌	✅	✅	✅	❌	❌

Nostr 生態中的 Damus 是什麼？

Damus 是目前 Nostr 協議中最熱門的應用。那麼，Damus 是什麼呢？

1、Damus 是什麼？

Damus是一款基於去中心化社交協議Nostr的應用，其將定位為“The social network you control”，意為用戶可以掌控自己的社交網路，體現了Web3.0強調的精神內核。就產品功能而言，用戶可以在廣場發布內容、發送信息私聊、進行閃電網路支付。

2、Damus 的特色

1. 無需注冊：用戶只需要填寫昵稱，即可生成一對公私鑰而無需使用郵箱等注冊登陸。之後用戶可以基於公鑰搜索關注好友。
2. 用戶所有：具有抗審查的特性，用戶可以控製自己的數據。
3. 加密對話：端到端的私信訊息傳遞。
4. 無需服務器：消息通過分布式的中繼端分發，無需運行任何基礎設施，也沒有單點故障。每一條貼文都有一個獨特的 Note ID，複製之後同樣可以在搜索頁面輸入直達。
5. 可編程：允許輕鬆集成機器人。
6. 可獲取收入：用戶可以運用比特幣閃電網路功能進行支付打賞。當前支持的閃電消費支付平台包括Strike、Cash App、Muun、Blue Wallet、Wallet of Satoshi、Zebedee、Zeus LN、LNLink、Phoenix、Breez、Bitcoin Beach、Blixt Wallet、River。

3、Damus 的表現

2022年12月Twitter創始人Jack向Nostr捐贈了14.17枚BTC（約合 245,000 美元），以進一步資助Nostr的開發。

2023年2月1日，Jack發布了關於Damus在蘋果應用商店和Google Play上架的消息，之後瞬間引爆了，僅半小時，Damus的用戶增加了近10萬。

個人認為，除了是Jack的名人效應之外，Damus出圈的原因還在於，之前不論是去中心化協議層還是應用層都有新項目產生，但由於協議層離C端用戶較遠，不利於理解，而應用層有規模效應的又不多，所以大部分人對去中心化社交如何落地，始終都是處於既期待又迷惑的狀態的，因而移動端去中心化產品Damus的出現便是將大家的期望具像化了。

4、Damus 的產品體驗

從功能上來說，Damus並沒有太多地突破用戶的想象，當前也仍然是一個亟待優化的初級版本，很多功能任然不完善，比如內容編輯頁面不可進行排版、點讚後不能取消、發布內容無法刪除等，但其進入門檻低，且擁有移動端，用戶可以輕鬆下載使用。Damus主打的用戶所有、加密對話、閃電網支付等概念啟發了用戶以及加密社區的討論。

5、Damus 的未來如何？

不論是之前Aave創始人開發的Lens Protocol還是現在Jack力挺的Damus，似乎社交產品的爆火都離不開行業內有影響力的人群的「喊單」，然而由於用戶的社交產品使用習慣較為固化，且用戶數據難以遷移，使得大部分新興的社交產品都隻是曇花一現，如何留住用戶依然是一個非常難的問題。即便做去中心化社交是一件不容易的事，好在Damus相對順利地完成了冷啟動，獲得了大量的關注度。就現在的發帖內容來看，中文用戶非常活躍，大家也自發地組織了各種交流社群。

Nostr 的野心：不止替代 Twitter

那麼，Nostr 僅僅就是想做個去中心化的 Twitter 嗎?

1、替代 Twitter

為達到替代 Twitter 的目的，客戶端利用了第 1 類的事件，即純文本筆記。一些客戶端包括：coracle, astral, nostr.ch, branle, damus, alphaama.com, Nostros 等等

- **比如 Damus, 就是替代 Twitter 的創造**

2、替代 Telegram

通過使用 4X（X 是 0 到 9 之間的數字），可以實現像 Telegram 那樣的公共頻道，比如上面主頁的 Anigma.io 是實現 Telegram 克隆的網路應用。你可以創建公共頻道，任何人都可以加入並聊天。在 anigma 中，可以向用戶發送私人的端到端加密訊息。

3、替代 Reddit

Nostr 也可以作為 Reddit 的替代品，可以發布帖子，用戶可以對這些帖子投票，比如上面網站大圖的 nvote。

4、 在線遊戲

nostr 的另一個有趣的用途是創建簡單的多人在線遊戲，比如 Jeste，在這個平台上，你可以通過 Nostr 與其他用戶在線下棋。

5、文本共享

Sendstr 是一個在線工具，你可以通過 nostr 協議在兩個設備之間分享端到端的加密文本數據。

Nostr 協議目前存在哪些問題？

1、中繼端激勵問題

雖然任何人都可以建立中繼端，但目前全球隻有200+公開的中繼端，因為搭建是存在門檻的，需要較好的處理性能和網路，同時也需要一定的技術和運維能力，但是中繼端缺乏收益，因而如何吸引更多的中繼端加入是個問題，如果基礎設施建立在脆弱的「自願主義」基礎上，則難以壯大為一個強大的社交網路。

然而，如果有激勵，則會面臨著，大部分激勵將逐漸掌握在少數人手裡，無法形成有效激勵，且容易受到攻擊的困境。針對運行中繼器激勵的問題，開發者認為，首先不應假設中繼器的運營者會無償服務，即便沒有所謂的「激勵」，p2p網路中的DHT節點仍然在持續運營。

2、社交隱私問題

目前的Nostr 中繼器只是簡單JSON 數據的轉儲。客戶端通過過濾器獲取。這使得nostr 成為客戶端之間的通用數據共享平台，那對於有隱私信息傳遞需求的場景而言，如何解決呢？畢竟即使是推特這樣的社交廣場也會有私信的需求存在。

目前較優的解決方案是，DH 算法（**迪菲- 赫爾曼密鑰交換**），這套1976 年問世的算法。它是第一個實用的在非保護信道中創建共享密鑰方法。只要得到共享密鑰，使用Nostr的雙方均可以發布加密後的信息，從而實現點對點的隱私通信。由於隱私常有閱後即焚的訴求，所以其中的服務器存儲成本還能進一步降低。

3、抗DOS 問題

會受到攻擊的是中繼器這一層，目前Nostr 協議並不直接指導和確定如何讓中繼器抗擊DOS 攻擊和垃圾信息，因此也是眾多中繼器實現的重點。

4、Nostr 的存儲問題

目前數據主要存儲在中繼端上，但這並不是永久存儲，用戶一旦更換客戶端，信息就清除了。中繼端用於缺乏激勵，沒有足夠的動力來為用戶數據進行存儲，因而也存在著中繼端主動或者被動刪除數據的可能。未來Nostr或可以針對存儲功能提供激勵，在確保去中心化和易用性的同時，使得數據更加具有可得性。

Nostr 協議的發展展望

總體來說，Nostr是一個非常簡單且具有高度互操作性的協議，其呈現了去中心化社交協議與自由的價值傳遞交織後湧現的可能性。客戶端和中繼端的組合，使得信息的發布和傳遞更加具有抗審查性，這與比特幣倡導的精神內核相吻合。

Nostr算是為去中心化社交新打開了一扇窗，自此之後，相信大規模的協議以及應用會迎來新的突破。
