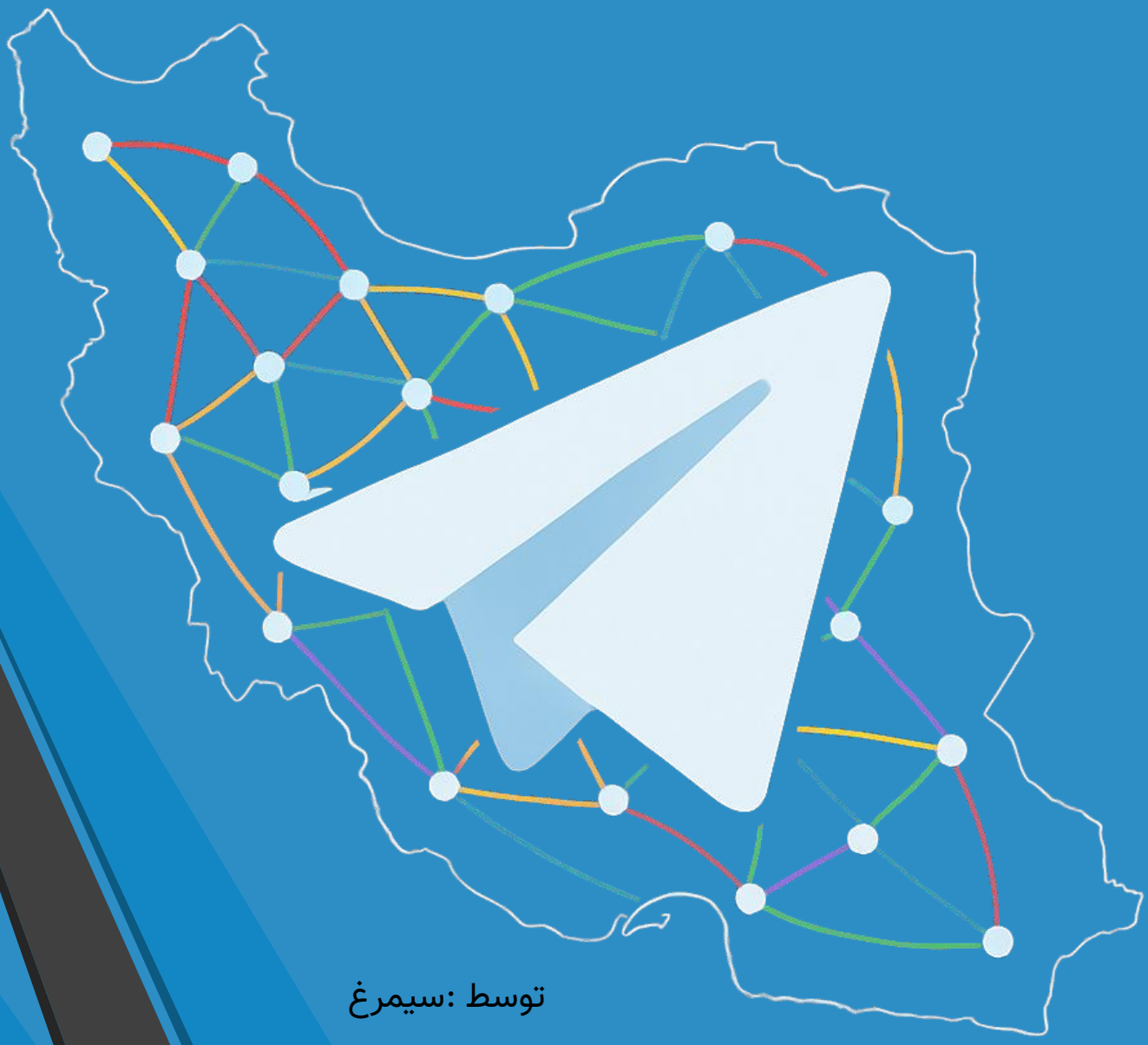
رسالهٔ یک شبکه (ویرایش ۳)

پروتکل آگورا برای گفت‌وگوی ملی امن، ناشناس و مقیاس‌پذیر



توسط :سیمرغ

شهریور ۱۴۰۴

چکیده

رژیم‌های خودکامه با تفرقه‌افکنی سیستماتیک میان مخالفان و ساکت کردن مردم، به بقای خود ادامه می‌دهند و بحران «صداهای گسسته» را ایجاد می‌کنند که در آن شهروندان احساس انزوا و ناتوانی می‌کنند. این واقعیت کنونی در کشورهایی مانند ایران است که در آن، جنبش‌های آزادی‌خواهانه به عمد و با ایجاد نفاق، تضعیف می‌شوند. این مقاله یک راه حل فناورانه برای این مشکل ارائه می‌دهد: **پروتکل آگورا**، سیستمی برای گفت‌وگوی ملی امن، ناشناس و مقیاس‌پذیر که برای ادغام با پلتفرمی پرکاربرد مانند تلگرام طراحی شده است.

این پروتکل یک فرآیند گفت‌وگوی امن، ناشناس و چندمرحله‌ای را ایجاد می‌کند که در آن شهروندان می‌توانند در مورد مسائل مبرم ملی بحث و رأی‌گیری کنند. از طریق یک سیستم پالایش شایسته‌سالار، طنین‌اندازترین و منطقی‌ترین ایده‌ها به صدر می‌رسند و در نهایت به یک اجماع ملی می‌انجامند که برای همهٔ شرکت‌کنندگان، شفاف و قابل مشاهده است. این پروتکل به طرز چشمگیری کارآمد است و قادر است دیدگاه‌های جمعیتی **۱۰۰ میلیون نفری** را در **شش هفته** به یک گروه اصلی ۱۰۰ نفره تبدیل کند .این ابزار نه تنها برای پر کردن شکاف‌های داخلی در میان مردم، بلکه برای ارائهٔ یک سنجش شفاف و داده‌محور از ارادهٔ واقعی مردم طراحی شده است تا آنها را برای حرکت به جلو با اتحاد و حس هدف مشترک، توانمند سازد.

این سند به تشریح مکانیک پروتکل، ویژگی‌های ایمنی قوی آن، مقاومت ذاتی آن در برابر دستکاری، و یک استراتژی دقیق و چندمرحله‌ای برای یک راه‌اندازی عمومی امن و عادلانه می‌پردازد. این سند به عنوان یک یادداشت مفهومی و نقشه راه فنی عمل می‌کند؛ مشخصات دقیق پیاده‌سازی و اثبات‌های امنیتی قبل از هر برنامه آزمایشی به صورت جداگانه منتشر خواهد شد.

۱. مسئله: بحران صداهای گسسته

در پی تحولات اجتماعی بزرگ، مانند جنبش «زن، زندگی، آزادی» در ایران، یک آسیب‌پذیری حیاتی برای شهروندانِ خواهان تغییر پدیدار می‌شود: از هم گسیختگی صدای جمعی آنها. دولت‌های خودکامه در استراتژی «تفرقه بینداز و حکومت کن» نه در میدان جنگ، بلکه در عرصه‌های دیجیتال و اجتماعی به استادی رسیده‌اند. آنها اختلافات جزئی میان گروه‌های مخالف را بزرگ‌نمایی و تشدید می‌کنند، با کمپین‌های اطلاعات نادرست بذر بی‌اعتمادی می‌پاشند و فضایی از ترس را حاکم می‌کنند که در آن، گفتمانِ آزاد، خطرناک است.

نتیجه، جمعیتی است که احساس انزوا و درماندگی می‌کند. افراد، حتی زمانی که اهداف بنیادین یکسانی دارند، قادر به برقراری ارتباط در مقیاس بزرگ برای کشف وجوه مشترک خود نیستند. آنها نمی‌دانند هموطنانشان واقعاً به چه چیزی فکر می‌کنند، اولویت‌هایشان چیست، یا از چه راه‌حل‌هایی ممکن است حمایت کنند. این فقدان بافت ارتباطی به یک اقلیت در قدرت اجازه می‌دهد تا اکثریتی از هم گسسته را کنترل کند. هر مسیر معناداری به جلو، نیازمند راه حلی برای این مشکل بنیادین است: نبود فضایی امن و مورد اعتماد برای آنکه یک ملت بتواند با خودش صحبت کند.

۲. فرصت: بهره‌گیری از شبکه‌های موجود برای تغییر

در حالی که این چالش، عظیم است، یک فرصت منحصر به فرد در زیرساخت دیجیتالی که مردم از قبل از آن استفاده کرده و به آن اعتماد دارند، وجود دارد. در ایران و بسیاری از کشورهای دیگر با دسترسی محدود به اینترنت، تلگرام ثابت کرده است که یک پلتفرم منحصراً مقاوم و محبوب است. با ویژگی‌های قوی ضد سانسور و تعهد به حریم خصوصی کاربران، این پلتفرم عملاً به یک فضای عمومی اجتماعی برای میلیون‌ها نفر تبدیل شده است.

این شبکهٔ موجود و مورد اعتماد، پایه‌ای ایده‌آل برای ساختن یک راه‌حل است. ما نیازی نداریم میلیون‌ها نفر را متقاعد کنیم که به یک اپلیکیشن جدید و ناشناخته بپیوندند. ما فقط باید ابزاری جدید در همان محیطی که آن‌ها از قبل در آن حضور دارند، در اختیارشان قرار دهیم. چالش، ساختن یک جامعه از صفر نیست، بلکه فراهم کردن یک انجمنِ امن و ساختارمند برای جامعه‌ای است که از قبل وجود دارد.

۳. راه حل: رسالهٔ یک شبکه

برای حل بحران صداهای گسسته، ما یک ویژگی جدید و یکپارچه برای تلگرام را پیشنهاد می‌کنیم: یک سیستم گفت‌وگوی ساختارمند که بر سه اصل بنیادی استوار است:

ناشناسی ساختاری

فرآیند ساختارمند

ارتقای شایسته‌سالار

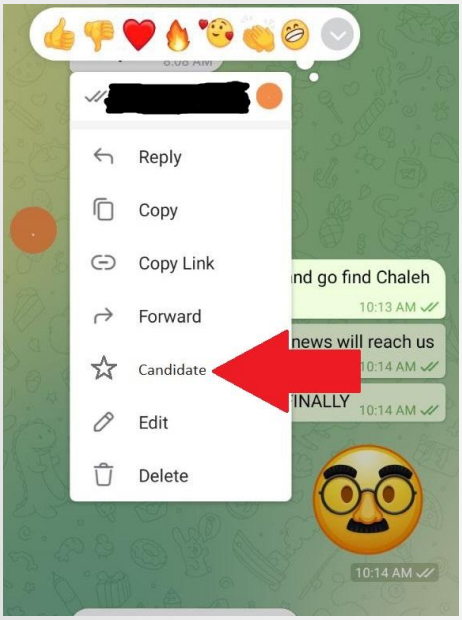
۳٫۱. فرآیند: از گفتگو تا اجماع

این سامانه در چرخه‌های دو-ماهانه (هر دو ماه یک‌بار) عمل می‌کند و یک جمعیت بزرگ را از طریق یک قیفِ گفتگو هدایت می‌کند.

- **مرحلهٔ ۱: آغاز.** در ابتدای هر چرخه، هر کاربری می‌تواند وارد «حالت کشور» در تلگرام شود. به هر کس یک آواتار و پروفایل ناشناس و تصادفی اختصاص داده می‌شود که کاملاً از هویت شخصی‌شان جداست. سپس در یک گروه سطح ۱ صد نفره که به صورت تصادفی تعیین شده، قرار می‌گیرند.
- **مرحلهٔ ۲: گفتگو (۷ روز).** به مدت یک هفته، ۱۰۰ عضو هر گروه می‌توانند در مورد هر موضوعی با اهمیت ملی بحث کنند. گفتگو در داخل گروهِ عمومی است و هیچ پیام خصوصی مجاز نیست تا اطمینان حاصل شود که تمام ارتباطات شفاف است.
- **مرحلهٔ ۳: نامزدی.** در طول هفته، هر عضوی می‌تواند یکی از پیام‌های خود را به عنوان «پیام نامزد» علامت‌گذاری کند. این پیام باید مهم‌ترین ایده یا پیشنهاد او را در بر گیرد. پیام برای همه پین (pin) شده و قابل ویرایش نیست.
- **مرحلهٔ ۴: رأی‌گیری و ارتقا.** در طول هفته، اعضا تعداد محدودی رأی (مثلاً ۵ رأی برای هر کاربر) به پیام‌های نامزدی که به نظرشان ضروری‌تر و منطقی‌تر است، می‌دهند. در پایان ۷ روز، ۱۰ پیامی که بیشترین رأی را کسب کرده‌اند به عنوان «ایده‌های برنده» اعلام شده و نویسندگان آن‌ها به طور خودکار به یک گروه سطح ۲ برای هفتهٔ بعد ارتقا می‌یابند. تمام گروه‌های سطح ۱ پس از آن منحل می‌شوند.

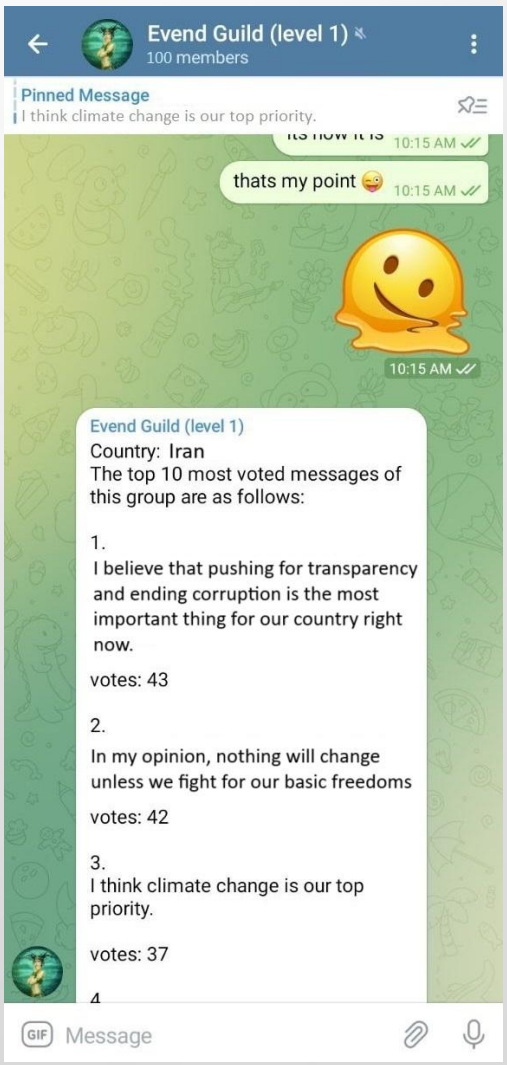
  - **شکستن آراء مساوی:** در صورت تساوی آراء برای آخرین جایگاه‌های صعود، یک رأی‌گیری دور دوم ۲۴ ساعته فقط میان نامزدهای مساوی برگزار می‌شود تا برندگان مشخص شوند.

۳٫۲. قیفِ پالایش



این فرآیند تکرار می‌شود. گروه‌های سطح ۲ از برندگان گروه‌های مختلف سطح ۱ تشکیل شده‌اند. آن‌ها دوباره ۷ روز فرصت دارند تا گفتگو و رأی‌گیری کنند. ۱۰ نفر برتر از هر گروه سطح ۲ به سطح ۳ صعود می‌کنند.

این روند تا زمانی ادامه می‌یابد که فرآیند به یک «گروه نهایی» متشکل از حداکثر ۱۰۰ شرکت‌کننده برسد که با موفقیت از چندین دور ارزیابی توسط همتایان خود عبور کرده‌اند.



۳٫۳. مرحلهٔ نهایی: شفافیت ملی

گروه نهایی منحصر به فرد است. بحث‌های آن برای هر کسی که در هر سطحی از فرآیند آن چرخه شرکت کرده، قابل مشاهده است. در پایان هفتهٔ نهایی، ۱۰ ایدهٔ برتر از این گروه می‌تواند به رأی‌گیری گسترده‌تری گذاشته شود (با تدابیر امنیتی که در بخش‌های بعدی بحث شده) و سپس به عنوان طنین‌اندازترین پیشنهادهای آن چرخه به صورت عمومی اعلام می‌شود. این گروه همچنین برای رسیدگی به بحران‌های فوری و اضطراریِ ملی، فعال باقی می‌ماند.

۳٫۴. قوانین پلتفرم و ایمنی

برای تضمین یک محیط امن و مدنی متمرکز بر بحث‌های محتوایی، قوانین زیر در گروه‌های پروتکل، اجرا می‌شود:

- **ارتباط فقط متنی:** برای جلوگیری از آزار و اذیت و حفظ تمرکز بر استدلال، هیچ فایلی (تصویر، ویدئو، صدا)، گیف یا استیکری مجاز نیست.
- **عدم ارسال لینک (در مراحل اولیه):** برای تضمین امنیت و جلوگیری از فیشینگ، لینک‌های خارجی در گروه‌های سطح ۱ غیرفعال هستند. یک سیستم اشتراک‌گذاری لینک «لیست سفید» ممکن است برای شرکت‌کنندگان در سطوح بالاتر فعال شود.
- **ایموجی‌های گزینش‌شده:** فقط لیست از پیش تأیید شده‌ای از ایموجی‌ها که برای بیان احساسات و نظرات هستند، در دسترس خواهد بود.
- **فیلتر کلمات نامناسب:** یک فیلتر خودکار، پیام‌های حاوی الفاظ رکیک را مسدود کرده و به فرستنده اطلاع می‌دهد تا یک سطح پایه از گفتمان مدنی تضمین شود.

۳٫۵. ویژگی‌های سلامت سیستم

برای اطمینان از عدالت و تمرکز، دو ویژگیِ دیگر، حیاتی هستند:

- **جلوگیری از تبانی:** هیچ قابلیت پیام خصوصی در این سیستم وجود ندارد. تمام ارتباطات در گروهِ ۱۰۰ نفره انجام می‌شود.
- **انسجام ایدئولوژیک:** در تمام سطوحِ بالاتر از سطح ۱، برای هر عضو، «پیام‌های نامزد» گروه‌هایِ پیشینَش، در پروفایل ناشناسِ او قابل مشاهده است. این به سایر اعضا اجازه می‌دهدَ تا انسجام و پیوستگیِ ایده‌های او را ارزیابی کنند، که به عنوان یک دفاع قدرتمند در برابر پوپولیسم و استدلال‌های بدخواهانه عمل می‌کند.

۳٫۶. مقیاس‌پذیری و کارایی بی‌سابقه

ساختار لایه‌ای و قیف‌مانندِ این پروتکل به آن اجازه می‌دهد تا با سرعتی چشمگیر به مقیاس یک ملتِ کامل برسد. نگاهی به ریاضیاتِ این فرآیند، خالی از لطف نیست: حتی اگر ۱۰۰ میلیون کاربر شرکت کنند، سیستم تنها به یک فرآیند شش مرحله‌ای برای رسیدن به یک گروه نهایی ۱۰۰ نفره نیاز دارد.

- هفتهٔ ۱: ۱۰۰ میلیون کاربر -> ۱ میلیون گروه سطح ۱
- هفتهٔ ۲: ۱۰ میلیون کاربر --> ۱۰۰ هزار گروه سطح ۲
- هفتهٔ ۳: ۱ میلیون کاربر ---> ۱۰ هزار گروه سطح ۳
- هفتهٔ ۴: ۱۰۰ هزار کاربر ----> ۱ هزار گروه سطح ۴
- هفتهٔ ۵: ۱۰ هزار کاربر -----> ۱۰۰ گروه سطح ۵
- هفتهٔ ۶: ۱ هزار کاربر --------> ۱۰ گروه سطح ۶
- هفتهٔ ۷: ۱۰۰ کاربر ----------> ۱ گروه نهایی

این نشان می‌دهد که این پروتکل یک تمرین نظری نیست، بلکه یک چارچوب قابل اجرا است که قادر به مدیریت یک گفت‌وگوی سراسری به شیوه‌ای معین و به موقع است.

۴. ایمن‌سازی پروتکل: یک دفاع چندلایه

۴.۱. آسیب‌پذیری: ایمن‌سازی سطح ۱ در برابر حملات سیبیل (Sybil). بزرگترین آسیب‌پذیری پروتکل در مرحلهٔ اولیهٔ آن نهفته است. سیاست «درهای باز» که برای تشویق مشارکت انبوه طراحی شده، می‌تواند توسط یک عامل دولتی با استفاده از حملهٔ سیبیل برای پر کردن گروه‌های سطح ۱ با ربات‌های خودکار، مورد سوءاستفاده قرار گیرد. این ربات‌ها، اگرچه تصادفی توزیع شده‌اند، می‌توانند با تعداد زیاد خود، رأی‌گیری را تحت سلطه درآورده و تعداد کمی از حساب‌های «دست‌نشاندهٔ» انسانی را به مراحل بالاتر برسانند و سیستم را از همان ابتدا به خطر بیندازند.

- **راه حل: تأیید هویت پیش‌رونده با رأی‌گیری وزن‌دار.** این راه حل، سطح ۱ را بدون ایجاد مانع اجباری برای ورود، ایمن می‌سازد و تمرکز را از جلوگیری از ورود به کاهش نفوذ عاملان تأیید نشده تغییر می‌دهد.
- **دسترسی پایه:** هر کاربری می‌تواند با حداقل موانع (مانند عبور از یک بررسی تشخیص ربات (مانند Turnstile کلادفلر یا reCAPTCHA v3 گوگل) و داشتن حساب تلگرام با عمر مشخص) به یک گروه سطح ۱ بپیوندد. به طور پیش‌فرض، هر شرکت‌کننده ۱ رأی دریافت می‌کند.
- **تأیید هویت تشویقی:** به کاربران این گزینه داده می‌شود که هویت یکتای خود را از طریق یک روش معتبر قبل یا در طول چرخهٔ سطح ۱ تأیید کنند. پس از تأیید موفقیت‌آمیز، قدرت رأی آن‌ها به طور قابل توجهی (مثلاً از ۱ به ۵ رأی) افزایش می‌یابد.
- **تأثیر:** این مدل، حملات سیبیل را به شدت پرهزینه می‌کند، زیرا یک مهاجم برای مقابله با نفوذ یک انسان تأیید شده به پنج ربات که بتوانند از مرحلهٔ اول تشخیص ربات عبور کنند، نیاز دارد. این یک انگیزهٔ قدرتمند برای کاربران ایجاد می‌کند تا برای حفاظت از یکپارچگی نتایج گروه خود، هویتشان را تأیید کنند.

۴. ایمن‌سازی پروتکل:
یک دفاع چندلایه (ادامه)

۴.۲. مسیرهای تأیید هویت. یک رویکرد چندجانبه برای ایجاد یک شبکهٔ مورد اطمینان به کار گرفته خواهد شد:

- **اثبات شخص بودن (PoP):** سیستم در ابتدا به سرویس‌های غیرمتمرکز PoP (مانند BrightID، Proof of Humanity یا Worldcoin) برای ایجاد اولین گروه از کاربران معتمد و تأیید شده، تکیه خواهد کرد.
- **تأیید اجتماعی:** پس از چند چرخه، یک سیستم تأیید اجتماعی فعال می‌شود که در آن کاربران جدید می‌توانند توسط چندین کاربر تأیید شدهٔ قبلی «تأیید» شوند.
- **سابقه در سیستم:** یک مسیر بلندمدت که در آن کاربران می‌توانند بر اساس سابقهٔ مشارکت خیرخواهانه در چرخه‌های متعدد، وضعیت تأیید شده را کسب کنند.

۴.۳. مقابله با هماهنگی خارج از پلتفرم. یک چالش اصلی، جلوگیری از هماهنگی کاربران برای رأی‌گیری در گروه‌های خصوصی خارجی است. برای مقابله با این موضوع، پروتکل از **پنهان‌سازی ساختاری** استفاده خواهد کرد:

- **شناسه‌های یکتا و غیرقابل جستجو:** به هر کاربر و گروه، یک شناسهٔ یکتا اما تصادفی و غیرعمومی اختصاص داده می‌شود (مثلاً گروه «شاهین سرخ»، کاربر «شرکت‌کننده-XJ48») این شناسه‌ها برای انسجام درون گروهی و نظارت ضروری هستند اما از خارج از سیستم قابل جستجو یا کشف نیستند، که این امر یافتن و تبانی با شرکت‌کنندگان خاص را بسیار دشوار می‌کند.

۴. ایمن‌سازی پروتکل: یک دفاع چندلایه (ادامه)

۴.۴. گمنامی پیشرفته و حفاظت از فراداده برنامه‌ریزی‌شده. فراتر از نام کاربر، «اثر انگشت» دیجیتال یا فرادادهٔ او (مانند زمان‌بندی پست‌ها، سبک نگارش) می‌تواند ریسک ایجاد کند. برای محافظت از شرکت‌کنندگان پرخطر، نسخه‌های آیندهٔ پروتکل باید شامل حفاظت‌های پیشرفته باشند:

- **ناشناس‌سازی ترافیک:** سازگاری با شبکه‌های حافظ حریم خصوصی مانند Tor (مسیریابی پیازی) یا میکس‌نت‌ها برای پنهان کردن آدرس IP و موقعیت کاربر.
- **لرزش زمانی (Timestamp Jitter):** ایجاد تأخیرهای کوچک و تصادفی (چند ثانیه تا یک دقیقه) در زمان‌بندی ارسال پست‌ها برای مختل کردن تحلیل الگو توسط ناظران خارجی، بدون آسیب رساندن به جریان گفتگو.

۴.۵. ملاحظات پیشرفته و نقشه راه فنی. حرکت از یک چارچوب مفهومی به یک پروتکل آمادهٔ پیاده‌سازی نیازمند رسیدگی به چالش‌های فنی پیشرفته است. پروتکل آگورا متعهد به رویارویی با این چالش‌ها با راه‌حل‌های پیشرفته است:

- **مدل تهدید رسمی (Formal Threat Model):** پروتکل توسط یک مدل تهدید رسمی تعریف خواهد شد که طیف گسترده‌ای از حملات، از جمله اجبار، تبانی و تحلیل ترافیک را در بر می‌گیرد و ویژگی‌های خاصی از حریم خصوصی، قابلیت تأیید و پویایی را تضمین می‌کند.

۴. ایمن‌سازی پروتکل: یک دفاع چندلایه (ادامه)

- **طرح رأی‌گیری رمزنگاری‌شده:** مکانیسم رأی‌گیری توسط یک روش شمارش آرای رمزنگاری‌شدهٔ خصوصی، قابل تأیید و مقاوم در برابر اجبار (مثلاً با استفاده از رمزنگاری آستانه‌ای و اثبات با دانش صفر برای شمارش صحیح) ایمن خواهد شد تا اطمینان حاصل شود که آراء هم محرمانه و هم به طور قابل اثبات دقیق هستند.
- **استقلال از پلتفرم:** در حالی که هدف اصلی یکپارچه‌سازی با یک پلتفرم بزرگ است، بهتر است طرح ب (مینی-اپ) برای استقلال از پلتفرم طراحی شود و از روش‌های احراز هویت جایگزین (مانند WebAuthn) که به APIهای سفارشی از یک پلتفرم میزبان نیاز ندارند، استفاده کند.
- **نظارت و مقیاس‌پذیری:** مکانیک‌های عملیاتی در یک مشخصات جداگانه با جزئیات شرح داده خواهد شد، از جمله اهداف توان عملیاتی، محدودیت‌های نرخ، سقف پیام‌های نامزد شده و pipeline خلاصه‌سازی شفاف و قابل حسابرسی برای مدیریت گفتگو در مقیاس ملی.
- **پذیرش عادلانه:** فرآیند دعوت تصادفی از تکنیک‌های نمونه‌گیری طبقه‌بندی‌شده برای اطمینان از اینکه گروه‌های شرکت‌کنندهٔ اولیه از نظر جمعیتی نماینده هستند و برای کاهش سوگیری انتخاب، استفاده خواهد کرد.

۵. پیاده‌سازی:
یک استراتژی دو مسیره

موفقیت پروتکل نباید به یک نتیجهٔ واحد وابسته باشد. بنابراین، ما یک استراتژی دو مسیره را برای انعطاف‌پذیر کردن پروژه دنبال خواهیم کرد.

طرح آ: پیشنهاد یکپارچه‌سازی بومی (هدف اصلی). استراتژی اصلی، ادامهٔ تلاش برای همکاری مستقیم با تلگرام برای ساخت پروتکل به عنوان یک ویژگی بومی است. این بهترین تجربهٔ کاربری و سریع‌ترین مسیر برای پذیرش انبوه را فراهم می‌کند.

طرح ب: یک مینی-اپ قوی، امن و غیرمتمرکز (طرح جایگزین): به طور همزمان، ما یک مینی-اپ پیچیده را طراحی خواهیم کرد که به منابع توسعهٔ مستقیم تلگرام وابسته نیست. اصول معماری کلیدی آن عبارتند از:

- **بک‌اند (backend) غیرمتمرکز:** منطق برنامه و سوابق رأی‌گیری بر روی یک شبکهٔ عمومی و غیرمتمرکز (مانند یک بلاکچین) برای شفافیت و مقاومت در برابر سانسور، عمل خواهد کرد.
- **پل احراز هویت ناشناس:** طراحی، یک پل احراز هویت ناشناس با استفاده از **اثبات با دانش صفر** را مشخص می‌کند. اگر پلتفرم میزبان چنین API را ارائه ندهد، سیستم به روش‌های مستقل از پلتفرم، مانند کلیدهای مبتنی بر دستگاه از طریق WebAuthn، باز خواهد گشت. این به مینی-اپ اجازه می‌دهد تا مشروعیت یک کاربر را بدون آنکه تلگرام شناسهٔ کاربر را فاش کند، تأیید کرده و گمنامی در طراحی را حفظ کند.
- **هویت خودگردان:** هویت ناشناس هر کاربر توسط یک کلید رمزنگاری شده در دستگاه خودشان کنترل می‌شود که می‌تواند به دستگاه‌های دیگر خودشان کپی شود و به آنها مالکیت کامل و مستقل از توسعه‌دهندگان یا تلگرام را می‌دهد.

۶. حاکمیت بلندمدت: پروتکلی برای مردم

آسیب‌پذیری: کنترل متمرکز بلندمدت. طراحی اولیهٔ پروتکل باید جای خود را به یک مدل حاکمیت غیرمتمرکز و جامعه‌محور بدهد تا سلامت و مشروعیت بلندمدت آن تضمین شود. برای جلوگیری از خطر تسخیر حاکمیت توسط یک گروه نخبهٔ کوچک، پروتکل توسط یک **DAO دومجلسی** —سیستمی با دو مجلس که برای کنترل و توازن طراحی شده است— اداره خواهد شد.

مجلس اول: «شورای اجماع»

- **ترکیب:** متشکل از اعضایی که با موفقیت به «گروه نهایی» یک چرخه رسیده‌اند و توانایی خود را در ایجاد اجماع به اثبات رسانده‌اند.
- **وظایف:** ایفای نقش به عنوان مباشران فنی، رأی‌گیری در مورد ارتقاءهای پیچیدهٔ پروتکل، تغییرات در مکانیک‌های اصلی (مانند الگوریتم رأی‌گیری)، و پارامترهای امنیتی برای یک دورهٔ محدود (مثلاً ۶ ماه).

مجلس دوم: «مجمع شهروندان»

- **ترکیب:** یک هیئت بزرگتر (مثلاً ۱۰۰۰ عضو) که به صورت تصادفی از میان تمام شرکت‌کنندگان فعال در تمام سطوح پروتکل نمونه‌گیری شده است.
- **وظایف:** نمایندگی «ارادهٔ مردم»، رأی‌گیری در مورد سیاست‌های جامعه، قوانین نظارتی و منشور عمومی پروژه برای یک دورهٔ کوتاه‌تر (مثلاً ۳ ماه).

۶. حاکمیت بلندمدت:
پروتکلی برای مردم (ادامه)

کنترل و توازن

برای تصویب یک تغییر بزرگ در پروتکل، به طور معمول باید توسط متخصص‌های شورای اجماع پیشنهاد و توسط مجمع شهروندان تصویب شود. این ساختار تضمین می‌کند که پروتکل هم توسط دانش عمیق سیستمی و هم توسط ارادهٔ گسترده‌تر جامعه‌ای که به آن خدمت می‌کند، هدایت می‌شود. این مدل، سازندگان پروتکل را از حاکمان دائمی به مباشران اولیه تبدیل کرده و یک مسیر روشن برای واگذاری کنترل به جامعه را فراهم می‌کند.

۷. استراتژی راه‌اندازی و پذیرش

برای حل «مشکل شروع کار» یعنی رسیدن به تعداد کاربران کافی بدون آسیب‌پذیری در برابر دستکاری اولیه، ما یک استراتژی راه‌اندازی چندمرحله‌ای با تسهیل‌گری تلگرام را پیشنهاد می‌کنیم.

- **مرحله ۱: کمپین آگاهی‌بخشی (دو هفته پیش از شروع):** تلگرام ویژگی «حالت کشور» را از طریق کانال‌های رسمی خود برای ایجاد هیجان و مشروعیت اعلام می‌کند.
- **مرحله ۲: فرآیند دعوت (یک هفته قبل از شروع):** تلگرام تعداد زیادی **دعوت‌نامهٔ تصادفی و غیرقابل انتقال** را از طریق پیام‌های امن درون‌برنامه‌ای برای کاربران یک کشور هدف ارسال می‌کند. به دعوت‌شدگان چند روز فرصت داده می‌شود تا دعوت را بپذیرند. اگر نرخ پذیرش پایین باشد، موج دومی از دعوت‌نامه‌های تصادفی برای رسیدن به تعداد هدف شرکت‌کنندگان اولیه (مثلاً ۱۰۰،۰۰۰ نفر) ارسال می‌شود.
- **مرحله ۳: فاز بلوغ عمومی (۶ ماه):** پروتکل برای شش ماه با چرخه‌های ماهانه راه‌اندازی می‌شود و عموم مردم می‌توانند بحث‌ها را تماشا کنند تا یک فرهنگ گفتگوی اندیشمندانه به طور طبیعی توسعه یابد و به عموم مردم فرصت می‌دهد تا با هنجارهای سیستم آشنا شوند.

۸. تأثیر بالقوه و فراخوان به اقدام

«رسالهٔ یک شبکه» چیزی فراتر از یک ویژگی نرم‌افزاری است؛ ابزاری برای انسجام اجتماعی است. با اجازه دادن به یک جمعیت برای کشف ارادهٔ جمعی خود، مستقیماً با استراتژی «تفرقه بینداز و حکومت کن» مقابله می‌کند. این طرح، چشم‌اندازی از افراد منزوی را به یک بدنهٔ متصل و اهل گفتگو تبدیل می‌کند که قادر به ایجاد یک مأموریت روشن برای تغییر است. این یک مسیر برای خروج از درماندگی‌ای که مانع پیشرفت می‌شود، فراهم می‌کند.

موفقیت آن به ائتلافی از آینده‌نگرانی بستگی دارد که می‌دانند چه چیزی در میان است. بنابراین ما به دنبال شرکایی برای به ثمر رساندن این چشم‌انداز هستیم. ما به دنبال این افراد هستیم:

- **فناوران و توسعه‌دهندگان** با تخصص در سیستم‌های غیرمتمرکز، رمزنگاری و توسعهٔ برنامه‌های امن برای کمک به طراحی و ساخت نمونهٔ اولیهٔ مینی-اپ.
- **سازمان‌های حقوق دیجیتال و ان‌جی‌اوها** برای ارائهٔ راهنمایی استراتژیک، حمایت و پشتیبانی از یک برنامهٔ آزمایشی.
- **آینده‌نگرانی در داخل تلگرام** که پتانسیل این ابزار را برای تحقق والاترین وعدهٔ این پلتفرم، یعنی اتصال مردم و دفاع از آزادی بیان، تشخیص می‌دهند.

زمان صداهای گسسته به پایان رسیده است. زمان ساختن شبکه فرا رسیده است.

تماس: simurgh_beau@proton.me