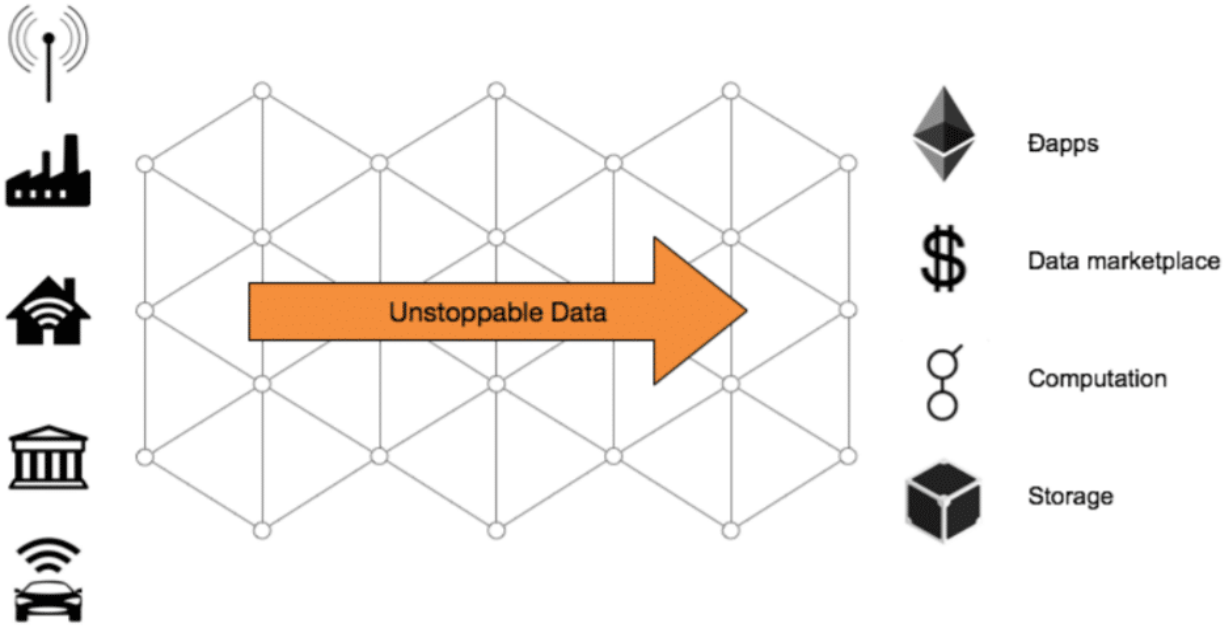
Data imparable para apps imparables: DATAcoin de Streamr

25 de julio de 2017
Versión 1.0

Este *whitepaper* es informativo y no constituye una oferta o un consejo de inversión. Cualquier elemento de este *whitepaper* puede cambiar significativamente conforme el proyecto se desarrolle.



Visión de Streamr

Streamr proporciona data imparable para aplicaciones imparables. Es la columna vertebral de data en tiempo real de la supercomputadora global: Una red descentralizada, escalable, de baja latencia, incorruptible, para transmisión y persistencia de data, operada por el token DATAcoin. Cualquier persona —u otra cosa— puede publicar nueva data en transmisiones de data, y otros pueden suscribirse a estos flujos para implementar Đapps, contratos inteligentes, microservicios y canales de data inteligentes.

Para incentivar la participación del usuario en la red, hay un mecanismo integrado para la monetización de data. Data valiosa proveniente del mercado de valores, dispositivos conectados, sensores IoT y los medios de comunicación sociales, puede ser ofrecida a compañías, desarrolladores y particulares. Las máquinas pueden vender su data de manera autónoma, obtener remuneración y comprar la data que requieren. Surge así un mercado global para data en tiempo real, con origen, encriptado y control de acceso de data integrados.

Junto con la red y el mercado de data descentralizados, el stack completo de Streamr incluye un poderoso motor analítico y un UI para el rápido desarrollo de Đapps en tiempo real. Transmisiones de data, contratos inteligentes y recursos de cómputo descentralizados pueden interconectarse en un ambiente de bajo código utilizando bloques de construcción de alto nivel. Streamr será el sitio en el que con más facilidad se crearán aplicaciones de blockchain confiables en tiempo real e impulsadas por data.

Una revolución se está llevando a cabo: los servicios de nube centralizados están siendo desbancados uno a uno por soluciones tokenizadas y descentralizadas. Golem, por ejemplo, reemplaza a Azure Virtual Machine, e IFPS reemplaza a Azure Blob Storage. Streamr se enorgullece de unirse a la revolución proporcionando una solución descentralizada al procesamiento de mensajería y eventos, reemplazando a plataformas como Azure EventHub y Azure Stream Analytics.

1. Antecedentes

La data en tiempo real se irá convirtiendo en un producto básico con el paso del tiempo. Enormes volúmenes de data con sello de tiempo están siendo generados por sensores y dispositivos conectados en el sector manufacturero, en el de servicios y en la cadena de suministro completa, lo que sustenta la base de la economía moderna, con buena parte de la data generada de manera continua.[1,2]

La cantidad de data aumenta exponencialmente junto al crecimiento del llamado internet de las cosas (IoT, por sus siglas en inglés) y la ubicuidad de dispositivos conectados. En el mercado IoT global, IHS Markit [3] pronostica que la base instalada crecerá de 15.4 miles de millones de dispositivos en 2015 a 30.7 miles de millones en 2020 y 75.4 miles de millones en 2025. Mucha de la data recién generada es valiosa: puede ser utilizada para optimizar operaciones de manufactura, monitorear activos con precisión creciente, localizar nichos de consumo existentes con gran nivel de detalle y crear servicios y modelos de negocios completamente nuevos.

Al mismo tiempo, hay una megatendencia que avanza hacia la siguiente generación del stack de cómputo. En un *futuro distribuido*, el código de backend de apps descentralizadas —o Đapps[4]— corre en redes peer-to-peer. Ethereum es una Đapp en sí misma, al igual que Golem, y hay muchas más en desarrollo.

De cualquier forma, las Đapps no corren de manera aislada: Necesitan data externa para funcionar. Así, el almacenamiento y la distribución de data del mundo real permanece centralizada, y las Đapps permanecen inermes a todos los problemas conocidos: concentración de poder, falta de robustez y vulnerabilidad a ataques cibernéticos.

Sin duda, ya es posible almacenar data en la blockchain. También hay apps descentralizadas de almacenamiento de archivos tales como IFPS, Swarm y Storj, y bases de datos como BigchainDB comienzan a aparecer. Mientras que tales soluciones son sin duda parte del nuevo entramado descentralizado, no proporcionan realmente una respuesta a casos en los que la data en tiempo real se necesita en volúmenes significativos. La cadena no está diseñada para alto rendimiento o baja latencia, no es escalatoria y el almacenamiento es costoso.

Lo que se requiere es una columna vertebral descentralizada en forma nativa como complemento para las apps descentralizadas. Esta columna vertebral de data en tiempo real será el eslabón faltante, y el eslabón que queremos ayudar a proporcionar. La infraestructura que creamos consiste en un stack tecnológico que ayuda a conectar e incentivar computadoras en una red global peer-to-peer (P2P). Esta es una red que proporciona baja latencia, transmisión de data robusta y segura, y persistencia, y todo en forma escalada. Las Đapps del futuro son impulsadas por data, y nuestra misión es asegurarnos de que la data siga fluyendo.

---

[1]Susan O'Brien: "5 Big Data Trends Shaping the Future of Data-Driven Businesses", Datameer, 11. Mai 2016 (https://www.datameer.com/company/datameer-blog/5-big-data-trends-shaping-future-data-driven-businesses/)

[2]Tony Baer: "2017 Trends to Watch: Big Data", Ovum, 21. November 2016. (https://ovum.informa.com/~/media/Informa-Shop-Window/TMT/Files/Whitepapers/2017_Trends_to_Watch_Big_Data.pdf)

[3]Sam Lucero: "IoT Platforms: enabling the Internet of Things", IHS Markit, März 2016. (https://cdn.ihs.com/www/pdf/enabling-IOT.pdf)

[4]Für eine (englischsprachige) Definition des Begriffs „Đapps“, siehe „Johnston et al.: The General Theory of Decentralized Applications“.(https://github.com/DavidJohnstonCEO/DecentralizedApplications)

También creamos un mercado para data en tiempo real. En el Streamr Data Marketplace, cualquiera puede publicar eventos en transmisiones de data, y cualquiera puede suscribirse a las transmisiones y usar la data en apps descentralizadas. Gran parte de la data es gratuita, pero cuando no, los términos de uso están almacenados en los contratos inteligentes de Ethereum. Un token digital —una DATAcoin— se requiere para acceder y operar el mercado de data y para compensar nodos en la red P2P. Los suscriptores pagan por la data con el token, y a los productores de data y a los participantes en la red se les reembolsan los montos de manera automática y segura.

Nuestro stack está construido en una capa de transportación descentralizada. Además de una mayor robustez, resiliencia y tolerancia a desperfectos, la descentralización facilita la apertura, la transparencia y la construcción de comunidad.
El poder sobre la data no se da junto a grandes corporaciones como Google, Amazon, Microsoft e IBM. La red consiste en una multitud de productores y consumidores de data, y nodos de brokers de mensajería entre ellos. Es posible hacerse una reputación y generar buen karma contribuyendo al intercambio de data y ayudando a ejecutar la red para beneficio de todos.

Creemos que el crecimiento sostenido de la comunidad de blockchain se facilitará al tener una capa de usabilidad. Las herramientas se requieren de forma que los no-expertos puedan crear contratos inteligentes con seguridad, y conectar esos contratos y Đapps a fuentes de data confiables. Ayudaremos a configurar el equipo adecuado para proporcionar un editor visual, wrappers y plantillas. En breve, queremos ser el lugar de referencia para cualquiera que esté en el negocio de la creación de servicios descentralizados impulsados por data.

En el resto de este documento describimos el stack tecnológico de Streamr, definimos el papel del token digital, explicamos el statu quo, presentamos el roadmap de I&D e introducimos al equipo.

2. Stack de Streamr

El canal de data en tiempo real descentralizado está construido sobre un stack tecnológico de muchas capas:

- **Streamr Editor** constituye una capa y herramienta de usabilidad que permite el rápido desarrollo de apps descentralizadas, impulsadas por data.

- **Streamr Engine** es un motor de procesamiento y análisis de eventos de alto desempeño que se ejecuta off-chain de manera descentralizada. Puede correr en un proveedor de cómputo descentralizado como Golem.

- **Streamr Data Marketplace** es un universo de transmisiones de data compartidos al que cualquiera puede contribuir y suscribirse.

- **Streamr Network** es la capa de transporte de data, que define una red incentivada peer-to-peer para mensajería en el canal de data descentralizado.

- **Streamr Smart Contracts** habilita nodos en la red Streamr para alcanzar consenso, retener transmisión de metadatos, manejar permisos y chequeos de integridad y facilitar la transferencia segura de tokens.

En la siguiente sección se revisa cada capa del stack (ver Figura 1) a detalle, siguiendo una estrategia de arriba abajo.

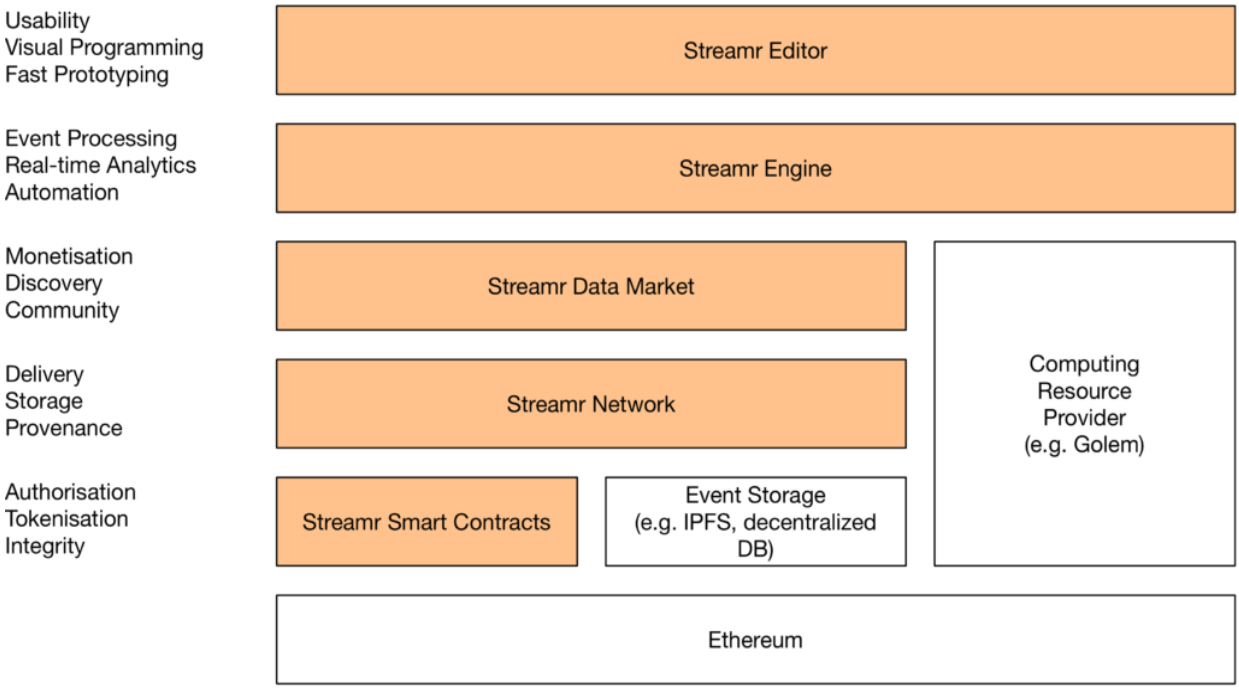


Figura 1. Stack tecnológico de Streamr.

2.1 Streamr Editor

Streamr Editor permite un rápido desarrollo de contratos inteligentes impulsados por data, reduce el umbral para la creación de Đapps, e incluye plantillas listas para casos de uso común integradas

Hay un interés considerable en la blockchain y las aplicaciones descentralizadas dentro de la comunidad de negocios, pero el número de casos de uso de la vida real es reducido. Esta es la etapa inicial, y no es irracional sostener que muchos de quienes desean involucrarse no son grandes expertos en las minucias de Ethereum, Solidity, encriptado, origen de data u otras cuestiones técnicas.

Desde nuestro punto de vista, el crecimiento comercial del ecosistema requiere herramientas que permitan a no-expertos preparar contratos inteligentes, conectar con fuentes confiables de data, hacer uso de módulos off-chain para filtración, agregación y refinamiento de datos, desplegar aplicaciones descentralizadas, monitorear la ejecución de contratos inteligentes y visualizar el flujo de entrada de data y eventos de blockchain.

Atendemos la necesidad de una capa de usabilidad al proporcionar poderosas herramientas (tales como un editor visual fácil de usar), wrappers y plantillas de contratos inteligentes, que están dirigidos a profesionales de dominios y usuarios de negocios. Estas herramientas ocultan la tecnología profunda bajo el cofre, manejan las integraciones y comunicaciones de data y automatizan los pasos de rutina en el despliegue y monitoreo de contratos inteligentes.

Prevemos un ecosistema en el que haya disponibles diversas plataformas y herramientas de usabilidad. La plataforma existente de Streamr implementa de por sí algunos elementos de la capa de usabilidad, que agregará más funciones en los meses y años venideros. La intención es alcanzar una etapa en la que se pueda construir y desplegar en minutos un contrato inteligente impulsado por data que sea útil y funcional. Esto es más que una fantasía; nuestro demo en la EDCON[5] de París en febrero de 2017 es una degustación de lo que se puede ya hacer (ver Figura 2).

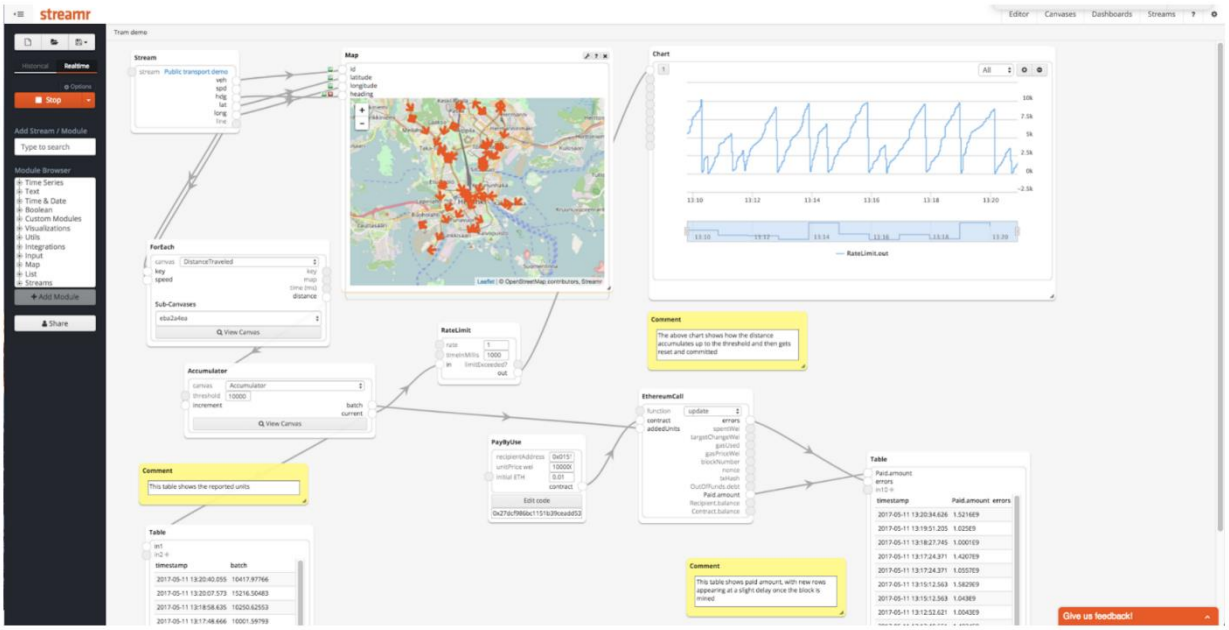


Figura 2. Una versión alpha del espacio de trabajo para editores de Streamr.

Éstas son algunas de las características planeadas para la capa de usabilidad:

- Un editor visual para crear contratos inteligentes, alimentado con data del mundo real, y construyendo canales de procesamiento de data off-chain.
- Módulos para comunicación con contratos inteligentes y para interactuar con la blockchain.
- Módulos para procesamiento off-chain: Filtración, refinamiento y agregación de data, despliegue de aplicaciones descentralizadas, monitoreo de ejecución de contratos inteligentes y visualización del flujo de entrada de data y eventos de blockchain.
- Un editor de Solidity en el que el código del contrato inteligente puede ser escrito y modificado en un ambiente sensible al contexto.
- Plantillas de Solidity basadas en código abierto, probadas e integradas para diferentes casos de uso de contratos inteligentes de Ethereum.
- Funcionalidad de Playback para simular funcionalidad del contrato inteligente, depurar el código del contrato y comprobar la funcionalidad antes del lanzamiento.
- Despliegue con un clic para lanzar un contrato inteligente ya sea en la red de pruebas o en la red principal.

[5] Henri Pihkala. „Connecting Ethereum ith the Real World: How to Easily Create Data-Driven Smart Contracts“, en European Ethereum Development Conference (EDCON), 17-18 de febrero de 2017. https://www.youtube.com/watch?v=C110rcj-Fok

2.2 Streamr Engine

Streamr Engine es el motor de análisis de alto rendimiento que se ejecuta off-chain con un proveedor de cómputo descentralizado (p. ej.: en un contenedor Docker en Golem).

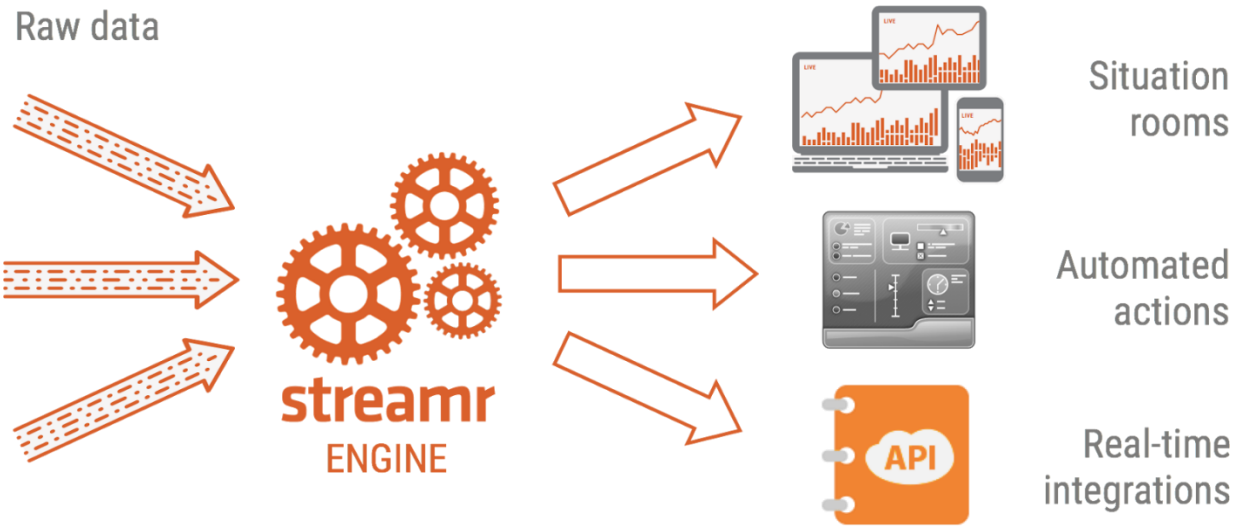


Figura 3. Típico patrón de flujo de data con resultados para el motor de análisis de Streamr.

Las Đapps, normalmente con interfaz de usuarios basado en red y backends basados en contratos inteligentes no cuentan actualmente con una manera de procesar data cruda y convertirla en información. Un grupo de sensores IoT o el mercado de valores puede producir miles o incluso millones de eventos por segundo, una cantidad imposible o demasiado cara de incluir en cualquier blockchain para cómputo.

Se requiere una capa de análisis de transmisiones para convertir data cruda en información refinada y lista para su consumo por Đapps y contratos inteligentes. La data cruda puede necesitar filtrarse, reducir su muestra, agregarse, combinarse con más data, correr por algoritmos de detección de anomalías o ser procesada por aprendizaje de maquinaria avanzada y modelos de reconocimiento de patrones. O tal vez se requiera hacer cosas que simplemente no pueden hacerse en contratos inteligentes, como llamar Interfaces de Programación de Aplicaciones (API) externas como parte de la cadena de procesamiento.

El Streamr Engine presta atención a eventos en la Streamr Network, y modela estructuras utilizando Streamr Editor, refina data entrante y reacciona a nuevos eventos en tiempo real. Hay muchas maneras de reaccionar, incluyendo las siguientes:

- Publicando data refinada en otra transmisión de la Streamr Network, acaso mostrada en tiempo real por una Interfaz de Usuario Đapp igualmente conectada a la red.
- Interactuando con un dispositivo IoT, por ejemplo, controlando un activador, abriendo un

cerrojo, encendiendo las luces o llamando al elevador.
- Enviando una alerta vía e-mail o lanzando una notificación.
- Llamando una función en un contrato inteligente.

El utilizar la Streamr Network como un mortero de mensajería entre las Đapps y el cómputo off-chain en el motor habilita una categoría completamente nueva de apps descentralizadas: apps impulsadas por volumen de data no-trivial. Obviamente, los resultados pueden igualmente ser consumidos por apps centralizadas tradicionales, al tiempo que se disfrutan los beneficios de mensajería y análisis descentralizados.

2.3 Streamr Data Marketplace

Streamr Data Marketplace es un universo global de transmisiones de data compartidas al que cualquiera puede contribuir y suscribirse. Es un sitio para monetización de data e intercambio de data máquina-a-máquina (M2M). El Data Market busca la anonimidad, pero permite la verificación de la identidad digital donde sea requerida.

El Streamr Data Marketplace es un lugar de encuentro para productores y consumidores de data. Los consumidores de data encuentran valor en la data ofertada, y desean acceder a ella con la intención de utilizarla como aportación para las Đapps, los contratos inteligentes o las apps tradicionales.

La data es organizada en transmisiones de data, el bloque de construcción básico del Streamr Data Marketplace y un ente primitivo en la Streamr Network (ver el Capítulo 2.4 abajo). Las transmisiones de data contienen eventos de fuentes de data que siguen emitiendo puntos de data nuevos en intervalos regulares o irregulares. A continuación, algunos escenarios en los que data en tiempo real es producida de manera continua.

- Un mercado de valores genera un nuevo evento cada vez que hay una nueva puja u oferta, y cada vez que se lleva a cabo una transacción.
- Un vehículo de transporte público emite su identidad, status, velocidad, aceleración, geolocalización y dirección cada pocos segundos.
- Un detector de movimiento transmite una señal cuando un objeto móvil se detecta en las cercanías.
- Los sensores de Internet Industrial de las Cosas (IIoT, por sus siglas en inglés) anexos a un convertidor de frecuencia miden la temperatura, velocidad y las vibraciones durante la operación del convertidor en una fábrica inteligente.
- Los sensores de la calidad del aire miden los niveles de monóxido de carbono, dióxido de azufre, dióxido de nitrógeno y ozono en un área urbana.
- Los sismógrafos miden el movimiento del suelo en un área con actividad volcánica.
- Las prendas inteligentes utilizadas por atletas profesionales recogen data biométrica como el pulso, la temperatura y la aceleración.

El Streamr Data Marketplace proporciona una amplia selección de data con sello de tiempo disponible para suscripción. De esta data, una parte proviene de vendedores y redistribuidores profesionales y establecidos, y una parte, de fuentes públicas, de data abierta. Es importante señalar que la plataforma permite a cualquiera contribuir y monetizar con su data. Al mismo tiempo que diversas compañías tienen valiosa data siendo transmitida desde sensores y dispositivos, los particulares también están produciendo información valiosa.

Por ejemplo, la gente que utiliza un smartwatch podría colocar la data de su frecuencia cardiaca a la venta en el Streamr Data Marketplace. Se puede ofrecer data de manera anónima, de modo que la privacidad no es violada. ¿Quién podría interesarse en esa data? Pues una compañía farmacéutica podría comprarla para investigaciones, o una organización de cuidado de la salud pública podría utilizarla para averiguar qué tan seguido hace deporte la gente, o cuál es el nivel de estrés del público. Un fabricante de smartwatches podría comprarla para obtener diagnósticos del desempeño de sus sensores de frecuencia cardiaca. Además, los productores de data pueden tener un ingreso diario sólo porque su data está disponible.

No hay razón alguna por la que las suscripciones en el Streamr Data Marketplace deban ser iniciados por desarrolladores de software humanos, ingenieros de data o científicos de data. De hecho, el mercado descentralizado bien puede terminar siendo dominado por transacciones máquina-a-máquina. Máquinas autónomas, robots, aparatos inteligentes tendrán toda la data necesaria en sus operaciones, y están produciendo data que es valiosa para otros participantes en el ecosistema.

Aparecerán patrones de refinamiento automáticos, que agregarán valor. Una inteligencia artificial podría suscribirse a un feed de mercado de valores crudos, aplicar reconocimiento de patrones de propietario para generar señales de comercio, y poner esas señales a la venta en el propio Streamr Data Marketplace.

Mientras buena parte del contenido del Streamr Data Marketplace estará disponible de manera gratuita para todos, habrá data que requiera de pagos, y habrá data en la que aplique una licencia de usuario final. En estos casos, se requerirá una licencia de suscripción. Una licencia dará el derecho de acceder a la data por un período específico, con ciertas condiciones, y a cambio de una tarifa. Hay una analogía cercana al escuchar música en la red: No adquieres los derechos de la data suscrita al igual que no obtienes los derechos de una canción al escucharla en Spotify o descargarla vía iTunes.

Las licencias de data se implementan como contratos inteligentes (ver Sección 2.5.4). El gran beneficio de la blockchain es que ofrece un método autónomo y descentralizado para almacenar los términos de uso y los derechos de acceso, y asegurarse de que los pagos de data se están realizando, como se acordó.

En un contexto más amplio, hay potencial para un poderoso efecto de red en el mercado. Entre más contenido haya, más atractiva se vuelve la propuesta tanto para contribuidores de data como para consumidores de la misma. En el Streamr Data Marketplace, un portal web (implementado como Đapp) facilita el descubrimiento de la data existente, proporciona una serie de herramientas abarcadoras para la creación y gestión de transmisiones de data, facilitando el suscribirse a las

transmisiones de data que se prefiera.

2.4 Streamr Network

Streamr Network es la capa de transporte de data en el stack tecnológico. Consiste en nodos broker de Streamr que generan una red P2P. La red alberga un mecanismo de publicar/suscribirse y soporta el almacenamiento de eventos descentralizado. El rendimiento de la red escala de manera lineal con el número de nodos participantes, y puede procesar millones de eventos por segundo.

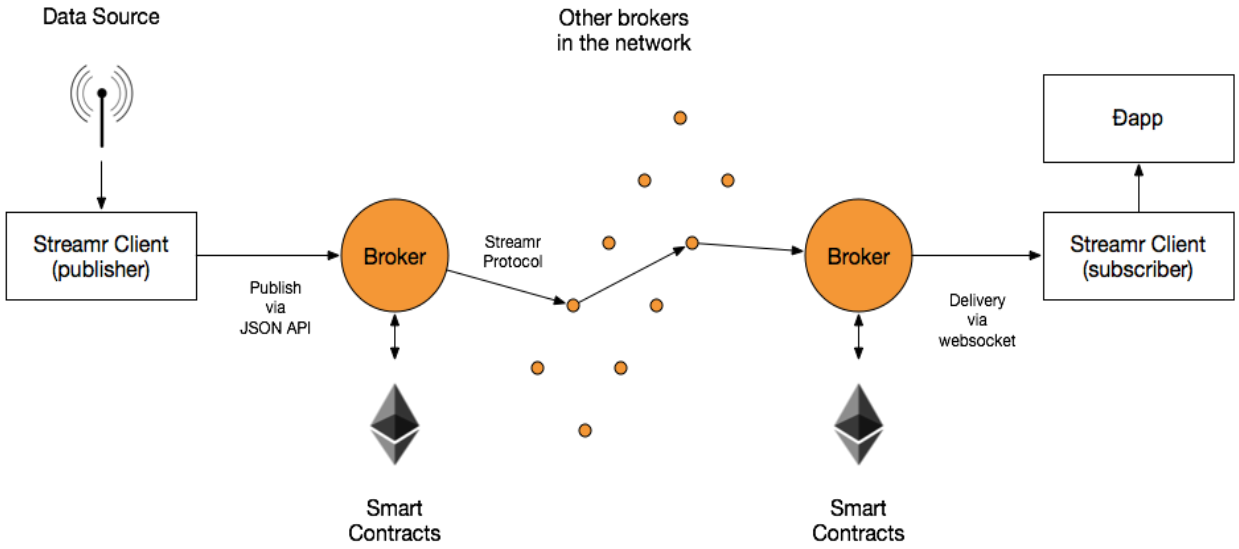


Figura 4. Ejemplo de un evento avanzando a través de la red de brokers desde una fuente de data hasta la Đapp de un suscriptor.

La Streamr Network (Figura 4) es una capa de transporte del stack Streamr. La red maneja toda la mensajería en un canal de data descentralizado. La capa consiste en entes primitivos (eventos y transmisiones) y nodos broker. Los nodos broker operan sobre los primitivos, y la colección de nodos broker constituyen la red P2P, que maneja almacenamiento descentralizado y mensajería descentralizada.

La capa de infraestructura utiliza el stack de Ethereum subyacente para sus operaciones. La coordinación entre nodos requiere un consenso robusto, lo que se implementa a través de contratos inteligentes. La data cruda de eventos en sí normalmente no se incluye en la blockchain, la cual, al particionarse permite a la Streamr Network escalar a millones de eventos por segundo, y más.

La Streamr Network combina las mejores partes de transportes de data en tiempo real, basados en la nube, escalables (p. ej.: Kafka, ZeroMQ, ActiveMQ), y lo que está disponible en la comunidad

descentralizada P2P/crypto (Whisper [6], Bitmessage[7]). Los marcos de trabajo basados en la nube utilizan un sharding eficiente y esquemas de persistencia para alcanzar el alto rendimiento, pero sólo en un ambiente de red local confiable.

Los protocolos peer-to-peer muestran estrategias efectivas para enrutamiento, descubrimiento de pares, NAT transversal, ofuscación de locación y demás, pero no logran el rendimiento necesario para aplicaciones con data intensiva del mundo real.

2.4.1 Eventos

Un evento[8] es una pieza de información con sello de tiempo. Cada evento contiene encabezados y contenido. Los encabezados especifican la metadata del evento, como pueden ser su sello de tiempo, origen y características de contenido. El protocolo de evento soporta características y formatos de carga útil de contenido; p. ej.: mensajes JSON o imágenes binarias. Las características de contenido indican en qué formato está el contenido. Los encabezados y contenido del evento se codifican en un formato binario para su transmisión.
Todos los eventos en la Streamr Network están firmados criptográficamente. Todos los eventos tienen un origen, por ejemplo, una dirección Ethereum. Una firma se calcula a partir de una clave privada y el resto del mensaje. La firma se utiliza para probar el origen y la integridad del mensaje. Como el formato de evento permite cualquier tipo de orígenes y firmas, el sistema resulta a prueba de obsolescencia.

La siguiente tabla enlista la información contenida en un evento.

Campo	Descripción
Versión	Versión del protocolo del evento
Transmisión	ID de la transmisión (dirección Ethereum de la transmisión del contrato inteligente)
Partición	Partición de la transmisión (ver sección de particionamiento)
Sello de tiempo	Sello de tiempo del evento (ISO 8601)
Características de contenido	Instrucción de cómo diseccionar el cuerpo (p. ej.: JSON)
Características de encriptado	El algoritmo de codificación utilizado para encriptar el contenido
Contenido	Carga útil de data
Características de origen	Instrucción de cómo interpretar el origen
Origen	Originador de data
Características de firma	Instrucción de cómo interpretar la firma
Firma	La firma criptográfica prueba el origen y la integridad del mensaje

[6] Gav Wood: "Whisper PoC 2 Protocol Spec" en GitHub, 15 de noviembre de 2017. https://github.com/ethereum/wiki/wiki/Whisper-PoC-2-Protocol-Spec
[7] Bitmessage Wiki: "Main Page“, en Bitmessage Wki, 17 de febrero de 2017. https://bitmessage.org/wiki/Main_Page
[8] Los eventos de Sreamr no deben confundirse con eventos en contratos inteligentes de Ethereum.

2.4.2 Transmisiones

Todos los eventos pertenecen a una transmisión. Puede haber cualquier cantidad de transmisiones, cada una de las cuales agrupa eventos que están relacionados lógicamente y almacenados en un orden cronológico ascendente.

La metadata de transmisión se almacena en un contrato inteligente de Ethereum. Cada transmisión está identificada por la dirección Ethereum del contrato. Para cuestiones de escalabilidad, los eventos (es decir, los puntos de data en sí) no se almacenan en contratos inteligentes o en la blockchain.

Una transmisión de data retiene una serie de permisos. Los permisos controlan quién puede leer eventos de la transmisión (suscribirse) y quién puede escribir nuevos eventos en la transmisión (publicar). El dueño de la transmisión controla los permisos, pero igualmente puede dar o delegar el control de permisos a terceras personas cuando sea necesario.

La siguiente tabla enlista la metadata de una transmisión.

Campo	Descripción
Id	id de la transmisión (dirección Ethereum)
Nombre	Nombre de la transmisión
Descripción	Descripción de la transmisión
Propietario	Propietario de la transmisión
Permisos	Un mapeo desde la Dirección Ethereum a los niveles de permiso

2.4.3 Publicar/ Subscribirse

La transmisión de data en la red sigue el paradigma de publicar/suscribirse[9]. Los eventos publicados en una transmisión son entregados enseguida a todos los suscriptores de la transmisión que estén autorizados y conectados. El suscribirse a transmisiones puede restringirse a sólo ciertos usuarios o estar libre para el público. De manera similar, el permiso de publicar contenido en una transmisión puede ser retenido por una sola persona, o varias, o todas.

El paradigma de publicar/suscribirse habilita varias topologías de mensajería utilizadas en aplicaciones del mundo real:

- Uno-a-varios (por ejemplo, un canal de noticias o un teletipo bursátil)
- Varios-a-varios (por ejemplo, un grupo de chat o un juego para varios jugadores)
- Uno-a-uno (por ejemplo, un chat privado o un canal de análisis)
- Varios-a-uno (por ejemplo, un sistema de votación)

Cabe señalar que publicar un evento no implica que éste sea entregado a cliente alguno: Puede ser el caso que no haya suscriptores. Aun así, el evento continúa, y es entregado a diversos nodos broker para su redundancia.

[9] Wikipedia: Publish/subscribe pattern (https://en.wikipedia.org/wiki/Publish–subscribe_pattern)

Técnicamente, hay dos tipos de suscriptores. La mayor parte del flujo de data va a suscriptores conectados a la red vía conexión directa a un nodo broker (ver Sección 2.4.4 abajo). Éstos pueden ser, por ejemplo, front-ends web de Đapps, cadenas de procesamiento de eventos corriendo en Streamr Engine, o dispositivos IoT controlados por data de la red.

Los contratos inteligentes son un tipo especial de suscriptor soportado por la Streamr Network. Los nodos broker de la red se incentivan para entregar eventos a contratos inteligentes suscritos. En este escenario, desde luego, aplican los límites de escabilidad de la blockchain. El mecanismo permite a la red actuar como un oráculo, lo que significa que la data puede enviarse a contratos inteligentes sin ayuda de un oráculo de tercera parte. Como toda la data en la red se firma en la fuente, siempre puede ser verificada, y es confiable.

2.4.4 Nodo broker

El nodo Broker de Streamr es el componente central de software en la red. Un nodo broker maneja tareas tales como publicación de eventos, suscripción a transmisiones, manejo de almacenamiento y comunicación con nodos Ethereum vía llamadas JSON RPC. El nodo broker expone su funcionalidad a aplicaciones conectadas vía API.

La API broker puede utilizarse desde apps que utilizan HTTP estándar y librerías Websocket en cualquier lenguaje. Para facilitar el uso, proporcionamos implementaciones de referencia en diversos lenguajes. La plataforma primaria de archivo de clientes estará escrita en JavaScript. Puede ser utilizada para entregar data a Đapps basadas en web funcionando en el navegador tan bien como aplicaciones back-end ejecutando node.js. Una API Websocket maneja la entrega de eventos desde fuentes de data a la red, y de la red a Đapps clientes. Para la gestión de transmisión se utiliza una API JSON.

La API de transmisión Websocket se encarga de las siguientes tareas:

- Verifica la autenticidad de una sesión
- Publica eventos
- Se suscribe a eventos en transmisiones
- Entrega eventos a clientes suscritos
- Consulta eventos históricos en transmisiones

La API JSON exhibe la siguiente funcionalidad:

- Crea una transmisión
- Configura una transmisión
- Borra una transmisión
- Obtiene información sobre una transmisión
- Encuentra transmisiones mediante criterios de búsqueda
- Publica eventos (de forma alternativa a la API Websocket)

- Consulta eventos históricos en transmisiones (de forma alternativa a la API Websocket)

La mayor parte del tráfico entre brokers consiste en mensajes de eventos, pero también hay tráfico relacionado con el enrutamiento y el descubrimiento de pares. Una importante tarea de coordinación entre brokers es la asignación de partición, en la que debe alcanzarse un consenso confiable. Este mecanismo se implementa como contrato inteligente, lo que equilibra el poder de la red Ethereum (ver Sección 2.4.5 abajo).

2.4.5 Particionado (Sharding)

El tráfico de eventos en toda la red se divide en partes independientes llamadas particiones. Cada nodo broker maneja el tráfico que corresponde a una serie de particiones. Así es como se alcanza la escalabilidad: no todos los nodos manejan todo el tráfico. Esto es similar al esquema de partición que se encuentra, por ejemplo, en Apache Kafka.

La partición para un evento particular se calcula haciendo un resumen criptográfico del id de la transmisión. Esta es una operación rápida que se realiza localmente. Utilizar el id de la transmisión como clave de partición significa que todos los eventos en una transmisión particular irán siempre a la misma partición. Esto permite a la red mantener el ordenamiento de eventos dentro de una transmisión, y almacenarlos eficientemente.

Puede suceder que una transmisión reciba tal volumen de mensajes que un broker aislado no pueda manejarlos. En este caso, otra ronda de particionado se aplica a las propias transmisiones, y el tráfico dentro de la transmisión se divide en partes independientes. En este caso, hacemos un resumen criptográfico de la tupla (id de transmisión, partición de transmisión) para asignar la partición de la red, y el publicador proporciona la clave de partición, que asigna al evento a una partición dentro de la transmisión. Se mantiene así el orden de los eventos para una clave de partición de transmisión.

El número de particiones en la red permanece constante hasta que se incrementa de manera automática con el tiempo. Como se describe en la siguiente sección, hay un contrato inteligente coordinador, que controla 13 las particiones de red. El número de particiones es proporcional al número de nodos broker participando en la red.

2.4.6 Coordinación de nodos

En sistemas de data distribuida tales como Apache Kafka y Apache Cassandra, la coordinación de nodos normalmente es alcanzada utilizando un componente como Apache Zookeeper. Hay un proceso centralizado para establecer consenso en procesos como elección de líder. De manera alternativa, algunos sistemas utilizan asignación manual de nodos coordinadores, lo que tiene privilegios especiales en la red.

En una red descentralizada, estos componentes centralizados o privilegiados no pueden existir. En su lugar, la Streamr Network utiliza la red subyacente Ethereum para establecer consenso para coordinación de nodos en la red P2P.

La tarea de coordinación clave es la asignación de particiones de red a nodos broker en la red, y el mantenimiento de cambios en esta información cuando los nodos aparezcan o desaparezcan. En lugar de un componente centralizado como Zookeeper, esta tarea se implementa por un contrato inteligente: el coordinador de red. El contrato de coordinador de red se despliega en la blockchain de Ethereum. Los nodos broker averiguan el estado actual de la red observando y consultando el contrato inteligente. La actualización de la red se alcanza simplemente cambiando a un nuevo contrato de coordinador de red.

Equilibrar nuevamente las asignaciones de partición es una de las tareas del contrato de coordinador de red. Sólo se realizan los cambios útiles, y si no hay ninguno, la función no hace nada. Cuando la red no está equilibrada, llamar a la función le otorga DATAcoin a quien lo hace. Este incentivo asegura que el equilibrio de la red se realiza siempre que se necesita.

Los nodos asignados a una partición reciben toda la data para esa partición. Algunos o todos realizan constantes sumas de verificación de data y las reportan al contrato inteligente coordinador de la red en ciertos intervalos. En una red pública grande, hay suficientes nodos para cada partición de modo que se les dificulte coludirse. La asignación de partición por el contrato inteligente coordinador de la red es también difícil de influenciar.

2.4.7 Incentivación

Los suscriptores son los consumidores de data en la red. La DATAcoin, el token de uso de la red, permite a los suscriptores suscribirse a las transmisiones. Otras partes ganan DATAcoin contribuyendo a la red: los nodos broker (los “mineros” de esta red) y los publicadores de data.

Los nodos broker son incentivados para hacer dos cosas: reportar sumas de verificación para sus particiones asignadas al contrato inteligente coordinador de la red (ver Sección 2.4.6 arriba), y entregar data a cualquier suscriptor de contratos inteligentes (ver Sección 2.4.3). Ambas operaciones cuestan algo de gas Ethereum, pagado por el broker. Este costo se cubre mediante DATAcoin que los brokers reciben por hacer funcionar la red.

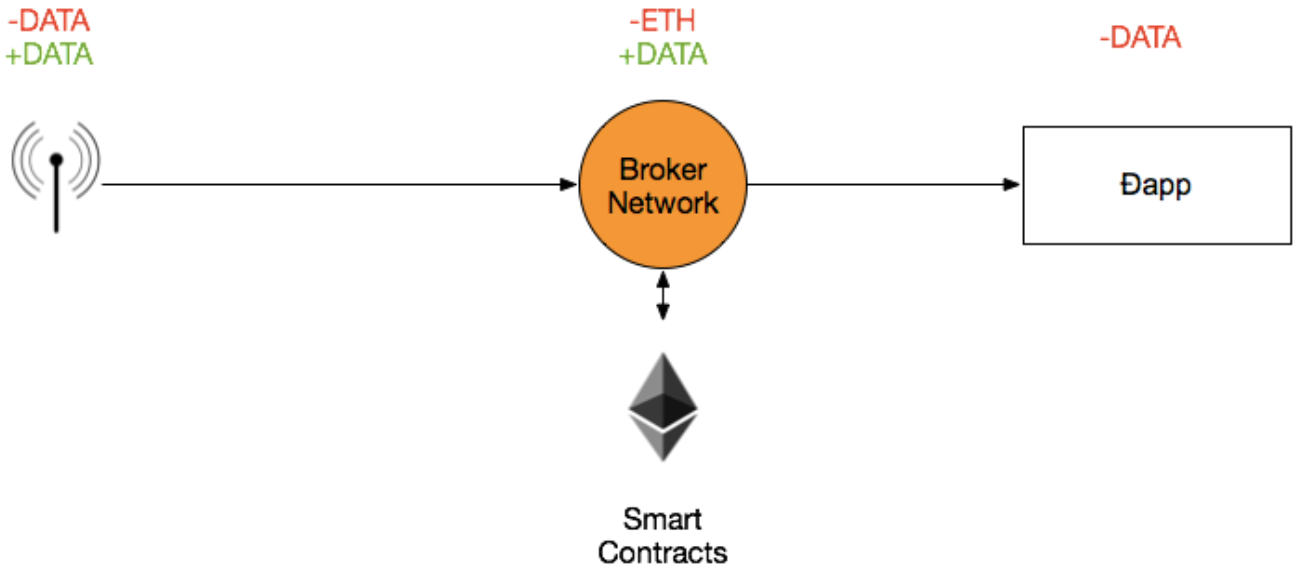


Figura 5. Diagrama esquemático de la estructura de incentivos en la Streamr Network.

Las sumas de verificación son calculadas y reportadas por múltiples nodos broker, y los brokers son recompensados sólo si concuerdan en las sumas en un umbral de coherencia señalado en el contrato inteligente coordinador (por ejemplo, 90% de los brokers asignados necesitan reportar una suma de verificación particular para que sea considerada válida). Si un nodo no reporta sumas de verificación, o reporta sumas anormales, o las sumas no son coherentes, no obtiene recompensa, y los nodos incumplidos tienen menos posibilidades de obtener la asignación de responsabilidades para una partición en el futuro.

Como se ha discutido, los contratos inteligentes pueden suscribirse a una transmisión. El suscriptor fija una recompensa en DATAcoin por entregar eventos al contrato inteligente. La recompensa se entrega a quien entregue primero la data. Normalmente éste sería el nodo broker directamente conectado con el publicador, dado que ese broker está en posición inmejorable para hacer la entrega. Otros nodos o suscriptores externos pueden observar este proceso y obtener oportunidades de entregar la data, si no es entregada por el sospechoso común.

También se necesita un mecanismo que prevenga el exceso de información en la red. Un costo mínimo debe asociarse con todas las operaciones de publicación y de entrega a suscriptores. La red puede agregar los costos y apoyarse de vez en vez en la blockchain subyacente por cuestiones de escalabilidad, de modo similar a la forma en que funcionan los canales de estado o los canales de micropago en algunas redes de blockchain.

2.4.8 Persistencia de eventos

Los eventos en transmisiones de data son continuos en la red peer-to-peer. Esto convierte de manera efectiva la red en una base de datos de series de tiempo descentralizada. La descentralización proporciona distintas ventajas, incluyendo mayor robustez, tolerancia a desperfectos, menor costo y el potencial para la anonimidad.

Como las transmisiones son secuencias de eventos, la manera más simple de almacenamiento es un registro de eventos. Un registro de eventos puede guardarse en cualquier almacén de bloques, tal como un sistema de archivos en los propios nodos, o en almacenes de objetos descentralizados tales como Swarm[10], IFPS[11] o Storj[12].

Para un almacenamiento con mucho mayor nivel de detalle y características de consulta, han surgido bases de datos descentralizadas tales como BigchainDB[13]. Una solución como ésta es un candidato probable para el almacén de eventos en la Streamr Network. De cualquier forma, el panorama está cambiando rápidamente, y no nos comprometeremos a una solución de almacenamiento específica por ahora.

2.4.9 Proveniencia de la data

La seguridad y la proveniencia de data son asuntos críticos siempre que se utiliza data externa como contribuciones a Đapps y contratos inteligentes. Como las transacciones de blockchain son irrevocables, hay una clara incentiva para que participantes honestos se aseguren que las contribuciones son de fiar. También hay incentivos para partes deshonestas —así como para hackers sin escrúpulos— para manipular la data para beneficio monetario.

En la Streamr Network cada punto de data se firma criptográficamente con una clave privada perteneciente al origen de la data. El área tiene un desarrollo veloz, y muchos diferentes métodos son posibles. Los eventos pueden firmarse, por ejemplo, con una clave privada Ethereum, certificado X.509 propio de un sensor IoT, hardware confiable se fija utilizando el chip Intel SGX y el relé Town Crier[14], o un servicio TLSNotary[15] que establece un puente de data desde una API web.

Por diseño, la Streamr Network no tiene preferencias para el método utilizado para comprobar la proveniencia de data, y puede, de hecho, soportar cualquier método disponible ahora o en el futuro. Los eventos en la red siempre llevan tanto la firma en sí como la información sobre qué método utilizar para verificar la firma. Los archivos de clientes que pueden publicar y suscribirse a eventos pueden, de manera progresiva, agregar soporte para diferentes métodos abstrayendo los servicios de ejecución de cada método y facilitando la verificación de firmas desde la perspectiva de un desarrollador.

El algoritmo de firma soportado inicialmente es el mismo secp256k1 ECDSA utilizado por Ethereum. Convenientemente, esto permite a la red mapear y publicar data de manera confiable a una dirección Ethereum.

2.4.10 Confidencialidad de data

[10]Viktor Trón et al: "Introduction to Swarm" (http://swarm-guide.readthedocs.io/en/latest/introduction.html)
[11]Siehe "IPFS - The Permanent Web" (https://github.com/ipfs/ipfs)
[12]Siehe "Storj: A Peer-to-Peer Cloud Storage Network" (https://storj.io/storj.pdf).
[13]Siehe "BigchainDB: A Scalable Blockchain Database" (https://www.bigchaindb.com/whitepaper/)
[14]Fan Zhang et al.: "Town Crier: An Authenticated Data Feed for Smart Contracts", en Procedimientos del ACM de 2016 SIGSAC Conference on Computer and Communications (CCS)“, Viena, Austria, 24.-28. De octubre de 2016, P. 270-282 (https://eprint.iacr.org/2016/168.pdf)
[15]“TLSnotary - a mechanism for independently audited https sessions”, en Whitepaper, 10 de septiembre de 2014 (https://tlsnotary.org/TLSNotary.pdf)

Dado que cualquiera puede participar en la Streamr Network al correr un nodo broker, las cargas útiles de eventos de transmisiones no públicas en la Streamr Network son fuertemente encriptadas utilizando criptografía de clave asimétrica. Únicamente aquellas partes que cuenten con una clave privada autorizada pueden leer la data. Los contratos inteligentes de transmisión tienen las claves públicas de cualquiera al que se permita acceder a la transmisión. Al momento de publicación, las claves públicas de receptores autorizados son utilizadas para encriptar la data de modo que sólo los receptores autorizados puedan acceder a la data.

Técnicas de encriptado multicast[16, 17 17] pueden ser utilizadas para equilibrar el tamaño de los mensajes con la complejidad de la creación de claves. El soporte de encripción integrado soporta también monetización de data directa, y servicios tales como el Streamr Data Marketplace pueden crearse para vender o rentar acceso a contenidos de transmisión. Los Publicadores pueden reestablecer la clave de la transmisión de data para denegar el acceso de forma selectiva, p. ej., en caso de que descubran suscriptores revendiendo su data fuera de la red.

Un enfoque descentralizado combinado con encriptado brinda seguridad. La data se fragmenta en diversas locaciones físicas desconocidas, y es protegida por fuerte encriptado mientras se encuentra en tránsito y almacenada. El diseño atiende los miedos de compañías y organizaciones preocupadas sobre la posibilidad de data en peligro vía acceso físico a centros de data e instalaciones de almacenamiento.

2.5 Contratos Inteligentes Streamr

Diferentes contratos inteligentes de Ethereum sostienen la operación de la Streamr Network y el Data Marketplace. La Streamr Network utiliza contratos inteligentes para incentivar, coordinar, otorgar permisos y revisar la integridad. El Data Marketplace se basa en características proporcionadas por la red para licenciamiento de data y monetización. DATAcoin, un token ERC20, es utilizada por ambas capas de incentivación, como una medida de reputación, y como método de pago.

2.5.1 Transmisión

El **contrato inteligente de transmisión** retiene información sobre una transmisión (ver Sección 2.4.2). Además de retener información estática, lleva los permisos para la transmisión. En particular, lleva claves públicas de receptores autorizados de transmisiones encriptadas, posiblemente relacionadas a una licencia de data (ver abajo).

2.5.2 Registro de transmisión

[16] Micciancio, Daniele y Saurabh Panjwani. „Multicast Encryption: How to maintain secrecy in large, dynamic groups?" (http://cseweb.ucsd.edu/~spanjwan/multicast.html)
[17] Duan, Yitao y Canny, John. Computer Science Division, Universidad de Berkeley. „How to Construct Multicast Cryptosystems Provably Secure Against Adaptive Chosen Ciphertext Attack". (http://www.cs.berkeley.edu/~jfc/papers/06/CT-RSA06.pdf)

El **contrato de registro de transmisión** retiene información sobre transmisiones conocidas en la red. Las transmisiones pueden ser agregadas al registro para propósitos de búsqueda. El registro de transmisión puede también registrar transmisiones en el servicio de nombres de Ethereum (ENS)

2.5.3 Coordinador de red

El **contrato coordinador de red** asigna particiones a nodos broker (ver Sección 2.4.6). Los nodos broker se registran a sí mismos con el coordinador y reciben actualizaciones del estado de la red al observar el contrato inteligente.

2.5.4 Licencia de data

El **contrato de licencia de data** representa un producto enlistado en el Streamr Data Marketplace. A cambio de DATAcoin, el contrato proporciona acceso a una serie de transmisiones asociadas al registrar la clave pública del comprador con las transmisiones. La licencia de data puede ser válida por un periodo determinado. Tras la expiración de la licencia, el comprador no tendrá acceso a la nueva data publicada en las transmisiones.
La razón de ser de un contrato de licencia es retener pruebas de que el receptor tiene el derecho de acceder a una transmisión de data en términos de uso específicos e inmutables y, simultáneamente, garantizar que el proveedor de data recibe el pago acordado por data en tiempo real en la manera y el momento en que es publicada. Los términos de uso pueden ser almacenados en el contrato de licencia de data ya sea de forma directa (y marcado como necesario) o como un link al almacenamiento enfocado en contenido, como IPFS. El contrato también puede contener pruebas de requerimientos legales satisfechos como resultado de un proceso de conoce-a-tu-cliente (KYC).

Los nodos broker reportan recuentos de eventos y resúmenes criptográficos en funcionamiento a contratos inteligentes de transmisión, que en su momento puede reportarlos al contrato de licencia asociado. Los contratos inteligentes de licencia pueden implementar seguros casi arbitrarios para prevenir fraudes por parte del publicador. Pueden, por ejemplo, bloquear el pago hasta que cierta cantidad de eventos haya sido publicada en la transmisión. El pago puede hacerse también de forma gradual en el transcurso del tiempo, o evento por evento al tiempo que son publicados. Puede haber también un mecanismo para suscriptores para que señalen data defectuosa afectando negativamente la reputación del publicador (ver sección 3: sobre DATAcoin y karma). Estas características de seguridad garantizan que el publicador no obtenga pagos si no entrega la data de la calidad prometida.

3. DATAcoin

DATAcoin es el medio de compensación entre productores y consumidores de data. También es un incentivo para nodos broker funcionales en la red P2P. DATAcoin es la base para karma, la medida de reputación en la comunidad. Desde una perspectiva más amplia, es una forma de ganar exposición a data como una mercancía valiosa.

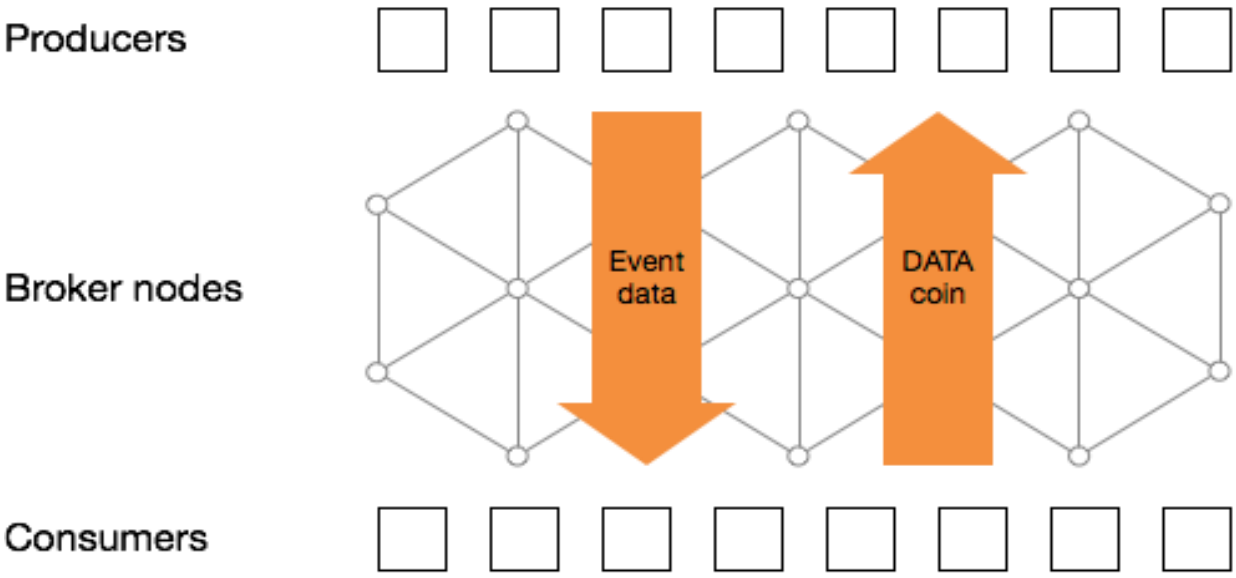


Figura 6. La DATAcoin fluye en la dirección opuesta a la data.

Hay un rol integral para un token digital en el canal de data descentralizada. DATAcoin es el token de uso común en la Streamr Network. DATA es el símbolo del token.

- El mantener y operar una red P2P requiere de recursos: tiempo, electricidad, capacidad de cómputo y ancho de banda de comunicación. La incentivación de los nodos broker participantes se describe en la Sección 2.4.7
- DATAcoin es el medio de compensación entre productores y consumidores. En otras palabras, implementa un mecanismo de monetización para productores de data. Es un incentivo para que los vendedores de data se involucren y ayuden al crecimiento de la comunidad para el beneficio de todos.
- DATAcoin es la base para karma, la medida de reputación en la comunidad de productores de data, consumidores de data y brokers de mensajería. Cada parte gana karma de transacciones con DATAcoin: Publicar data, consumir data y correr nodos broker que operan la red. Un productor de data gana karma cuando los eventos que publicó se entregan a los suscriptores. Los suscriptores ganan karma cuando reciben eventos. Los nodos broker ganan karma por ayudar con la entrega y persistencia de data. La contabilidad resulta fácil: La cantidad de nuevo karma equivale a la cantidad de DATAcoin intercambiada. La diferencia es que el karma decae y expira con el paso del tiempo, mientras que el balance de tokens permanece.

La DATAcoin se implementa como un token ERC20 en Ethereum. El contrato inteligente de token mantiene balances de DATAcoin y garantiza que los pagos se manejen en una forma autónoma y segura. Seguir el estándar ERC20 garantiza la interoperabilidad con carteras y otros tokens.

La DATAcoin será creada en un evento de generación de token (TGE) calendarizada para septiembre de 2017. Sus detalles, términos y condiciones, y el programa detallado serán anunciados posteriormente.

4. Estado actual

Ya hay una plataforma altamente avanzada lista para crear canales de data, visualizaciones y microservicios de cómputo off-chain. La plataforma proporciona un punto inicial funcional, pero para alcanzar la descentralización total debe ser preparada para correr en un contenedor descentralizado y utilizar la nueva capa de Streamr Network para transporte de mensajes.

No estamos comenzando de cero. Hay una plataforma funcional y altamente avanzada para la creación de canales de data, visualizaciones, procesamiento off-chain, y contratos inteligentes Ethereum. El software está construido para el ambiente de nube pensando en escalabilidad, integraciones y tolerancia a desperfectos. Marcos de trabajo de Big data como Kafka y Cassandra son utilizados para manejo y mensajería de data. La plataforma Streamr fue demostrada en directo en la EDCON de febrero de 2017 y en varios encuentros de blockchain desde entonces.

En lo relativo al pedigree, creamos la primera versión del software para nuestro propio uso en intercambio algorítmico de alta frecuencia hace casi 5 años. Los directivos tienen todos antecedentes financieros, en los que se desempeñaron como analistas cuantitativos (*quants*), desarrolladores de sistemas de cambio, *traders* de arbitraje estadístico (*stat arb traders*) y, en algunos casos, todos los mencionados. Las finanzas cuantitativas son un campo en el que el procesamiento automático de altos volúmenes de data en tiempo real ha estado en acción desde los últimos 10-15 años, y más. Es únicamente en años más recientes en que el mismo tipo de modus operandi y la misma clase de herramientas y plataformas están encontrando su camino hacia el mundo del IoT, IoE y, ahora, en el espacio de las blockchain.

La plataforma actual es funcional, escalable y en constante uso por clientes corporativos. Sin embargo, muchos de los componentes no se traducirán de forma directa al nuevo mundo. El almacenamiento necesita descentralizarse, y la mensajería, la funcionalidad publicar/suscribirse y la monetización y encriptado de data requieren incorporarse a la capa de transporte, mientras que la red peer-to-peer necesita establecerse junto con la coordinación e incentivación de nodos. El roadmap de cómo hacer estas cosas se presenta en la siguiente sección.

5. Roadmap

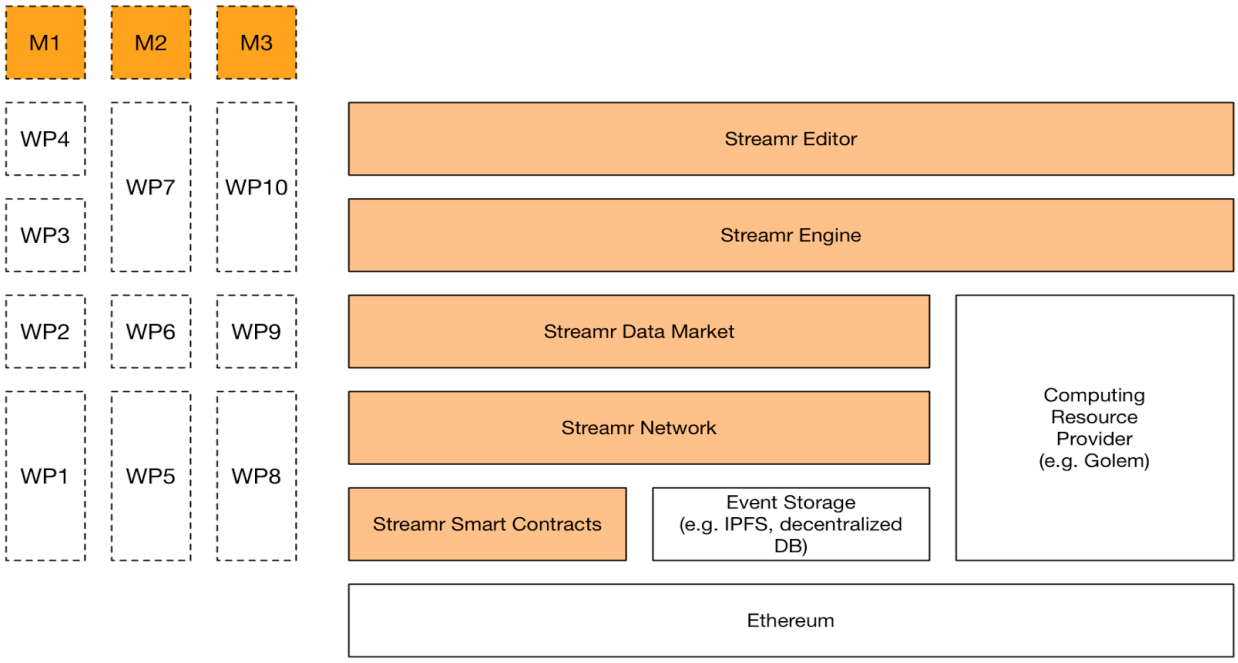


Figura 7. Roadmap de I&D para el proyecto Streamr.

El roadmap (Figura 7) está dividido en tres hitos (M1-M3). Cada hito brinda iterativamente nuevas características a las capas del stack. Cada uno de los tres hitos consiste en paquetes de trabajo (WP1-WP10). Completar todos los WP de cada hito lo completa. Cada paquete de trabajo tiene un enfoque específico en ciertas capas del stack. Se trabajará en todos los WP de un hito de manera simultánea, pero los WP del siguiente hito no se comenzarán hasta que el hito actual sea completado.

Habrá también una auditoría de seguridad al finalizar cada hito. Todos los contratos inteligentes serán auditados, así como las partes relevantes de cualquier código de contrato no-inteligente, por ejemplo, el propio cliente del broker.

Hemos elegido el enfoque integral del stack iterativo bajo el siguiente razonamiento:

- Podemos proporcionar a la comunidad algo que está trabajando y es utilizable desde el día uno.
- Estamos comenzando con un stack tecnológico existente. El stack es modular de modo que cualquier capa puede ser mejorada en cualquier momento.
- Entregables tangibles y útiles se alcanzarán sin importar cuáles de los hitos alcancemos.
- La comunidad no será dejada a su suerte con una solución a medio camino; habrá tecnología funcional que satisfaga muchos casos de uso de negocios.

5.1 Hito 1

Hito 1 lanza la primera versión de la red de entrega de data incentivada y los contratos inteligentes subyacentes. El trabajo en otras capas refuerza lo que ya tenemos y busca una total integración con el ecosistema Ethereum.

WP1 (Red, Contratos Inteligentes): Prototipo de red de brokers desentralizada.

- Crear la primera versión prototipo del nodo broker descentralizado
- Integrar firma y verificación libp2p secp256k1 ECDSA
- Protocolo de eventos
- API JSON y Websocket
- Contrato inteligente de transmisión
- Contrato inteligente de registro de transmisión
- Contrato inteligente de control de red
- Asignación de partición
- Reporte de suma de verificación
- Prevención de Exceso de carga utilizando cuotas de publicador/suscriptor
- Esquema básico de recompensa con DATAcoin

La vieja capa de mensajería por nube y la nueva red descentralizada coexistirán por un tiempo, hasta que el broker descentralizado alcance tamaño y estabilidad adecuados. El Engine y el Editor de producción existentes correrán con el viejo broker hasta que la capa de red se actualice.

WP2 (Marketplace): El esqueleto del mercado

- Descubrimiento de transmisiones de data disponibles al público, categorización y búsqueda iniciales
- Implementación del producto de transmisión, artículos disponibles para compra que garanticen el acceso a series de transmisiones a cambio de DATAcoin
- Que los usuarios puedan definir productos de transmisión y ofrecerlos en el mercado.
- Poblar el mercado con transmisiones de data en tiempo real desde diferentes verticales, como las que siguen:
    - Data de mercado financiero: precios de acciones, precios de opciones, precios de mercancías, índices de criptomonedas, índices de intercambio de dinero fiat, volumen de cambio y acciones corporativas.
    - Data de medios sociales: Twitter, Instagram, Facebook, Reddit, Flickr, etc.
    - Data de transportación: salidas, llegadas, geolocalización, velocidad, dirección de aeroplanos, naves, trenes y transporte local.
    - Data de clima: temperatura, precipitación, humedad, nubosidad, velocidad del viento, tanto actual como pronosticada
- La primera versión del mercado tendrá una especie de “llantitas de entrenamiento” centralizadas para simplificar la gestión del acceso y emular la forma centralizada/descentralizada de la red de producción.

WP3 (Engine): El motor se vuelve Ethereum

- Puente Streamr-Web3 para soportar interacciones con Ethereum desde Streamr
- Emisión de Contratos Inteligentes, soporte de ABI para contratos preintalados
- Llamadas de función local y transaccional

- Observación de eventos
- Gestión de clave y cuenta
- Soporte para diferentes redes de prueba y para la red principal
- Firmas y verificación de firma
- *Dockerizar* el Motor para Golem u otro proveedor de cómputo descentralizado

WP4 (Editor): Cómputo constante on-chain y off-chain

- Mejorar el Visual Editor para que soporte cabalmente todas las características relacionadas con Ethereum en el Engine.
- Editor de Solidity integrado para escribir módulos personalizados de contrato inteligente.
- Una selección integrada de plantillas de contrato inteligente para los casos de uso más comunes (pagos, apuestas, monitoreo de SLA, pronósticos, etc.), y la habilidad de utilizarla con facilidad.
- Transmisiones de data del mundo real a estas plantillas.
- Rehacer la Interfaz de Usuario/Experiencia de usuario (UI/UX) del Editor y la aplicación web asociada.

5.2 Hito 2

En este hito, lanzamos la primera versión del Data Marketplace junto con las características que necesita en la capa de red subyacente.

WP5 (Red, Contratos Inteligentes): Soporte para monetización y encriptado de data

- Primera versión estable
- Soporte de encriptado básico
- Contrato inteligente de licencias de data
- Soporte de contratos inteligentes como objetivo de suscripción
- Añadir soporte para métodos de firma de data posteriores, p. ej., basados en X.509, SGX
- Almacenamiento básico en almacén de bloque descentralizado o en bases de datos descentralizadas
- Implementar y utilizar karma
- Prueba de estrés, optimización de la escalabilidad

WP6 (Mercado de Data): Marketplace completamente descentralizado

- Las “llantitas de entrenamiento” retiradas de la implementación inicial del mercado en M1 para alcanzar descentralización completa, con licencias de data modeladas como contratos inteligentes en la blockchain, y utilizadas para otorgar permisos y controlar accesos
- Mecanismo de distribución de claves inicial para soportar el contenido de transmisiones de permiso controlado en red pública
- Verificar la identidad del vendedor
- Mecanismo de reputación del vendedor

WP7 (Engine, Editor): Alcanzar la descentralización

- Migrar a la nueva capa de Streamr Network
- Lanzamiento en Golem u otro proveedor de contenedor
- Tolerancia a desperfectos y recuperación de fallos en ambiente descentralizado

5.3 Hito 3

La meta del hito 3 es alcanzar la visión Streamr por completo. La I&D del hito 3 está comprometida a cambiar según se requiera, considerando que los hitos previos generarán diversidad de ideas, y la comunidad solicitará nuevas características. El hito 3 también contiene esfuerzos significativos de marketing que lleven a la adopción del stack.

WP8 (Network): Enrutamiento avanzado, ofuscación de locación

- Ofuscación de locación
- Encriptado multicast
- Prueba de estrés, optimización de escalabilidad
- Trabajo en cualquier problema detectado en lanzamientos a gran escala
- Trabajo en características solicitadas por la comunidad
- Trabajo en la integración con plataformas emergentes

WP9 (Mercado de data): Construcción de comunidad

- Agregar más transmisiones de data al Data Marketplace
- “Lista de deseos” de transmisión, programa de recompensas para acelerar adopción
- Mejoras al mecanismo de reputación
- Incremento en los esfuerzos de construcción de comunidad

WP10 (Engine, Editor): Productificación

- Mejora del UI y UX de las herramientas
- Asimilación, videos tutoriales, materiales de ayuda
- Agregar integraciones a plataformas relevantes en blockchain, IoT, AI u otros espacios

6. Equipo de gestión de proyectos

Henri Pihkala, M.Sc.

Henri es un ingeniero en de software, un emprendedor serial y ex *trader* algorítmico. Ha liderado el desarrollo de dos plataformas de *trading* algorítmico de alta frecuencia y diseñado y gestionado la construcción de la plataforma analítica distribuida de nube de Streamr. Henri es apasionado de la arquitectura compleja, la escalabilidad, la usabilidad y la blockchain.

Risto Karjalainen, Ph. D.

Risto es un científico de data y profesional de las finanzas con un Ph. D. de la Wharton School. Es un *quant* con una carrera internacional en *trading* automatizado y sistemático y gestión de bienes institucionales. Los intereses de Risto incluyen cómputo en tiempo real, aprendizaje de máquinas, algoritmos evolucionarios, finanzas conductuales, la blockchain y tecnología financiera en general.

Nikke Nylund, B.Sc.

Nikke ha sido estratega de *trading* algorítmico de baja latencia. Tiene cerca de 20 años de experiencia gerencial y empresarial como fundador y/o inversor serial en ICT y compañías de tecnología con varias salidas exitosas a su nombre. Nikke tiene un grado de BSc en Finanzas y Emprendeduría de la Helsinki School of Economics.

Michael Malka, M.Sc.

Michael es un emprendedor y tecnólogo entusiasta con 20 años de experiencia en diferentes puestos, desde desarrollador de software hasta CEO. Se ha involucrado en proyectos de software en diferentes sectores, desde *startups* hasta bancos y telecomunicaciones. Michael estudió ciencias de la computación en la University of Helsinki antes de comenzar su primera compañía de software.

7. Conclusión

Este *whitepaper* delinea nuestra visión para una columna vertebral de data en tiempo real, que sea robusta y descentralizada en forma nativa, diseñada para apps descentralizadas. Creemos que la combinación de un mercado de data en tiempo real y el canal de data será un elemento transformador para desarrolladores de contratos inteligentes de Ethereum y el ecosistema Đapp en general. Tenemos la ambición de construir un stack tecnológico considerado cabalmente e implementado en forma profesional, que atienda las necesidades futuras de nuestra audiencia y proporcione data imparable para apps imparables.

Nuestro stack tecnológico es en capas y modular, y está construido sobre una capa de transporte descentralizada. Hay una red peer-to-peer que consiste en nodos broker incentivados. La red utiliza un mecanismo de publicar/suscribirse y soporta el almacenamiento descentralizado de eventos encriptados. El rendimiento escala linealmente con el número de nodos participantes, y la red puede procesar millones de eventos por segundo.

La columna vertebral de data es un facilitador ideal en la economía M2M, en la que máquinas autónomas, bots y robots compran o venden pequeños fragmentos de data. La idea[18] es que las máquinas intercambian recursos tales como almacenamiento, capacidad de procesamiento, ancho de banda de comunicación, etc. Creemos que utilizar DATAcoins llevará a costos de transacción mucho más bajos que el trueque.

Streamr ist Teil der Computing-Revolution, bei der monolithische Lösungen durch dezentrale Computing-Alternativen ersetzt werden. Im Bereich des verteilten Computing ersetzt Golem die Azure Virtual Machines. Im Bereich Blockspeicher ersetzen IPFS, Storj und andere Azure Blob Storage. In Bereich der Datenpipelines und des Messaging ersetzt Streamr zentrale Messaging- und Eventverarbeitungsplattformen wie Azure EventHub und Azure Stream Analytics. Es findet ein Machttransfer von Konzernen und Unternehmen zu einzelnen Bürgern, autonomen Agenten, Apps und Maschinen statt, der zu Verbesserungen in den Bereichen Privatsphäre, Effizienz, Belastbarkeit und Fehlerrobustheit sowie letztendlich zu einem höheren Wohlstand für die Stammgäste der vernetzten Gesellschaft führt

[18] Alex Puig: "How the Blockchain could enable the Machine Economy (M2M)", 11 de enero de 2016 (https://www.linkedin.com/pulse/how-blockchain-could-enable-machine-economy-m2m-alex-puig)