k·tb

nodo de alta performance

Modelo de Negocios y Campaña Flipstarter

Abril 2020

Leandro Di Marco
Fernando Pelliccioni

Versión	1.0
Fecha de Revision	14 04 2020
Autores	Leandro Di Marco Fernando Pelliccioni
website	kth.cash
email	info@kth.cash
telegram	t.me/knuth_cash

Abstract

Knuth tiene la visión de llevar Bitcoin Cash a la vida de cada día. Planeamos llevarlo a la práctica construyendo una plataforma monetaria escalable que ofrezca un servicio: dinero electrónico descentralizado e incensurable. Estamos convencidos de que el camino más adecuado para tal fin implica estructuras simples y optimizadas. Knuth se mantiene firme en esa perspectiva, reconociendo en la accesibilidad el más poderoso catalizador para una adopción global.

También queremos allanar el camino para los recién llegados. Queremos ayudar a una nueva generación de desarrolladores a crear soluciones sorprendentes, a llevar el comercio trans fronteras a niveles sin precedentes.

Knuth es, en pocas palabras, una implementación de nodo completo centrada en extra performance y flexibilidad. Está diseñado para carteras, sitios de cambio, exploradores de bloques y mineros. Se caracteriza por su arquitectura modular y código elegante. Pero Knuth también es una plataforma de desarrollo que ofrece un conjunto de librerías como base para la creación de aplicaciones.

Creemos que cada implementación de Bitcoin Cash, para tener éxito debe pasar por tres pasos importantes: seguir la cadena, minar bloques, proponer mejoras. Estamos totalmente comprometidos con esa tarea.

Con un presupuesto racional para la presente campaña y un paquete de entregables flexible a discreción de los contribuidores, que no haya confusiones, nuestro compromiso para con Bitcoin Cash está presente y más fuerte que nunca. Knuth planta su bandera contra cualquier fuerza hostil, interna o externa, que incluso intente socavar la iniciativa de llevar dinero electrónico al mundo.

Nuestra política es la transparencia, nuestro proceso el impulso, nuestra cultura la competencia. El desafío de llevar Bitcoin Cash a su máximo potencial es ahora.

¡Prepárarte!

k·th

Contenidos

1. Introducción

Nuestra visión es traer Bitcoin Cash a la vida diaria. Nuestra propuesta es hacerlo construyendo una plataforma monetaria que ofrezca un servicio y solamente un servicio: dinero, en la forma de efectivo electrónico.

Al analizar el status quo en el que Bitcoin Cash se encuentra, no podemos evitar hacerlo desde una perspectiva de negocios. Esto significa, teniendo una buena comprensión y entendimiento de la competencia de voluntades representadass en la arena. Bitcoin Cash está compitiendo contra el más poderoso monopolio de todos los tiempos: el dinero fiat. Un sistema que posee sus multiples aristas aguzadas por siglos de experiencia, reforzado por miles de nodos y puntos de acceso conectados a su red, y potenciado por al menos 70 años de poder computacional.

¿Cómo puede Bitcoin Cash competir contra eso?

2. Segmento de Clientes

Contruir un sistema monetario que desafíe el aparato financiero actual, uno que brinde libertad económica a los pueblos, va a requerir de un gran esfuerzo y de mucha gente involucrada. No simplemente unos pocos, sino un sólido grupo de personas. Esto se debe a que, para competir contra el sistema monetario actual, vamos a necesitar reemplazar millones de líneas de código, miles de aplicaciones y soluciones que están en uso hoy en día, todos los días.

Tenemos que evolucionar y retirar cualquier ingenuidad de la ecuación. Bitcoin Cash es el recién llegado a un mercado que está completamente maduro. La porción que Bitcoin Cash desea debe ser conquistada, tomada, no por la fuerza, no mediante publicaciones en redes sociales, no dividiendo a la comunidad, sino a través de trabajo arduo, con el pensamiento aplicado a la acción, con infraestructura que funcione, que sea escalable y eficiente. Bitcoin Cash necesita más personas. Necesitamos atraerlos.

En Knuth estamos convencidos de que el camino de la simplicidad es el más adecuado para esa atracción. Evitar complejidad innecesaria tanto como sea posible es lo mejor para Bitcoin Cash. Knuth se posiciona firme en esa perspectiva, reconociendo en la accesibilidad la mejor opción para cada parte interesada del ecosistema. Ofreciendo una plataforma legible y fácil de entender permitirá a estas partes interesadas orientar su energía y trabajo hacia aspectos más relevantes para sus soluciones y operaciones.

Del mismo modo, reconocemos que Bitcoin Cash debe mejorar sus esfuerzos para permitir que personas calificadas lleguen y entren en sus círculos. Por alguna razón, las cosas terminan volviéndose difíciles para los recién llegados.

Con Knuth, queremos allanar el camino para los recién llegados. Queremos que su experiencia sea natural y emocionante. Queremos ayudar a una nueva generación de desarrolladores de software a crear soluciones sorprendentes, a una nueva generación de desarrolladores de negocios a llevar el comercio trans fronteras a niveles sin precedentes.

Trabajar con una actitud que fomente la complejidad en pos de la complejidad en sí misma, que rechace a los recién llegados con arrogancia, nos hará fracasar, fracasar como proyecto, fracasar como sistema monetario y

fracasar como dinero electrónico.

Por esa razón, Knuth promueve la atracción, capacitación y retención de desarrolladores de diferentes áreas y niveles. Nuestra propuesta de valor es una plataforma especialmente diseñada para ellos, construida sobre una arquitectura modular, simple de modificar, simple de expandir y fácil de aprender. Al seguir este camino, Knuth hace todo lo posible por atraer a los desarrolladores de software y de negocios, y por lo tanto a las compañías detrás de ellos, con la intención de impulsar la adopción masiva de Bitcoin Cash. Estas personas y empresas son la clave de cómo creemos que Bitcoin Cash debería avanzar, son las partes interesadas en traer el futuro al presente.

Tenemos que entender que estos desarrolladores no son solo programadores. Bitcoin Cash necesita incluir personas que pueden no tener conocimientos de programación, pero que entiendan lo que los usuarios necesitan o desean, que puedan analizar la experiencia de los mismos, que puedan comprender lo que las empresas requieren para formar parte del ecosistema, y esas personas deben ser parte integral del proceso.

En resumen, Knuth está diseñado para un mercado segmentado que incluye:

1. Mineros y pools de minería con el claro objetivo de tener un nodo de alta performance;
2. Sitios de cambio que necesiten una indexación completa confiable;
3. Empresas y negocios con la intención de construir aplicaciones sobre una plataforma modular y segura;
4. Desarrolladores que deseen llevar sus proyectos a nuevos niveles con una solución lista para el mercado;
5. Recién llegados que deseen dar sus primeros pasos en el mundo blockchain a través de una ruta directa y fácil de entender.

3. Propuesta de Valor y Logros Técnicos

A medida que la tecnología Bitcoin Cash evoluciona, crece la necesidad por contar con una variedad de disciplinas, como criptografía, programación, base de datos, redes, marketing, economía y más. No hay forma de contar con personas que cubran individualmente todos estos dominios con el nivel de experiencia suficiente, tal vez un dominio o dos, además de una comprensión general del resto o incluso menos.

A diferencia de los softwares construidos con una arquitectura monolítica, la modularización propuesta por Knuth colabora en el sentido de abrir puertas para un ecosistema diverso, donde el código se vuelve interactivo, reutilizable y confiable, fácil de leer y fácil de depurar.

Nuestra propuesta de valor se resume a lo siguiente:

Knuth es una implementación de nodo completo centrada en extra performance y flexibilidad, lo que lo hace ideal para carteras, sitios de cambio, exploradores de bloques, mineros, y para cualquiera que desee ir más lejos con la tecnología blockchain. Se caracteriza por su arquitectura modular y código elegante. Knuth también es una plataforma de desarrollo que ofrece un conjunto de librerías en varios

lenguajes de programación como base para crear aplicaciones.

Nuestros logros técnicos a la fecha son:

Alta Performance
Como fue mencionado, Knuth es, en esencia, una implementación de alto rendimiento del protocolo Bitcoin. Es una implementación de nodo completo, pero también una plataforma de desarrollo. Su núcleo está escrito en C++. Sobre el mismo, se proporcionan varias librerías y módulos escritos en diversos lenguajes de programación.

Multi-Platforma
Knuth es una solución multi-plataforma. Se lo puede usar en cualquier arquitectura computacional y sistema operativo. Solo requiere una máquina de 64 bits. Su código puede compilarse y usarse de forma nativa en Linux, Windows, macOS, FreeBSD y otros sin problema alguno.

Sistema de Build
Nuestro sistema de build está diseñado con diversas ventajas en mente. En general, estas ventajas están relacionadas con la capacidad de Knuth para detectar automáticamente la microarquitectura de los procesadores y optimizar el binario generado al momento de la compilación.

La primera de las ventajas es que Knuth automatiza la administración de dependencias externas, lo cual es ofrecido para ahorrar tiempo y esfuerzo, pero también para garantizar que solo sean instaladas las dependencias adecuadas. Esto se resume en correctitud y seguridad para los usuarios.

En segundo lugar, Knuth también automatiza la administración de módulos internos. Al instalar Knuth, nuestro sistema de compilación descargará, o en su defecto, compilará cada uno de los módulos requeridos, y luego procederá a compilar el ejecutable. Esto da como resultado una economía de tiempo de compilación.

Finalmente, teniendo en cuenta la performance, Knuth cuenta con dos modos de instalación:

- **Modo extra-performance mode**: Nuestro sistema de compilación descargará el código completo de Knuth y lo compilará aprovechando al máximo las características de las plataformas/procesadores en uso. Los tiempos de compilación pueden ser mayores, pero el resultado final será un binario súper optimizado, ideal para usuarios que necesiten esa porción extra de rendimiento..
- **Modo easy-rider**: binarios de Knuth precompilados para sistemas operativos convencionales (Linux, macOS y Windows). Estos binarios son ideales para usuarios prospectivos. Este modo focaliza en la optimización del tiempo y en una solución lista para ser usada. Los binarios precompilados están listos para las siguientes instrucciones y extensiones: 64-bits, movbe, mmx, sse, sse2, sse3, ssse3, sse41, sse42, popcnt, lzcnt, avx, avx2, aes, pclmul, fsgsbase, rdrnd, fma3, abm, bmi, bmi2, f16c, xsave, xsaveopt, cx16.

Modos de Base de Datos
Diseñado para ofrecer un alto nivel de especialización para casos de uso particulares, el nodo Knuth puede ser inicializado en 3 modos de base de datos diferentes al momento de la instalación:

- **Normal**: proporciona mempool completo, conjunto UTXO completo, bloques indexados completos. Este modo es ideal para usuarios que desean colaborar con la red, simplemente siguiendo la cadena y haciendo que los bloques/transacciones sea transmitidos.
- **Pruned**: proporciona mempool completo y conjunto UTXO completo, pero solo incluye los últimos n bloques (siendo n configurable por el usuario). Este modo está diseñado para atender las necesidades de las operaciones de minería y operadores de pools que necesitan rendimiento y confiabilidad.
- **Full-indexed**: proporciona mempool completo, conjunto UTXO completo, bloques indexados completos, transacciones indexadas completas y direcciones indexadas completas. Este modo es ideal para sitios de cambio, exploradores de bloques y para todos los que necesitan acceso directo a la información encapsulada en blockchain y para liberar todo su potencial de manera eficiente.
- **Read-only**: un modo ortogonal que se puede utilizar en combinación con cualquiera de los mencionados anteriormente. Este modo de ejecución proporciona a los usuarios solo derechos de lectura en la base de datos. Este modo es ideal para el escalado de capacidades de consulta, ya que ofrece la posibilidad de tener varios nodos en modo lectura conectados a la misma base de datos.

JSON-RPC

Knuth soporta el protocolo JSON-RPC, que es un estándar de facto en el mercado.

Protocolos de Segunda Capa

Knuth proporciona soporte interno para protocolos de segunda capa, incluyendo la indexación completa para transacciones relacionadas. En particular, este soporte fue diseñado para el protocolo Keoken desarrollado en 2018. Aunque Keoken terminó no siendo disponibilizado en forma comercial, el mismo concepto puede implementarse en Knuth para otros protocolos similares como por ejemplo el Protocolo Simple Ledger (SLP).

Modularización

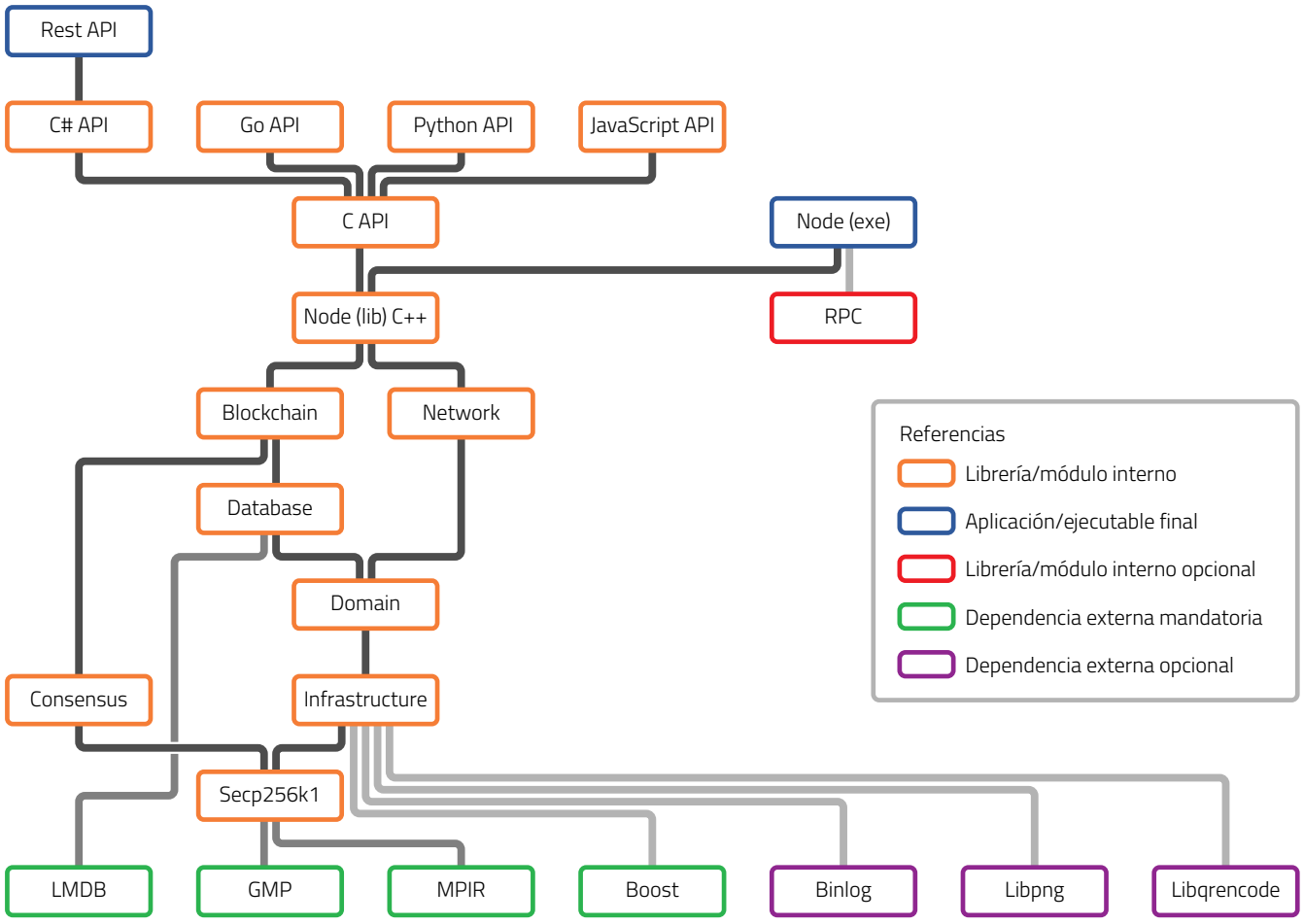
Knuth está construido siguiendo una arquitectura completamente modular. Además, cada módulo es una librería que puede ser usada de forma independiente o junto con las otras, formando lo que denominamos “el nodo”. Esto, además de la ventaja en términos de usabilidad, agrega una organización de código clara y legible que sigue el principio de responsabilidad única y, lo que es más importante, cualquier cambio de protocolo puede ser introducido en Knuth de forma más rápida y eficiente que en cualquier otra implementación.

Los módulos principales son:

- **Secp256k1**: Librería C optimizada para firmas ECDSA y operaciones de clave privada/pública en la curva secp256k1.
- **Infrastructure**: Capa de infraestructura de domain-driven-design. Actúa como una librería de soporte para todos los demás módulos. Está a cargo del registro, soporte unicode, formatos de codificación, soporte de números enteros grandes, algoritmos criptográficos y más.

- **Domain**: Capa de domain-driven-design. Contiene información sobre el dominio Bitcoin. Es el corazón del negocio del software. El estado de los objetos del negocio se mantiene aquí.
- **Consensus**: Incluye el código fuente considerado como crítico para el script de consenso de Bitcoin Cash.
- **Database**: Una base de datos blockchain de alta performance basada en LMDB. Esto es ideal para un servidor blockchain de alto rendimiento ya que las lecturas son significativamente más frecuentes que las escrituras, y sin embargo las escrituras deben proceder sin demoras. El módulo Blockchain usa la base de datos como su tienda blockchain.
- **Blockchain**: Define una API para acceder a los objetos de dominio blockchain.
- **Network**: Implementación parcial del protocolo de red Bitcoin P2P. Se excluyen todos los protocolos que requieren acceso al blockchain. El módulo Node amplía la capacidad de red P2P e incorpora Blockchain para implementar el nodo completo.

Arquitectura



- **Node**: Nodo completo de Bitcoin Cash como una librería C++. Es la puerta de entrada para acceder a los APIs Blockchain y Network.
- **Exe**: Ejecutable del nodo completo Bitcoin Cash.
- **Programming language APIs**: Además de proporcionar un nodo completo como programa ejecutable, también se ofrece un nodo como librería. Esto está diseñado para que cualquier usuario pueda crear aplicaciones utilizando las librerías en los lenguajes compatibles. La aplicación creada se convierte en un nodo ya que las librerías de Knuth operan en el mismo espacio de memoria que el nodo mismo. Esto permite un acceso eficiente a los objetos de dominio (como bloques y transacciones) sin pasar por las capas de red que hacen que el acceso sea más lento. Las librerías se ofrecen en los siguientes lenguajes: C, C++, C#, Eiffel, Go, Javascript, Python y Rust. Además, dadas las herramientas proporcionadas, los usuarios pueden crear sus propias librerías en el lenguaje de preferencia.
- **RPC**: Este módulo proporciona soporte para el protocolo JSON-RPC.
- **Rest-API (Insight style)**: Para aquellos que prefieren una API Rest, Knuth cuenta con su propia implementación de la API Insight de Bitpay. Este modulo está escrito usando nuestra API C# y tiene todas las ventajas de ejecutar el nodo Knuth por detrás. Esta implementación remarca el potencial de las API de lenguaje de programación de Knuth para crear una variedad de aplicaciones.

Procesos y Estándares de la Industria

Knuth cuenta con los mejores procesos y estándares disponibles. Está escrito en C++, un lenguaje caracterizado por su eficiencia, específicamente en C++ 17, que es el último estándar oficial de C++ disponible. Como nota, nuestra política es utilizar el último estándar disponible con al menos 3 años de madurez. Knuth utiliza las mejores librerías C y C++ del mercado, como Abseil, Boost, GMP, y ICU entre otras.

En relación al toolchain, Knuth utiliza los más valorados por la comunidad C++: GCC, Clang, MSVC, CMake, Conan, clang-tidy, clang-format.

Knuth también utiliza los siguientes servicios de integración continua, garantizando el más alto grado de conformidad dentro de múltiples sistemas operativos: Travis-CI, Appveyor, Cirrus-CI. Y en los scripts de integración continua, Knuth usa las siguientes herramientas: clang-tidy, clang-format, sanitizers y optimizaciones guiadas por perfil.

Multi Moneda

Desde los primeros días de Knuth (y su principal antepasado, Bitprim), sus desarrolladores se distinguieron por tener una mente curiosa e inquisitiva, con una orientación característica hacia la experimentación programática y de protocolo. Es por eso que Knuth, aunque centrada en Bitcoin Cash, también soporta Bitcoin (BTC) y Litecoin (LTC).

Con el tiempo, esto resultó ser de relevante importancia. Por un lado, muestra la flexibilidad de Knuth en términos de cuán fácil es agregar una nueva moneda a su código base y, en particular, qué tan rápido se puede hacer. Por otro lado, descubrimos que al adaptar el código para soportar otra moneda, se crearon espontáneamente casos de borde, lo que a su vez nos ayudó a corregir posibles errores no reportados relacionados al código de Bitcoin Cash (BCH).

Como resultado de esto, Knuth hoy en día

soporta las tres monedas, lo que puede ser interesante para sitios de cambio y carteras multi monedas que prefieran utilizar un único software de nodo en lugar de varios.

4. Plan de Desarrollo

En Knuth entendemos que el objetivo principal de Bitcoin Cash es convertirse en dinero electrónico a escala global. Por ese motivo, estamos convencidos de que cada característica o funcionalidad que sea agregadas al código, sin importar cuál sea, debe funcionar en favor de ese objetivo.

Knuth está en línea con la idea de evitar cualquier cambio que tenga el potencial de hacer que Bitcoin Cash se vuelva más complejo; no solo eso sino que cualquier cambio de protocolo debe estar orientado a:

1. Solucionar una falla de seguridad confirmada.
2. Ayudar a la experiencia cotidiana del usuario de Bitcoin Cash.
3. Hacer las tareas más fáciles para los desarrolladores.

En caso de que exista la más mínima duda, esa funcionalidad debe pasar por un proceso de maduración y análisis más extenso en el backlog, así como mayor exposición en la comunidad Bitcoin Cash para obtener los comentarios pertinentes. En términos simples, la visión principal es dinero digital.

En Knuth, creemos que para que una implementación Bitcoin Cash tenga éxito, debe pasar por varios pasos importantes. Primero, debe correr como nodo completo sin minería asociada, lo que demostrará que el nodo puede realizar la descarga de bloque inicial (IBD), ponerse al día con el último estado, seguir las reglas de consenso correctas y la cadena correcta, lo que significa que el nodo no introducirá accidentalmente cambios en las reglas de consenso que puedan conducir a la separación de la cadena principal.

En segundo lugar, la implementación debe ser capaz de crear nuevos bloques a través de minería y que la red los valide.

En tercer lugar, y no menos importante para las implementaciones, mejoras e innovaciones deben traídas al protocolo, y la comunidad debe ser convencida de aceptar estas innovaciones y actualizaciones, ayudando así al crecimiento de la comunidad.

De esta forma, el plan de Knuth a largo plazo incluye la siguiente propuesta:

1. **Implementación de tests de conformidad del Block Template para minería**
   Uno de los principales objetivos de Knuth para 2020 es demostrar a la comunidad su potencial como nodo de minería. Las diversas pruebas que hemos llevado a cabo hasta la fecha son consistentes con la idea de que Knuth está en un estado de madurez suficiente para ese propósito. Sin embargo, queremos llevar esa consistencia y seguridad al extremo, reduciendo cualquier riesgo posible a su mínima expresión y poder demostrarlo de manera confiable a la comunidad.

   Para llevar esto a la práctica, creemos que la mejor manera es garantizar conformidad con las implementaciones dominantes (Core, BCH Node, ABC, BU). Para hacerlo, queremos ser capaces de ejecutar las extensas baterías de test de las respectivas implementaciones sobre Knuth.

Para ejecutar estos tests, debemos proceder con las tareas de adaptación relevantes en el código de lo tests en sí, así como en el de Knuth. Estamos totalmente seguros de que este esfuerzo resultará en minimizar cualquier riesgo financiero asociado a las divisiones no intencionadas de la cadena, alertar a otras implementaciones de posibles incompatibilidades y un sólido reconocimiento por parte de la comunidad y usuarios con respecto a la correctitud de nuestro nodo.

Las tareas relacionadas a este proyecto son:

a. Investigación y análisis de los tests de minería de las principales implementaciones (Core, ABC, BU y BCHN). Extracción de todas las formas posibles de intercomunicación entre la batería de test y los nodos. Enumeración de esas interfaces. Tiempo estimado: 80 horas.
b. Adaptación de Knuth para admitir comandos RPC que no estén implementados pero que son necesarios para ejecutar los tests. Tiempo estimado: 160 horas.
c. Adaptación de Knuth para admitir otras variantes de inspección (contenidas en la batería de test) en el nodo (es decir, inspección de archivos log). Tiempo estimado: 160 horas.
d. Incorporación de todos los tests relevantes en la suite de tests actual de Knuth. Tiempo estimado: 80 horas.
e. Corroboración y adaptación de la batería de test que sera ejecutada en Knuth. En caso de incompatibilidad, se vuelve al primer paso. Tiempo estimado: 80 horas.
f. Creación de una API de alta performance para poder ejecutar las baterías de test reemplazando JSON-RPC. Nota: La ejecución de tests es demandante en términos de tiempo, lo que retrasa el desarrollo y el mantenimiento. También conlleva un costo en los servicios de CI (Integración Continua). Desarrollar una API más eficiente que reduzca los tiempos de test. Tiempo estimado: 320 horas.
g. Adaptación de la batería de test para que funcione con la nueva API de tests. Tiempo estimado: 160 horas.

2. **Remover la limitación de 25/50 transacciones encadenadas**
   Entendemos que una buena parte de la comunidad Bitcoin Cash desea remover esta limitación. Por ese motivo lo tomamos como una prioridad para nuestro equipo de desarrollo. Pero también entendemos que eliminar esta limitación no es simplemente cambiar una constante por otra, sino mejorar el algoritmo mediante el cual se agregan nuevas transacciones al Mempool.

   Las implementaciones de referencia utilizan un algoritmo de orden cuadrático. Creemos que podemos desarrollar una metodología más eficiente para solucionar el problema. Esta tarea se encuentra actualmente 60% avanzada. Tiempo restante estimado: 400 horas..

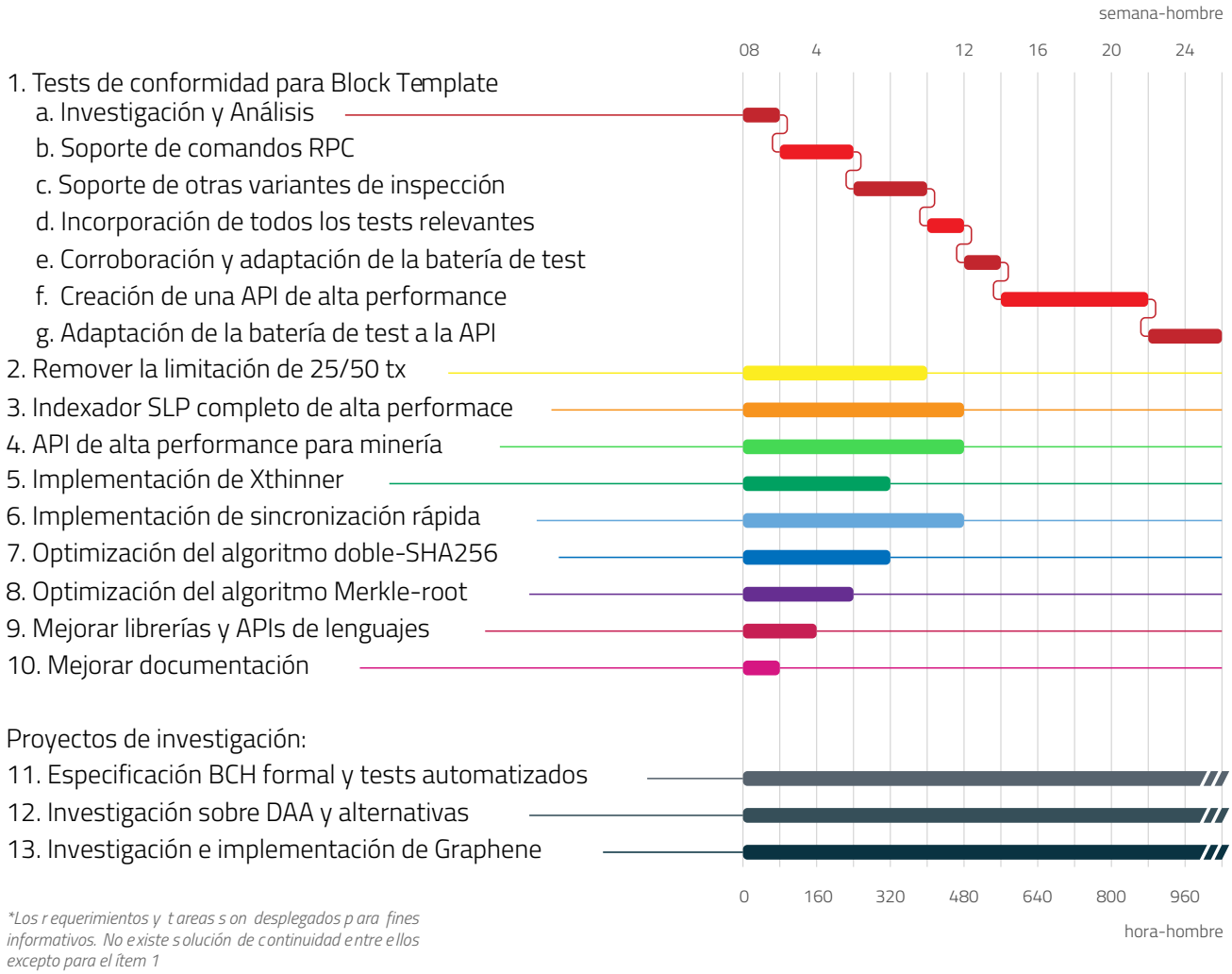
3. **Indexador Single Ledger Protocol (SLP) completo de alta performace**
   Single Ledger Protocol (SLP) ha ganado impulso en la comunidad Bitcoin Cash como un protocolo de segunda capa. Creemos que tener un indexador completo eficiente dentro del nodo sería de gran utilidad para la comunidad en su conjunto y particularmente para las aplicaciones

creadas sobre nuestra plataforma o las que la usan como servicio. Tiempo estimado: 480 horas.

4. **API de alta performance para minería**
   Knuth está enfocado en la performance. Una de las áreas en las que el rendimiento se convierte en un factor diferenciador es en la minería. Nuestro análisis indica que aunque el protocolo JSON-API puede ser de gran utilidad para ciertos procesos, no lo es tanto para minería. Esto se debe a que está construido en HTTP, un protocolo de red de muy alto nivel para este tipo de actividad. Además, la codificación JSON puede verse como generalista e ineficiente en comparación con una codificación diseñada específicamente para uso en minería. Tiempo estimado: 480 horas.

5. **Implementación de Xthinner**
   La propagación de bloques es de gran

Plan de Desarrollo



**Los requerimientos y tareas son desplegados para fines informativos. No existe solución de continuidad entre ellos excepto para el ítem 1*

importancia para la red en general, pero en particular, para los mineros y los operadores de pools. Xthinner ha mostrado una mejora significativa en la propagación de bloques, y su implementación en Knuth sería valiosa. Tiempo estimado: 320 horas.

6. **Implementación de una sincronización rápida**
   Tener un nodo listo para ser utilizado en minería lo más rápido posible es uno de nuestros objetivos. Es por eso que queremos implementar UTXO commitments o cualquier otra tecnología que permita la sincronización rápida de nodos para su uso en minería. Tiempo estimado: 480 horas.

7. **Optimización del algoritmo doble-SHA256**
   El algoritmo SHA256 (doble SHA256) es de suma relevancia en un nodo Bitcoin Cash. Hemos estado explorando cómo mejorarlo sustancialmente aprovechando las instrucciones vectoriales presentes en los procesadores modernos. Esto mejorará significativamente la validación de bloques y el cálculo de raíz de merkle. Tiempo estimado: 320 horas.

8. **Optimización del algoritmo Merkle-root**
   A medida que Bitcoin Cash escale y la adopción aumente, el ecosistema verá más transacciones por bloque. Vale la pena mencionar que los algoritmos de raíz de Merkle no son del todo eficientes en relación al consumo de memoria cuando el número de transacciones aumenta. Hemos estado explorando cómo mejorar este comportamiento, obteniendo también una mejora en los tiempos de validación de bloques y la creación de los template de bloque. Tiempo estimado: 240 horas.

9. **Mejorar librerías y APIs de lenguajes**
   El mantenimiento y la mejora continua de librerías y APIs es una prioridad. Aunque este sea un trabajo continuo, nos gustaría poder dedicarle al menos 160 horas en los próximos 6 meses. Tiempo estimado: 160 horas.

10. **Mejorar documentación**
    La documentación es una herramienta fundamental para la exposición y el uso adecuado de Knuth. Aunque este también sea un trabajo continuo, nos gustaría poder dedicarle al menos 80 horas en los próximos 6 meses. Tiempo estimado: 80 horas.

11. **Proyectos de investigación:**
    Además de las tareas específicamente dirigidas, tenemos una serie de proyectos de investigación en backlog que serán beneficiosos no solo para Knuth sino para todo el ecosistema. Son proyectos de gran escala que implican una excelente comunicación e interacción con la comunidad y otras implementaciones.

    i. **Especificación formal para Bitcoin Cash y tests automatizados**
       Aunque tener una especificación de Bitcoin Cash escrita en lenguaje humano es claramente importante, ya que facilita el mutuo entendimiento entre los desarrolladores involucrados, ya sea que trabajen en la implementación de nodos u otros servicios de infraestructura, creemos que Bitcoin Cash se beneficiaría enormemente de contar con una especificación más rigurosa.

Por tal razón, Knuth propone escribir una especificación formal en un lenguaje de programación lógico diseñado precisamente para la verificación matemática automatizada de la correctitud del software.

El objetivo final es demostrar que una implementación determinada de Bitcoin Cash funciona como se espera, automáticamente, ejecutando un programa informático.

Plan de largo alcance. Duración mínima: 2 años..

ii. **Investigación sobre DAA y alternativas**
El algoritmo de ajuste de dificultad (DAA) actual ha sido percibido desde diversas perspectivas por el ecosistema Bitcoin Cash desde su incepción, algunos positivas y otros negativas. En Knuth, queremos participar en el proceso de investigación para descubrir los efectos reales de este algoritmo en las operaciones de minería y, si es necesario, proponer mejoras o incluso un desarrollo alternativo. Sabemos que este es un proyecto que requiere una gran transparencia y participación de la comunidad.

iii. **Investigación e implementación de Graphene**
Nuestro análisis inicial acerca de Graphene lo muestra como una opción interesante como mecanismo de propagación de bloques. Sin embargo, es una tecnología que requiere mayor investigación y pruebas antes de ser implementada. Nuestra propuesta para mejorar la propagación de bloques sería primero implementar Xthinner, al tiempo que la investigación requerida sobre Graphene es llevada a cabo. En caso de resultados positivos se procedería con la implementación de Graphene.

Nota: Todos los tiempos estimados en este plan a largo plazo están basados en aproximaciones técnicas y cálculos utilizando los recursos disponibles a la fecha. En caso de existir algun cambio, será publicado debidamente en tiempo y en forma con las justificaciones requeridas a través de los canales oficiales de Knuth, de esta manera, manteniendo la transparencia para con la comunidad.

5. Entregables y Agenda

Todas las tareas mencionadas anteriormente representan un plan ambicioso que, si bien estamos convencidos traerá beneficios para el ecosistema Bitcoin Cash, sabemos también que es de largo alcance.

Dadas las condiciones actuales del mercado, parece relevante hacer uso de la propuesta Flipstarter de la mejor manera posible. En nuestro caso, esto se traduce en presentar una campaña con un alcance limitado, pero que nos permite mostrar el valor ya invertido en Knuth, así como su potencial futuro.

Por esta razón, presentamos una campaña para financiar 960 horas hombre (aproximadamente 6 meses) que se distribuirán a lo largo del ciclo 2020. Desde esta perspectiva, nuestros entregables claramente no pueden incluir de forma exhaustiva la lista completa que presentada más arriba como plan general. Aunque tenemos nuestras preferencias, nos gustaría permitir que los potenciales contribuidores elijan, de acuerdo con su criterio, cómo los fondos provistos deberían ser usados.

Al hacer sus respectivas promesas al proyecto Knuth, los contribuidores pueden agregar como comentarios, dentro de la plataforma Flipstarter, el número ordinal de las tareas propuestas de su preferencia. En el caso de obtener fondos, Knuth hará todo lo que esté a su alcance para cumplir primero las tareas con más votos. En caso de no existir detalles proporcionados, Knuth asumirá el orden presentado.

Dada esta metodología que proponemos, es difícil para nosotros presentar una lista de entregables bajo un calendario fijo. Pero creemos que este es un método excelente que brinda a la comunidad un espacio interesante para la participación. Nuestros financiadores podrán expresar sus opiniones sobre qué tarea prefieren ver primero materializada de forma clara y transparente.

Paralelamente, existen otras tareas y actividades asociadas que no consideramos lo suficientemente relevantes como para ser incluidas en el presente documento, ni tampoco fueron contabilizadas de forma independiente al momento de elaborar un presupuesto que tenga sentido. Estas actividades están relacionadas con la preparación de la campaña Flipstarter, la actualización del sitio web, la reparación de errores y mantenimiento del nodo, la administración de versiones, devops, equipamiento de pequeño porte y gastos menores..

6. Presupuesto

El gran desafío de cualquier campaña de recaudación de fondos hoy en día es el complejo contexto socioeconómico en el que nos encontramos, donde los efectos del virus COVID-19 están devastando la sociedad. En paralelo, los proyectos relacionados al ecosistema Bitcoin Cash también tienen sus desafíos bajo el status quo actual.

Aunque estos dos factores no nos desmoralizan, porque estamos seguros de estar ayudando a construir una sociedad mejor, es importante tenerlos en cuenta. Esto es especialmente cierto cuando se trata de presentar un presupuesto financiero como el que estamos haciendo.

Tenemos claro los costos de un proyecto de este tipo. Tenemos muy claro el precio internacional de desarrolladores de software senior, así como los costos de hacer negocios e impulsar una organización. Pero también tenemos muy claro la situación por la que Bitcoin Cash está atravesando, y en Knuth, no nos sentimos cómodos imponiendo una carga adicional. Pero también es cierto que estamos interesados en mostrar el potencial de nuestro trabajo y nuestra solución, y principalmente colaborar con la comunidad.

Por todas estas razones, hemos decidido presentar una campaña limitada en términos de entregables y presupuestos financieros racionales. El presupuesto que solicitamos para las 960 horas hombre de trabajo es de USD 100,000 (BCH 460 al momento de escribir este documento).Esta es nuestra forma de colaborar con el ecosistema, de mostrar nuestro valor, de comenzar pequeño para crecer después lo más fuerte posible. Danos la oportunidad de probarlo.

7. Planes de Respaldo

En el caso de que nuestra campaña Flipstarter no obtenga los fondos necesarios, planeamos poner a disposición otros medios para recibir fondos de posibles contribuidores. Esas fuentes serán informadas en breve por los

canales oficiales.

Con respecto al desarrollo técnico de Knuth, en caso de una campaña fallida, nuestro equipo entrará en un modo de mantenimiento y hará todo lo que esté a su alcance para mantener el nodo actualizado y bajo las reglas de consenso así como lo ha estado haciendo hasta la fecha. Cualquier nuevo desarrollo/investigación y el tiempo requerido para ponerlo en práctica pasarán por un análisis detallado bajo el contexto adecuado.

De cualquier manera, Knuth es una iniciativa open source y agradece cualquier colaboración voluntaria, sea técnica como financiera, para poner en práctica el plan presentado. Damos la bienvenida a cualquiera que quiera colaborar.

Al margen de eso, Knuth se encuentra en la fase de evaluación de nuevas fuentes de ingresos que no dependan exclusivamente de la recaudación de fondos, sino de la entrega de servicios específicos al ecosistema Bitcoin Cash. Se pueden encontrar más detalles sobre esto en la sección Flujos de Ingresos.

Un aspecto no trivial a la hora de considerar una campaña de recaudación de fondos es la volatilidad de Bitcoin Cash en el corto plazo. En el caso de que nuestra campaña Flipstarter tenga un final exitoso, no nos gustaría nada más que mantener los fondos recaudados en BCH como unidad de cuenta, y poder consumirlos directamente sin intercambios involucrados, pero sabemos que esto trae aparejado algunos desafíos y puede comprometer los fondos obtenidos negativamente.

Una solución posible sería mantener el 50% de los fondos obtenidos en BCH y el 50% restante en alguna stablecoin como USDH. Cualquier asunto relacionado con este tema será debidamente abordado de manera oportuna y con la retroalimentación adecuada de la comunidad.

Como nota importante, vale la pena mencionar que bajo cualquier escenario posible durante la próxima actualización el 15 de Mayo de 2020, Knuth seguirá la cadena con mayor prueba-de-trabajo.

8. Políticas, Procesos y Cultura

Canales
Knuth es un proyecto open source que se esfuerza por agregar valor al ecosistema Bitcoin Cash a través de una saludable ambición, pero también con su piedra fundamental en la realidad. Por esta razón, queremos estar cerca de nuestros usuarios y clientes.

En breve tendremos nuestro sitio web actualizado y en funcionamiento. También tenemos nuestros recursos en GitHub, que están abiertos a cualquier persona que se sienta inclinada a participar y colaborar. Alentamos no solo a los miembros de la comunidad a hacerlo, sino también a los recién llegados, creyendo que nuestra fortaleza está en la diversidad y en el intercambio de conocimientos bajo un código de mutuo respeto y cooperación.

Nuestro sitio web y la cuenta read.cash son los canales previstos para comunicaciones oficiales e informes periódicos, ya sean financieros o técnicos. También contamos con Telegram, Slack y correo electrónico disponible para el público. Si es necesario, no dudes en enviarnos un mensaje. Si está interesado en correr Knuth, construir algo genial con él o simplemente probarlo, déjanos un mensaje y haremos todo lo posible para ayudarte.

Sitio Web: kth.cash
Github: github.com/k-nuth/kth
Email: info@kth.cash
Telegram: t.me/knuth_cash
Read.cash: read.cash/@kth
Slack: k-nuth.slack.com
Twitter: @KnuthNode

Relacionamiento de Usuarios
Nos gustaría tener una relación fluida con nuestros usuarios, con otras implementaciones de nodos y con la comunidad en general, donde bajo los preceptos de colaboración y co-creación podamos sentar las bases para una relación profesional duradera.

Queremos estar particularmente presentes para los nuevos desarrolladores en el ecosistema. Queremos crecer junto con ellos, aprender y encontrar soluciones juntos. Knuth fue diseñado con ellos en mente, y ese camino no será abandonado sino motivado.

Asociaciones Clave
La colaboración entre implementaciones de nodos es de fundamental importancia para el beneficio del ecosistema Bitcoin Cash. Este concepto está profundamente arraigado en la filosofía de Knuth. Así como también es bastante claro que una competencia saludable es beneficiosa y, desde todos los puntos de vista, inspiradora, por ser un reflejo interesante de las fuerzas que gobiernan el libre mercado.

Basados en los principios de colaboración y competencia saludable, queremos aprender de otras implementaciones de nodos y compartir experiencias, ya sean estrategias tecnológicas o comerciales. Sabemos que este camino generará beneficios para la comunidad. Para competir, es necesario maximizar la experiencia de usuario, mantenerse en innovación permanente sin sacrificar confiabilidad, comprender dónde estamos y ver el camino a seguir.

Ese es nuestro compromiso, que está suscrito el ethos de Bitcoin Cash

Nota: Knuth es parte de un grupo de implementaciones de nodos que practica la divulgación responsable de eventuales problemas de seguridad.

Tiempo, Política e Interés
El desafío de llevar Bitcoin Cash a su máxima potencia es aquí y ahora, pero nuestra comprensión indica, que como ecosistema, no tenemos mucho tiempo para llevarlo a la práctica. En Knuth, entendemos a Bitcoin Cash como un producto. Como producto, necesita usuarios, y los usuarios solo vendrán con una experiencia de usuario aumentada. En Knuth, estamos profundamente interesados en este aspecto y en cómo podemos facilitar el camino en esa dirección.

Bitcoin Cash necesita al menos cien veces más usuarios en los próximos años. Si no podemos lograr eso, nunca veremos la verdadera visión de Bitcoin realizada. Y esto no tiene nada que ver con la parte técnica. Tiene más que ver con los negocios. El sistema financiero fiat ya está en conocimento de la existencia de Bitcoin Cash. Tiene una clara imagen del objetivo de Bitcoin Cash. Ya les hemos mostrado lo que queremos. Lo hemos declarado a los cuatro vientos. Y, sin embargo, desde el punto de vista estratégico, estamos fallando.

Una vez que una estrategia es declarada, no hay mucho tiempo para ejecutarla. No hay tiempo para esperar y pensar. No, se comanda y se opera, porque de lo contrario, cualquier posible oponente (el sistema financiero fiat) tendrá la posibilidad de adaptarse. Para cuando se

alcance el objetivo, será evidente que el mismo oponente ya se encuentra allí, esperando, más fuerte que antes. Este es el juego en el que nos encontramos. Es un juego que no ganaremos si continuamos en esta dirección. Es un juego que, nos guste o no, tiene política e intereses asociados en su mismo núcleo.

Política porque involucra personas. La economía es social y su medio una red. Y donde hay personas hay política. Interéses porque implica dinero. Nuestro producto es dinero. Y donde hay dinero, hay intereses. La política y los intereses son parte del juego. Es imposible eliminar la política porque de hacerlo, estaríamos eliminando a las personas. Del mismo modo, es imposible eliminar los intereses porque de hacerlo, estaríamos perdiendo el sistema monetario que queremos construir. Por lo tanto, debemos comprender de una vez por todas que Bitcoin Cash se basa en personas y en dinero, e involucra política e intereses. Si el ecosistema Bitcoin Cash no cae en la cuenta de esto lo suficientemente rápido, nunca alcanzará su objetivo.

Knuth tiene una dirección clara, atraer más personas y dinero al ecosistema Bitcoin Cash. Si tenemos éxito, esperamos más política y más intereses. Sin lugar a dudas es un desafío, pero es necesario para crear el sistema que queremos a escala global.

9. Responsabilidad

Knuth comprende la importancia de la transparencia para con la comunidad y tiene la intención de cumplir con ese estándar de forma plena. Knuth publicará reportes de progreso mensuales detallando los aspectos relevantes de la operación.

Estos reportes estarán disponibles a través de los canales oficiales mencionados anteriormente. Incluirán, entre otras cosas, métricas generales, progreso de tareas, entregables ofrecidos y estados financieros relacionados con los fondos provistos por la comunidad. Cada uno de estos aspectos incluirá sus correspondientes formas de verificación, como los commits de Github para aspectos técnicos (desarrollo de software) y direcciones/carteras/transacciones para aspectos financieros.

La comunidad Bitcoin Cash dispondrá de acceso a este material, y alentamos a cualquier parte interesada a usarlo como base para cualquier inquietud o pregunta relacionada. Queremos crecer con responsabilidad y transparencia.

10. Flujos de Financiación y de Ingresos

En Knuth, tenemos el más alto respeto por el voluntarismo y las iniciativas auto establecidas. Sabemos que son de gran importancia en la comunidad open source. Y si bien aceptamos la ayuda de todos aquellos que están dispuestos a ofrecerla, tenemos claro que el camino por delante es muy exigente en términos de recursos, aún más en las condiciones antes mencionadas. Estamos en una carrera contra el tiempo, y nuestro gran oponente no es ni más ni menos que el sistema financiero fiat.

Para mantener la carrera necesitamos un flujo de caja que no es en absoluto despreciable. Al mismo tiempo, no tenemos intenciones de convertirnos en una carga para el ecosistema que pretendemos ayudar, eso nos convertiría en parásitos, y no es el camino que hemos trazado para Knuth.

Por otro lado, queremos evitar, a toda costa, iniciativas oscuras con el potencial de generar

una mala imagen para nuestra organización o desatar teorías de conspiración sobre cómo Knuth obtiene sus fondos. Nuestro compromiso es con la transparencia. Tenemos la intención de mantener una política de apertura con respecto a nuestro plan de negocios y que sea acelerada en línea con las corporaciones del ecosistema.

Nuestros planes se pueden agrupar en dos aspectos: flujo de financiación y flujo de ingresos.

Flujo de Financiación
En primera instancia, tenemos la recaudación pública de fondos como mecanismo principal de financiación para llevar a cabo nuestras operaciones. Knuth participa en la campaña Flipstarter de Abril de 2020, la cual consideramos un paso significativo en la evolución de la recaudación de fondos en Bitcoin Cash.

Nos encantaría tener los recursos como para integrar la tecnología Flipstarter en nuestro sitio web y así continuar con nuestras propias campañas, pero por el momento, ese objetivo está más allá de nuestro presupuesto.

Sin detrimento de eso, Knuth también cuenta con una forma directa de financiación por requerimiento/funcionalidad a través de su sitio web (kth.cash), donde cada elemento incluye información detallada y los fondos mínimos necesarios tanto para comenzar como para finalizar la tarea.

También, estamos analizando la posibilidad de lanzar un consorcio de software bajo el compromiso de ser fundamentalmente descentralizado. Este consorcio dará la bienvenida a empresas, universidades e instituciones de investigación que deseen:

- Avanzar en el estado-del-arte de las implementaciones de nodos;
- Contribuir a la investigación en la integración de tecnología Bitcoin Cash;
- Apoyar la formación de estudiantes en tecnología Bitcoin Cash.

La participación en dicho consorcio tendría una cuota de membresía a cambio de beneficios tales como:

- Acceso temprano a los resultados de investigación mediante reportes y/o software del consorcio;
- Colaboración en temas de interés mutuo;
- Derechos de participación y voto en el comité del consorcio.

Esta idea y sus diversos aspectos se encuentra aún en estado de desarrollo y análisis. Cualquier actualización relevante se comunicará de manera oportuna a través de canales oficiales.

Flujo de Ingresos
En segunda instancia, Knuth, con objetivos de crecimiento exigentes, quiere conquistar su espacio como organización comercial, en el cual empresas de innovación relacionadas a Bitcoin Cash nos lleven a nuevas fronteras al tiempo que cumpliendo la visión del dinero electrónico para el mundo.

Esperamos que nuestro sentido de propósito común aproximará a las personas queriendo ser parte del desarrollo de productos y servicios Bitcoin Cash de calidad. Esto, esperamos, traerá un flujo de ingresos que sera submitido a aumentar nuestra oferta en beneficio del ecosistema.

Estos planes comerciales, que serán

notificados en tiempo y forma, no interferirán de manera alguna con nuestra filosofía open source. Nuestro producto bandera, Knuth, continuará siendo abierto al mundo, siempre.

Nuestro énfasis está en la performance, no solo en los productos y servicios ofrecidos, sino también en la forma en la que operamos. Nuestros principios sociopolíticos y metodologías operativas nos alejan de las organizaciones burocráticas y de lenta respuesta. Nos esforzamos por procesos que se puedan deconstruir en unidades simples, procesos fáciles de entender y resultados productivos.

11. Equipo

Si bien Knuth puede parecer un recién llegado a la escena de implementaciones de nodos, esto es solo una impresión superficial. Analizando un poco más en profundidad, el linaje tecnológico del que Knuth es parte se hace evidente. Knuth es el descendiente directo del nodo Bitprim, que a su vez, es descendiente de Libbitcoin, creado en 2011, que es la segunda implementación completa del protocolo Bitcoin, después del cliente original. Aunque existen diferencias considerables entre Knuth y sus predecesores, el primero intenta sacar el máximo provecho de su memoria genética, por así decirlo, incrustada en su código.

El equipo está formado por personas provenientes de dos ramas principales: desarrollo de software y negocios corporativos, en ambos casos, con vasta experiencia. A la fecha, el equipo es optimizado y funcional, con la intención explícita de ganar velocidad y expedición sin comprometer la robustez.

Para obtener más informaciones sobre nuestro equipo, visita nuestro sitio web en, check out our website at www.kth.cash ■