**Plantilla del Estado del Arte**

**Author (s):** Danushka Jayasinghe, Sheila Cobourne, Konstantinos Markantonakis, Raja Naeem Akram and Keith Mayes

**Títle of paper:** Philanthropy On The Blockchain

**Journal:** Lecture Notes in Computer Science

**Volumen: 10741**

**pag – pag (year): 25-30 (2017)**

**Problema que el autor desea resolver (Max 0.5 página)**

Este artículo explora cómo la cadena de bloqueo puede en el sector filantrópico, a través de donaciones caritativas, servicios en moneda fiduciaria o Bitcoin a través de una plataforma de donantes basada en la web. El estilo filantrópico se utiliza luego para un estudio de caso que proporciona ayuda humanitaria.a una comunidad que vive en un entorno geográfico difícil

con disponibilidad limitada de Internet. Un sistema de pago móvil basado en SMS se propone que las donaciones recibidas se aprovisionen con los fondos existentes Red GSM, teléfonos móviles muy básicos y One Time Password (OTP) fichas de seguridad. El esquema propuesto se evalúa finalmente en cuanto a la seguridad mientras se discute el impacto que tiene en las organizaciones benéficas y los donantes.

**Descripción del aporte del autor (1 – 1.5 páginas)**

{Procedimiento realizado}

Primero, investigar los beneficios del blockchain:

1. Transparencia de las donaciones: al utilizar las direcciones de Bitcoin para las donaciones existe una pista de auditoría disponible públicamente que detalle exactamente adónde fue a parar una donación en particular.

2. Reducción de los costos de transacción: Las bajas tarifas de transacción internacional son una de sus características de los pagos en cadena, como se observa en el cuadro 1. Moneda Bitcoin (BTC), Reino Unido, Estados Unidos Dólar (USD), Libra esterlina (GBP).

3. Velocidad de la donación: Todas las transacciones de Bitcoin se emiten inmediatamente. Cada transacción que se incluye en un bloque extraído válido y se añade a la cadena de bloques se llama una confirmación que dura poco más de siete minutos.

4. Provisión de donaciones: La provisión de las donaciones a los beneficiarios puede ser

desafiante.

Segundo, la propuesta:

El autor propone un sistema en el que un donante puede realizar su donación en Bitcoin a través de una plataforma de donantes. Los donantes de Bitcoin pueden utilizar cualquier billetera/cliente de Bitcoin para donar, o usar moneda fiduciaria que se convierte automáticamente en Bitcoin por un intercambio en línea. Una vez que se hace una donación, el donante puede consultar los fondos donados han sido utilizados o no. La organización benéfica luego utiliza las donaciones para asignar la ayuda financiera a los beneficiarios individuales. Los beneficiarios pueden entonces realizar transacciones de Bitcoin para las actividades diarias.

Tercero, la elección del mejor método de transacción:

Opción 1: Las direcciones multi-firma se derivan usando una multi-firma en el que se necesita más de una clave privada para autorizar una transacción. Por ejemplo, una multi-firma 2 de 3 es cuando se asocia una dirección Bitcoin con tres claves privadas y se necesitan al menos dos de las tres claves privadas para autorizar una transacción de Bitcoin. En nuestra propuesta, usamos'Pay To Script Hash' (P2SH) para procesar multi-firmas.

Opción 2: Los contratos inteligentes pueden definirse como un conjunto de instrucciones representadas en código informático publicado en una red distribuida, que recibe entradas,

ejecuta instrucciones y proporciona salidas. Puede permitir que una organización benéfica ofrezca características adicionales tales como: aprovisionamiento rutinario de donaciones cuando los beneficiarios son bajos en efectivo, la emisión de pequeños préstamos microfinancieros, el mantenimiento de registros, la donación solicitudes a los donantes e informes automáticos de auditoría de una actividad benéfica.

Por ultimo, propone: El modelo filantrópico en un entorno offline.

Los esquemas basados en cadenas de bloques tienen restricciones, tales como requerir Internet y sistemas compatibles dispositivos: ordenadores, tabletas o teléfonos inteligentes que puedan realizar funciones criptográficas procesos. Personas en una zona geográfica sin acceso a Internet fiable le resultaría difícil utilizar las transacciones basadas en monedero alojado. Hay más cobertura de red GSM que el acceso a Internet en la mayoría de los países del mundo, y el uso de teléfonos móviles dentro de la cobertura de la red GSM es considerablemente mayor en comparación con otras tecnologías de comunicación, por lo que estanos indica que consideremos una solución basada en el servicio de mensajes cortos (SMS).

{Conclusiones}.

Este documento identificó en primer lugar las ventajas de las cadenas de bloques para las organizaciones benéficas, y luego analizó cómo podrían emplearse las soluciones de cadena de bloques, incluso con su potencial restricciones. La primera contribución es un nuevo modelo filantrópico que apalanca la blockchain Bitcoin. El sistema de pago utiliza ya sea una 2 de 3 firmas múltiples proceso de transacción con la red Bitcoin, o un contrato inteligente para servicios avanzados de utilizando la red RSK. La segunda contribución es un SMS Sistema de pago Bitcoin que se puede utilizar en un entorno offline a través de la función red GSM existente.

**Referencias bibliográficas referenciadas en el informe (0.5 página)**

* 1. Coinapult SMS, https://coinapult.com/sms/info
* 2. Rootstock platform, http://www.rsk.co/
* 3. BTC For SMS (2017), <http://www.btcforsms.com/>
* 4. FlexiSpy (2017), <https://www.flexispy.com/en/features/spoof-sms.htm>
* 5. GiveTrack: Donation tracking (March 2017), https://bitgivefoundation.org/ bitcoin-charity-2-0-initiative/
* 6. M-PESA (December 2016), https://www.safaricom.co.ke/personal/m-pesa