Scaliter, Ariel E.

Working Paper

Descentralización de compra y distribución de ayuda alimentaria utilizando blockchain, contratos inteligentes y múltiples tokens fungibles

Serie Documentos de Trabajo, No. 724

Provided in Cooperation with:
University of CEMA, Buenos Aires

Suggested Citation: Scaliter, Ariel E. (2020) : Descentralización de compra y distribución de ayuda alimentaria utilizando blockchain, contratos inteligentes y múltiples tokens fungibles, Serie Documentos de Trabajo, No. 724, Universidad del Centro de Estudios Macroeconómicos de Argentina (UCEMA), Buenos Aires

This Version is available at:
https://hdl.handle.net/10419/238349

UNIVERSIDAD DEL CEMA
Buenos Aires
Argentina

Serie
DOCUMENTOS DE TRABAJO

Área: Finanzas

DESCENTRALIZACIÓN DE COMPRA Y DISTRIBUCIÓN DE AYUDA ALIMENTARIA UTILIZANDO BLOCKCHAIN, CONTRATOS INTELIGENTES Y MÚLTIPLES TOKENS FUNGIBLES

Ariel E. Scaliter

Abril 2020
Nro. 724

www.cema.edu.ar/publicaciones/doc_trabajo.html
UCEMA: Av. Córdoba 374, C1054AAP Buenos Aires, Argentina
ISSN 1668-4575 (impreso), ISSN 1668-4583 (en línea)
Editor: Jorge M. Streb; asistente editorial: Valeria Dowding jae@cema.edu.ar

Descentralización de compra y distribución de ayuda alimentaria utilizando blockchain, contratos inteligentes y múltiples tokens fungibles.

Ariel E. Scaliter*
UCEMA, Abril 2020

Resumen

La tecnología de Blockchain aplicada a la distribución de ayuda alimentaria para poblaciones vulnerables permite optimizar de manera significativa los costos de logística, la transparencia y la velocidad en que la asistencia llega a los beneficiarios. La descentralización de las compras contribuye a la reactivación de la economía regional y al empleo potenciando las posibilidades de los beneficiarios de la ayuda alimentaria. También constituye una oportunidad única para testear desde el Banco Central las tecnologías que podrían utilizarse para la implementación de una moneda digital soberana (CBDC). Los resultados y conclusiones del presente trabajo aplican a la mayoría de los países en desarrollo y a aquellos con crisis alimentaria a partir de la pandemia del covid-19.

Palabras claves: Blockchain, CBDC, Tokens Fungibles, Emergencia Alimentaria, Contratos Inteligentes, Transparencia, Descentralización

* Los puntos de vista del autor no necesariamente representan la opinion de UCEMA.

Introducción

En la actualidad existe una demanda creciente a partir de los efectos devastadores del Covid 19, para asistir a las familias que han visto mermados o incluso desaparecer sus ingresos por la crisis provocada por la pandemia. Los gobiernos , con buen criterio de asistencialismo social, están trabajando contra reloj para hacer llegar un conjunto de alimentos y bienes básicos para subsistencia.

El presente documento tiene por objeto describir de forma detallada , una solución práctica para la distribución de cajas o bolsones de alimentos a beneficiarios que se encuentran alcanzados por los planes de ayuda del Gobierno.

La forma actual de adquisición de dichos bienes y su distribución, están pensados para épocas normales, los procesos , tiempos de licitación, forma de pago y demás cuestiones administrativas obligan a los gobiernos a realizar procesos de compras de emergencia que corren el riesgo de ser ineficientes en cuanto al costo, el alcance efectivo a los beneficiarios y no contribuyen a crear un efecto positivo en las economías regionales y en las pequeñas y medianas empresas debido a la centralización de las compras en unos pocos proveedores. Este factor de multiplicación toma especial relevancia ya que la descentralización de compras en comercios y proveedores locales contribuiría a crear un circulo virtuoso dentro de las comunidades afectadas, dando impulso a la reactivación de la economía.

La utilización de tecnologías basadas en blockchain, con capacidad de creación de múltiples tokens fungibles y contratos inteligentes, puede ser una solución eficiente para este y muchos otros problemas ligados a la cadena de distribución de ayuda y asistencia a los mas necesitados, creando procesos transparentes , reactivando las economías locales y sus pymes, y optimizando las compras del estado con la consiguiente disminución del gasto publico, fomentando la inclusión financiera y tecnológica de la población.

Descripción general del proceso de optimización de la distribución de ayuda alimentaria

La definición de UA (unidad de ayuda) puede variar según el programa o comunidad en la que se esta trabajando. Utilizamos el caso de alimentos por tratarse de la necesidad mas urgente de asistencia , donde ademas existe basta experiencia para la definición de la canasta de productos mínimos que deben conformar dicha UA (unidad de ayuda).

Por otro lado la asistencia alimentaria probablemente deba continuar por un periodo posterior a la finalización de la pandemia, ya que las consecuencias en la destrucción de empleo e ingresos en las clases más bajas es impredecible.

A continuación se detallan los pasos conceptuales a considerar para la implementación del proceso completo:

1) Se definen una cantidad de productos P y las cantidades de cada uno de esos productos que conforman una unidad de ayuda (UA) (ej. 2 cajas de leche en polvo, 3 paquetes de 1 kg de fideos, etc.)

2) Se define una cantidad de beneficiarios (n), que deben recibir la unidad de ayuda (UA).(ej: 150.000, 500.000 beneficiarios)

3) Se define el presupuesto del gobierno para este plan de ayuda (PPA) sumando los costos de adquisición (CUA) de cada unidad de ayuda (UA), los costos de distribución (CDUA) como porcentaje del costo total de adquisición (CTUA) de las (n) unidades de ayuda. El presupuesto total debe incluir el costo final de la unidad de ayuda (UA) entregada a cada uno de los (n) beneficiarios, ya que de no considerarse pueden aparecer costos ocultos y problemas en la trazabilidad y auditoria final del programa. (ej: $70.000.000, $300.000.000, etc.)

4) Se crea un Token fungible equivalente a la unidad de moneda local, el cual vamos a llamar T1, el cual es emitido y autorizado por el banco central para este fin. La cantidad total de tokens

será equivalente al presupuesto total calculado (PPA) y se asigna al ministerio que lleva adelante el plan de ayuda.Solo portan emitirse tokens T1 por la cantidad exacta de presupuesto asignado para el programa. Se deposita en la wallet WMT1 (billetera digital) del ministerio mediante transferencia digital en custodia en banco central. (utilizamos adrede la palabra token y no moneda digital para evitar las implicancias legales y los tiempos que llevaría implementar una CBDC ,moneda soberana digital). (ej.: en el caso de argentina 1 T1 será equivalente a 1 peso)

5) El misterio crea un Token fungible equivalente a una unidad de ayuda UA, que llamaremos (Tua) siendo la cantidad total de tokens máximo creados igual a (n). Dichos tokens se transfieren a la wallet del ministerio WMTua. La creación de cada Token de UA solo puede ser realizada si existe un colateral en T1 equivalente al valor de compra de una UA.

6) La definición de la cantidad de productos que conforman la UA, sus valores unitarios incluyendo el costo de distribución, y la relación de intercambio entre T1 y Tua debe ser pública y debe poder ser accesible por cualquier usuario u organismo de control.

7) Cada uno de los (n) usuarios beneficiarios tendrá una billetera digital o wallet (Wub) donde recibirá las cantidades de Tokens de unidades de ayuda (Tua) que el gobierno considera según su necesidad. Estas unidades de ayuda serán enteros mayores a cero, y la frecuencia y cantidad de las mismas estarán previamente definidas por medio de contratos inteligentes, siendo la transferencia de los tokens (Tua) desde la wallet (WMTua) a las wallets de los usuarios(Wub) de forma automática y autónoma.

8) Cualquier comerciante en cualquier punto del país podría ofrecer la caja o el bolso de comida definido como UA, previo registro en la Base de datos de comerciantes, donde describirá los productos P que incluye . Una vez registrado se le asigna una billetera digital de comerciante Wc, la cual permite recibir y transferir tokens Tua. Esta base de datos de comercios con UA disponibles es geo referenciada y accesible públicamente, por lo cual cualquier usuario beneficiario podría elegir un comercio cercano donde comprar con sus Tua . Los comercios podrán ser evaluados por los usuarios beneficiarios en cuanto a calidad de productos, servicio , etc., creando de esta forma un sistema de control intrínseco de los propios beneficiarios.
   El gobierno tendría en tiempo real la cantidad de oferta y demanda de UA existentes, como la evaluación de los comercios.

9) Los proveedores mayoristas y fabricantes pueden participar del programa de 2 formas, vendiendo al estado directamente los productos P (en el caso que el ministerio implemente un sistema de licitación dentro del blockchain) y recibiendo tokens T1 o vendiendo a los comerciantes y recibiendo tokens Tua. En ambos casos obtienen una billetera digital de proveedor la cual permite recibir y transferir tokens T1 y/o Tua.

10) Para aquellas zonas donde no existan comerciantes que ofrezcan UA el gobierno realizará la distribución correspondiente. Estas compras serán realizadas a los proveedores registrados en la base de datos de proveedores que cumplan con los requerimientos y pagadas con tokens T1 vía smart contract de forma automática contra entrega (sistema de licitación en blockchain, tipo subasta, pagos y multas via smart contracts), permitiendo de esta forma un ahorro sustancial en costos administrativos y evitando que en el precio de venta los proveedores tengan que incluir el costo financiero que implica recibir pagos del estado en 90 o 120 días en contextos de alta inflación.

11) Los proveedores de los productos P y los comerciantes que distribuyen las UA pueden intercambiar los tokens Tua y los tokens T1 por instrumentos legales en bancos comerciales transformándolos en depósitos bancarios. Los procedimientos para realizar dicho swap serán previamente publicados, detallados e instrumentados en los correspondientes bancos comerciales o fintech.

12) Si bien la red es privada y permisionada se habilitará a un conjunto amplio de ONG's, entes de defensa a consumidores, organismos de control, periodistas y cualquier entidad que quiera registrarse para visualizar todas las transacciones realizadas en el blockchain.

Definiciones del sistema y componentes principales.

Unidad de ayuda (UA)

Se define como unidad de ayuda UA al conjunto de elementos que el gobierno quiere hacer llegar a cada uno de los beneficiarios.

Cada UA estará compuesta por un conjunto de elementos que definiremos como Productos (P).

Cada Producto P tendrá asociado un costo de compra unitario CP, el cual será calculado en base al estudio de mercado previamente realizado por el gobierno, publicado con acceso libre y registrado en el Blockchain. Este proceso también puede automatizarse de forma simple si se define una ecuación que lo represente.

El costo directo unitario (CUA) de cada unidad de ayuda (UA) será equivalente a la sumatoria de los costos unitarios de cada producto P.

La cantidad total de unidades de ayuda (UA) será equivalente a la cantidad total de beneficiarios con dicha ayuda. A esta cantidad de usuarios la definiremos cómo (n).

Siendo el costo total de adquisición de n.UA's : (CTUA)= n .CUA

Según la Organización de las naciones unidas para la alimentación y la agricultura (FAO), la ampliación y mejora de los programas de protección social y de asistencia alimentaria se ha transformado en urgente a raíz de la pandemia del Covid 19, aunque en los países en desarrollo de Latinoamérica esta es una necesidad latente desde antes de la pandemia y probablemente una vez finalizada será aun mas crítica.

Estas medidas ofrecen una solución intermedia para ayudar a los más vulnerables a respetar la obligación de permanecer en casa, ya que su subsistencia depende de sus ingresos diarios. En un contexto de despidos masivos, las familias tienen dificultades para llevar comida a la mesa. y el riesgo para las cadenas de suministro de alimentos.

Más de 160 países han decretado el cierre nacional de las escuelas, lo que afecta a más del 87% de la población estudiantil mundial y conlleva la cancelación de las comidas escolares, las cuales son, con frecuencia, la única fuente de nutrición de los niños y niñas de hogares vulnerables. Los servicios de comidas y los proveedores de comidas escolares también están experimentando pérdidas de ingresos.Una extensión automática del sistema planteado en el presente documento seria incorporar a las escuelas como beneficiarios , siendo estos un intermediario para la distribución de las UA.

En lo que respecta a los hogares vulnerables, la emisión de transferencias monetarias puntuales o múltiples en la etapa inicial puede suavizar el verdadero impacto de la crisis tras su estallido. Las transferencias monetarias tienen la capacidad de ayudar a las familias hasta que las circunstancias mejoren, en especial en caso de interrupción de los servicios sociales. Los sistemas móviles de pago son idóneos para garantizar la entrega rápida y minimizar el contacto humano asociado al intercambio de efectivo. Reemplazar parte del dinero por Tua aseguraría al gobierno que el dinero invertido va exclusivamente a la compra de alimentos.

Según la FAO, al 20 de marzo de 2020, 45 países han introducido programas de protección nuevos o han ampliado los programas de protección existentes en respuesta a la pandemia.

• Italia está ayudando a los trabajadores despedidos, para lo cual ha establecido una moratoria para el pago de hipotecas personales y empresariales y ha cancelado deudas en el marco de un paquete de socorro de 25 000 millones de EUR denominado “Cura Italia”. El programa incluye un pago puntual de 600 EUR a hogares con niños menores de 12 años.
- Los Estados Unidos de América ofrecen un plan de estímulo económico de 2 billones de USD, que incluye un pago puntual de 1 200 USD a la mayoría de los adultos y un pago adicional de 500 USD a cada niño y que amplía la cobertura por desempleo. Este paquete se suma a un

programa de ayuda de 100 000 millones de USD que, entre otras cosas, ofrecía vacaciones pagadas de emergencia a trabajadores.
- Francia ayuda a los padres a quedarse en casa para cuidar de los niños y ofrece licencia por enfermedad a las personas en cuarentena domiciliaria.
- China, RAE de Hong Kong, y Singapur están facilitando pagos en efectivo únicos y universales a todos los ciudadanos.
- Portugal va a entregar hasta 1 097 EUR a los trabajadores por cuenta propia durante un máximo de 12 meses.
- El Perú ha creado un bono para proteger a tres millones de familias vulnerables y ha adelantado el pago de las pensiones de los ciudadanos de edad, sobre la base de programas existentes, como Pensión 65. Además, ha establecido una prestación complementaria para familias vulnerables, que se suma a la transferencia monetaria nacional.

Costo de Distribución de unidad de ayuda (CDUA)

Se define como costo de distribución de unidad de ayuda al costo total de logística que debería asumir el gobierno en caso de centralizar el total de la compra, almacenaje y distribución de las UA's.

Este costo puede ser definido como un porcentaje (%) del costo total de adquisición de cada unidad de ayuda (CTUA) . Existen numerosos estudios que detallan para distintos tipos de productos el costo de logística y distribución asociado que puede variar entre el 8% y el 16% según el sitio de acopio y el método de distribución empleado. Estimamos que en el caso del Gobierno este costo es aún mayor, ya que cuentan con pocos centros de acopio y el alcance de los programas de distribución de alimentos es nacional.

Estos ahorros relacionados con los costos de logística, se transforman en utilidad marginal adicional para los proveedores y comerciantes locales, ya que pueden crear redes de distribución mas eficientes y disminuir los stocks, cumpliendo de esta forma una de las premisas del sistema que es reactivar las industrias locales y el trabajo en dichas comunidades a partir de la descentralización de la compra y distribución de la unidades de ayuda.

Por lo cual, el gobierno deberá calcular un presupuesto total para este plan de ayuda (PPA) que sería equivalente al costo total de adquisición de los productos mas un porcentaje (%) correspondiente al costo de logística.

PPA= CTUA (1 + %CDUA)

Solo a modo de ejemplo, podemos analizar los componentes del precio de la leche , producto básico en todos los planes de ayuda alimentaria. Este cálculo variará en cada país, pero tomaremos el costo argentino como ejemplo.

Según los datos de la Camara Argentina de Comercio, sobre costo argentino de 2017, la logística representa el 14,5% del precio de la leche .

Salarios	29,9 %
Logística	14,5 %
Estado	39,0 %
Gastos de Producción	40,5 %
Ganancia agregada	-2,9 %
TOTAL (precio final - 100% - más 21% de IVA)	121 %

Fig 1. Agrupación de cuentas que forman el precio de la leche

Esta situación inicial se ve aun mas agravada en la formación final del precio de la leche por eslabones de la cadena, como se puede ver en el siguiente gráfico:

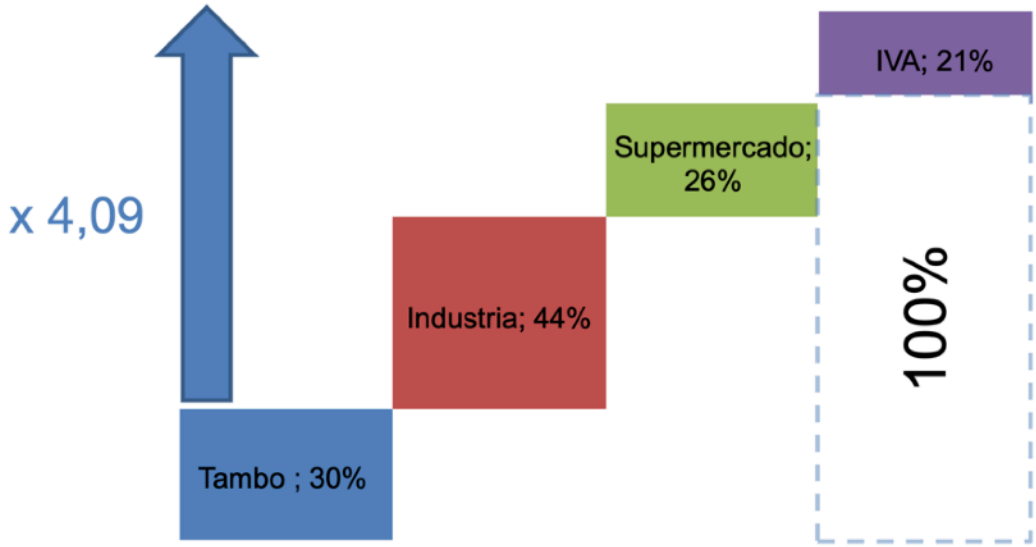

Fig 2. Formación Final del precio de la leche
Si a estos valores , sumamos los costos ligados a la venta al estado y el financiamiento en contextos de alta inflación, queda absolutamente claro la necesidad de implementar nuevos mecanismos de adquisición y distribución que optimicen el actual sistema.

Beneficiarios (u)

Se definen cómo beneficiarios a todos aquellos usuarios (u) que se encuentren registrados en la base de datos de usuarios beneficiarios (BDu). Es fundamental contar con la base de datos de usuarios para poder conocer la ubicación geográfica donde tendría que llegar cada uno de las unidades de ayuda (UA).

Nota: Por simplicidad a los fines de este documento definimos un único tipo de usuario beneficiario (ub), siendo posible técnicamente definir varios tipos de usuarios, como ser entidades intermedias, iglesias, comedores, escuelas, centros de ayuda, etc, los cuales podrían ser definidos como ua, ub…ux , posibilitando de esta forma que la ayuda llegue inclusive a aquellos usuarios no registrados en la base de datos de beneficiarios (BDu) o que no cuentan con la capacidad tecnológica mínima para tener una billetera digital para transaccional con el token de unidad de ayuda (Tua).

La Base de datos usuarios BDU contendrá el detalle de cada usuario beneficiario (u1,u2, ……u n)

Hasta aquí , las definiciones precedentes relacionados con la base de usuarios beneficiarios no difieren en absoluto de los sistemas actuales centralizados, siendo estos elementos necesarios para hacer una distribución de cualquier plan de ayuda. Se incorporarán los elementos tecnológicos necesarios para la consiguiente implementación sobre una blockchain multi chain con smart contracts para lograr la descentralización de la compra y distribución.

Definiciones generales ecosistema blockchain

El concepto principal por detrás de la tecnología de Blockchain radica en la posibilidad de crear mecanismos automáticos de registros y verificaciones de transacciones que no requieran de intermediarios, que sean autónomos en su funcionamiento y distribuidos , que puedan ser

accesibles por cualquier persona y de esta forma crear sistemas inmutables e incorruptibles desde la perspectiva de la modificación de los datos que en el existen.

Confianza. La clave para la adopción del sistema de distribución de alimentos basado en blockchain.

La utilización de un sistema de blockchain para tokenizar la ayuda alimentaria es un paso intermedio que puede ser implementado por los gobiernos en el camino de futuras implementaciones de CBDC (Central Bank Digital Currency).

Este tipo de implementaciones deben considerar sistemas abiertos e inclusivos, no se puede depender de una única gran compañía para implementarlo, debe ser abierto a la innovación, debe ser inclusivo desde la perspectiva de la usabilidad, considerando las distintas limitaciones que pueden tener desde el aspecto tecnológicos los beneficiarios. Debe poder ser utilizado con distintos tipos de teléfonos, mas o menos inteligentes, distintos sistemas operativos y distintos niveles de conectividad a internet.

Por otro lado, el sistema debe guardar un equilibrio permanente entre privacidad y transparencia. Por tratarse de valores pequeños en cuanto a las transacciones individuales se prioriza la privacidad del usuario y la velocidad de la transacción, mientras que por tratarse de valores mayores en las transacciones entre comercios, proveedores, bancos y estado, se prioriza la transparencia.

No debemos minimizar el factor multiplicador que genera la inclusion financiera y digital simultánea de un gran colectivo de la población, lo cual indirectamente puede influir en forma positiva en la optimización de los planes de salud publica, educación y seguridad.

La transición entre los sistemas actuales de pago en efectivo y los digitales debe ser gradual y demostrar que tiene reglas confiables, debe comenzar con casos simples como el expuesto en el presente trabajo e ir agregando nuevos servicios que no representen una complejidad excesiva que socave la confianza lograda en cada etapa.

En dicho sentido, la tecnología de Blockchain nace para cubrir esa brecha de confianza entre dos personas o entidades que quieren realizar una transacción. Cumple de forma autónoma con todas las reglas establecidas para una transacción determinada sin necesidad de intermediarios.

La capacidad de los sistemas de Blockchain para evitar el problema del doble gasto, al momento de realizar un pago (que no se pueda gastar mas de una vez un único valor), sin necesidad de entidades financieras que actúen como intermediarias, baja de forma significativa los costos de cada transacción y la fricción generada por el sistema de bancos comerciales.

En nuestro caso, para ejemplificar la solución de doble gasto , cada vez que un token es utilizado para adquirir una unidad de ayuda (UA) , el sistema de blockchain registra dicha transacción en un registro público , por lo cual todas las transacciones son registradas públicamente y accesibles. Una vez publicada la transacción, esta debe ser aprobada basada en todas las transacciones anteriormente publicadas en dicho registro, para comprobar fehacientemente que el poseedor del token es realmente la persona que quiere gastarlo y no fue utilizado con anterioridad. Cuando esto es comprobado, se registra esta transacción y se registra el nuevo poseedor del token, evitando de esta forma que pueda ser gastado más de una vez.

La certificación de este proceso se realiza de diferentes maneras, dependiendo el tipo de blockchain que sea utilizado, y el protocolo de prueba que sea utilizado por los nodos verificadores. Estos nodos a su vez guardan copias exactas de los distintos registros públicos y por medio de mecanismos de consenso totalmente autónomos y sin intervención humana, comparan dichas copias para evitar posibles nodos corruptos que quieran cambiar algún registro, eliminando dichos nodos en caso de detectar cualquier variación.

El registro de cada transacción guarda también el momento temporal en la que fue realizada, y es guardada en bloques continuos , que se enlazan con sus bloques precedentes y siguientes mediante una clave criptográfica (hash) que asegura la inmutabilidad del sistema.

Esta encadenación de bloques mediante el hash da el nombre al sistema (cadena de bloques o blockchain).

Existen en la actualidad infinidad de sistemas y tecnologías de blockchain, aquellas que son publicas y que no requieren de autorización para ser utilizadas o transformarse en un nodo verificador de la misma. Estas redes permiten a las organizaciones , individuos e instituciones publicas o privadas transaccional con eficiencia, seguridad y transparencia , ademas de abrir nuevas oportunidades para innovar y generar nuevos modelos de negocios y cambiar varias de las industrias existentes.

Pero las redes de blockchain públicas no permisionadas no siempre son la mejor opción cuando se trata de proyectos ligados a Gobierno, Salud y Entidades Financieras, donde existe una necesidad de asegurar la privacidad en parte de la información o existen requerimiento regulatorios complejos que aún no han sido adaptados para trabajar sobre redes publicas . Es por dicha razón que si bien aún no hay un único consenso y la tecnología avanza muy rápido, se proponen para este tipo de proyectos donde el gobierno y los bancos comerciales están involucrados, sistemas de blockchain privados y permisionados, de forma tal de poder aislar datos sensibles sobre las personas e instituciones, permitiendo de esta forma interactuar también con redes publicas de forma segura y confiable. En particular seleccionaremos como algoritmo de consenso proof of stake ya que nos permitirá máxima velocidad en las transacciones, seguridad y menor consumo energético.

category of consensus algorithm	Used for	Time before finality	# of nodes on the network	Tolerance to malicious participants	Energy consumption
Proof of Work	Public networks	High	High	1/2	High
Proof of Stake	Public networks	Low	High	1/3	Low
Delegated Proof of Stake	Public networks	Low	Low	1/3	Low
Practical Byzantine Fault Tolerance	Permissioned networks	Low	Low	1/3	Low
RAFT/PAXOS	Permissioned networks	Low	Low	1/3	Low

Fig 3. Comparison of some consensus algorithms

Red Permisionada, tokens fungibles.

Se define en esta aplicación un Sistema blockchain permisionado. A diferencia de los sistemas de blockchain no permisionados o públicos (como bitcoin) , todos los nodos que participan en un sistema privado permisionado deben ser admitidos por una entidad central (en nuestro caso el Banco Central).

Si bien no forma parte del presente trabajo entrar en el detalle de las especificaciones técnicas de los distintos sistemas de Blockchain, definiremos que el sistema de blockchain utilizado para generar los diferentes tipos de tokens es un sistema permisionado y privado, controlado por el Banco Central, el cual tendrá la capacidad de emitir un token del banco central equivalente a la unidad de moneda nacional. Por lo cual una unidad de moneda nacional es equivalente a una unidad de Token generado. Para el presente trabajo definimos a dicho token como T1, ya que la aplicación y desarrollo de una moneda digital del banco central es un proceso largo y requiere de

muchos aspectos que no son necesarios para este caso de uso. Solo serán generados los tokens T1 requeridos por el ministerio responsable de la ejecución del plan de alimentos.

También el administrador del Blockchain podrá permitir la creación de otros tokens fungibles los cuales podrán ser intercambiados sobre la misma blockchain, los cuales representaran unidades de cuenta diferentes y tendrán una relación entre sí. En este acaso de aplicación trabajaremos únicamente con 2 tokens T1(token equivalente a 1 unidad de moneda nacional) y Tua (token equivalente a una unidad de ayuda UA).

Definimos a todos los tokens que intervendrán en este caso de uso como tokens fungibles. Se definen cómo fungibles porque cualquiera dos unidades del mismo token pueden ser intercambiadas, es decir que tienen el mismo valor nominal. Esto es similar al caso del dinero en efectivo, 2 billetes de 10 pesos pueden intercambiarse uno por otro , 2 litros de leche de la misma marca o tipo, dos cajas de ayuda que contienen los mismos elementos.

Wallets o Billetera Digital.

Definimos cómo wallet a la billetera digital que habilita a los diferentes usuarios a almacenar, enviar y recibir los tokens generados.

Cada tipo de usuario puede contar con un tipo de billetera que puede tener características o derechos diferentes. Debe poder enviar o recibir uno o varios tokens, puede tener limitaciones en cuanto a las cantidades o unidades, puede ser bloqueada en caso de uso incorrecto, o cualquier otro tipo de función necesaria para cumplir con los objetivos del programa.

El proceso por el cual se transfieren los tokens entre dos usuarios, es un proceso que se conoce dentro de los sistemas de Blockchain habitualmente como firma digital. Cada usuario cuenta con una clave privada y una clave publica que le permite interactuar con los otros usuarios del sistema.

En este caso de uso, la interfase de usuario, será una interfase de usuario simple, similar a la interfase que se utiliza en la billeteras electrónicas mas populares en el país (mercado libre, Glovo, nubi, etc) y como las billeteras electrónicas que se utilizan en los bancos comerciales.

En el caso de las wallets del ministerio y los bancos comerciales involucrados se utilizarán mecanismos de múltiples firmas y control de identidad digital mas sofisticados para mantener el control de las claves privadas.

Smart contracts

Los smart contracts o contratos inteligentes son reglas que se aplican a los tokens para automatizar aquellos procesos o transacciones que tienen acciones ligadas. Por ejemplo la conversión entre tokens, la autorización a transferir automáticamente cada vez que acontece un evento determinado o cada un plazo de tiempo prefijado, a congelar fondos en caso de detectarse un evento determinado, a realizar pagos cuando se recibe una mercadería o cualquier acción que derive en otra acción .

La implementación de smart contracts puede realizarse de diversas maneras según el tipo de blockchain que se seleccione, pero la mayoría de los blockchains que pueden ser utilizados para este caso de uso ya cuentan con múltiples templates de smart contracts que aplican perfectamente, no encontrando necesidad de crear nuevos tipos de contratos inteligentes que no existan en la actualidad.

Por otro lado, en caso de necesidad de crear algún tipo de smart contract nuevo, absolutamente todas las plataformas son abiertas y colaborativas, tienen lenguajes de programación públicos y redes de pruebas donde ejecutar dichos contratos y verificar su correcto funcionamiento antes de su implementación.

Serían recomendables para este tipo de casos aquellos blockchain que puedan administrar smart contracts en Layer 1 , para agregar niveles de seguridad y velocidad en las transacciones.

Smart contracts en Layer 1

Como hemos explicado anteriormente, los sistemas de blockchain permiten que exista una confianza absoluta en las transacciones, a partir de la publicación en un registro público de cada una de las transacciones. Esas publicaciones se realizan a nivel de Layer 1, es decir , son las transacciones nativas que fueron desarrolladas en el propio código de creación del blockchain.

En la medida que fueron apareciendo nuevos sistemas de blockchain como Ethereum que permiten la ejecución de contratos inteligentes, comienzan a aparecer algunas preocupaciones ligadas a la seguridad y eficiencia , ya que son utilizados otros mecanismos para la ejecución de dichos contratos inteligentes por fuera del Layer 1 .

En nuestra solución, necesariamente tenemos que buscar sistemas que ejecuten dichos contratos de manera rápida y eficiente, con el menor grado de consumo de recursos técnicos y tiempos y evitando por tratarse de dinero digital publico cualquier tipo de debilidad en cuanto a la seguridad.

Las funcionalidades básicas que estamos buscando realizar, pueden ser implementadas en Layer 1 , ya que existen en la actualidad algunos sistemas como Cardano o Algorand, entre otros, los cuales ya fueron diseñados para este tipo de implementaciones.

En particular:

- *Definir reglas de transacciones básicas, como permitir a cualquier usuario comprar cualquier item a un vendedor determinado a un precio prefijado, sin ninguna intervención de terceros.*

- *Transacciones Acreditadas a determinados usuarios. Permitir solamente a un tipo de usuario realizar determinadas transacciones , sin necesidad de aprobar cada transacción en forma individual.*

- *Wallets inteligentes. Permitir solamente a determinados usuarios transaccional con determinados tokens.*

Nodos Validadores

Por tratarse de una red permisionada y privada, se utilizarán como nodos validadores aquellos organismos estatales que cuenten con la infraestructura necesaria para poder convertirse en nodo de la red, aquellos bancos públicos o privados que participen o quieran participar del proceso de conversión para transformar tokens en depósitos bancarios y aquellas fintechs que quieran participar del proceso como depositarios finales o con productos de valor agregado.
Este punto es importante , ya que la selección correcta del blockchain a utilizar tendrá que considerar la infraestructura con la que se cuenta y los tipos de nodos que van a participar , para crear una implementación rápida, segura y compartir los costos de dicha infraestructura distribuida entre todos los participantes. Por la naturaleza misma del blockchain cuanto mas nodos existan , más distribuida la red y más segura es.

Definiciones particulares ecosistema blockchain

Tipos de tokens (T1 y Tua)

Cómo fue descripto precedentemente en este caso de uso estaremos creando 2 tipos de tokens.

El token T1, que representa la unidad de cuenta digital equivalente a la unidad moneda nacional.
1 T1 = 1 $.

El token Tua, que representa la unidad de cuenta digital equivalente a una unidad de ayuda UA.
1 Tua= valor necesario para adquirir una UA

La relación entre ambos tokens esta dado por las siguientes ecuaciones:

El presupuesto total del plan de ayuda es la suma de productos y su costo logístico en $ para la adquisición de (n) unidades de ayuda (UA). En un contexto de alta inflación como el que vivimos este valor puede cambiar cada vez que se inicia un ciclo de compra y distribución.

PPA ($) = CTUA ($) (1 + %CDUA)

Por lo cual la cantidad total de T1 a emitir será igual a PPA.

Dado que cada token Tua debe representar una unidad de cuenta UA, la cantidad total de tokens Tua que se deben emitir será (n) que es la totalidad de unidades de ayuda.

Por lo cual Tua= (PPA/n). T1

Es importante que PPA se mantenga actualizado de forma tal que en cualquier nuevo ciclo de compra , el valor que representa (Tua) sea equivalente al valor actual de todos los productos y la logística que representan cada UA. La actualización del presupuesto PPA también podrá ser realizada en forma automática dentro del Blockchain.

Tipos de usuarios

Tendremos al menos 7(siete) tipos de usuarios en el sistema

1. **Usuario Banco Central (ubc)** que es el responsable de emitir el T1 y administrar los nodos validadores y otros usuarios del sistema (Ministerios, bancos comerciales, fintech y veedores).
2. **Usuario Ministerio (um)** que es el responsable por la emisión del Tua y administrar a los usuarios beneficiarios, comercios y proveedores.
3. **Usuario beneficiario (ub)** que es el beneficiario del plan de asistencia alimentaria.
4. **Usuario Comercio (uc)** que coloca a disposición de los usuarios beneficiarios (ub) las unidades de ayuda (UA).
5. **Usuario Proveedor (up)** que son los proveedores que ofrecen los Productos (P) que conforman la unidad de ayuda (UA).
6. **Usuarios Entidades Financieras (uef)** que son los bancos comerciales o fintech que pueden recibir los tokens Tua y convertirlos en T1 o en instrumentos habilitados por Banco Central.
7. **Usuarios Veedores (Uv)** que son usuarios que pueden ver todas las transacciones en el sistema para auditarlo o crear sugerencias para mejores practicas.

Tipos de Wallet

Cada wallet tendrá funcionalidades diferentes según los servicios que sean necesarios. Solo haremos la descripción correspondiente a las operaciones de almacenamiento, recepción , envió o swap de tokens, ya que las funcionalidades adicionales como geolocalización de comercios, ubicación de los usuarios y los detalles relacionados con los elementos de firma digital y criptograma exceden el alcance del presente trabajo.

Wallet	Enviar Tua para	Recibir Tua de	Enviar T1 para	Recibir T1 de
Banco Central	NO	NO	Ministerio	Ministerio Entidad Financiera
Ministerio	Beneficiarios	Cuenta generadora Tua Ministerio. Entidad Financiera	Banco Central	Banco Central
Beneficiario	Comercio	Ministerio	NO	NO
Comercio	Proveedor. Entidad Financiera	Beneficiarios	NO	NO
Proveedor	Entidad Financiera	Comercio	Entidad Financiera	Ministerio
Entidad Financiera	Ministerio	Comercio Proveedor	Banco Central	Proveedor Ministerio

Fig. 4 Tabla funcionalidad de wallets.

Wallet Banco Central (ubc): Permite enviar T1 a usuario Ministerio **(um)** y recibir T1 de usuario ministerio **(um)** y de usuario entidad financiera **(uef)**

Wallet Ministerio (**um)**: permite recibir T1 solo de usuario Banco Central **(ubc**) y enviar T1 solo a usuario Banco Central (**ubc)** . Permite recibir Tua de cuenta especial Ministerio (generación de Tua) y de entidad financiera (uef) y permite enviar Tua solo a usuarios beneficiarios.(**ub)**

Wallet de usuario beneficiario (ub) : permite recibir (Tua) solo de usuario Ministerio **(um)** y transferir (Tua) solo a usuario comercio (**uc)**.

Wallet de usuario comercio (uc): permite recibir (Tua) solo de usuario beneficiario **(ub) y** permite transferir (Tua) a usuario proveedor **(up)** y a usuario entidad financiera **(uef)**

Wallet usuario proveedor (up): permite recibir T1 de usuario ministerio **(um)** y enviar T1 a usuario entidad financiera (**uef)** y permite recibir Tua de usuario comercio **(uc)** y enviar Tua a usuario entidad financiera (**uef)**.

Wallet entidad financiera (uef): permite recibir T1 de usuario proveedor **(up)** y de usuario ministerio **(um)** y enviar T1 únicamente a usuario banco central **(ubc).** Permite recibir Tua de usuario comercio **(uc)** y de usuario proveedor **(up)** y enviar TuA a ministerio para su eliminación.

De esta forma vemos como las wallets o billeteras electrónicas no solo cumplen la función práctica de enviar y transferir los distintos tipos de tokens, sino que también contienen junto con los tokens todas las reglas necesarias para asegurar que los procesos pre definidos serán cumplidos en forma automática y sin necesidad de participación de ningún intermediario.

Conclusiones:

Como hemos descripto en el presente trabajo, la implementación de un sistema de blockchain para la administracion completa del programa de asistencia alimentaria , permite un control absoluto de cada una de las fases que componen la cadena de suministro, desde la asignación de presupuesto, la distribución de los beneficios, el control de la entrega de la asistencia, los pagos a los comercios y los proveedores, la conversión de los tokens por parte de las entidades financieras y la auditoria y control por parte de las fuerzas vivas de la sociedad.

Por otro lado , el uso de contratos inteligentes permite definir de forma unívoca las reglas a las que cada tipo de usuario estará supeditado y los posibles intercambios de los distintos tipos de tokens entre los distintos tipos de usuarios. Estos mismos contratos podrían utilizarse para el pago automático de impuestos, la asignación de beneficios fiscales para comercios en zonas menos favorecidas, incentivos para las pymes proveedoras y cualquier otro tipo de política que contribuya a la reactivación de la economía.

Los criterios de diseño aseguran un alto nivel de usabilidad, entendiendo la misma como el acceso de todos los posibles beneficiarios del sistema, independientemente del dispositivo o conectividad que posea, y por otro lado mantiene una relación optima entre seguridad, privacidad y transparencia.

El sistema propuesto puede ser utilizado como laboratorio para la implementación de una moneda digital nacional (CBDC) controlada por el Banco Central, iniciando así un proceso de transformación necesario e inevitable.

Esperamos que el presente trabajo sirva como punto de partida para que responsables del gobierno, técnicos y empresas especializadas propongan soluciones tecnológicas que contribuyan a lograr mayor transparencia y eficiencia en la asistencia a los grupos en riesgo , contribuyendo de esta forma a la reactivación económica del país.

Bibliografia

Ethereum (2016). Ethereum. https://github.com/ethereum/.

S. Nakamoto (2019). Bitcoin: A Peer-to-Peer Electronic Cash System. http://www.bitcoin.org/bitcoin.pdf.

Jing Chen , Silvio Micali (2017) .Algorand white paper https://arxiv.org/abs/1607.01341

Fundacion Cardano (2019).OUROBOROS PROOF OF STAKE ALGORITHM https://docs.cardano.org/cardano/proof-of-stake/

N.Cachanosky (2019) .CAN BITCOIN BECOME MONEY? THE MONETARY RULE PROBLEM

J.Villaverde , Daniel Sanches (2018). Can Currency Competition Work? Federal Reserve Bank of Philadelphia

Jon Nicolaisen (2017) at the Norwegian Academy of Science and Letters, https://www.norges-bank.no/en/news-events/news-publications/Speeches/2017/2017-04-25-dnva/

Bordo, Michael and Pierre Siklos (2017). “Central Banks: Evolution and Innovation in Historical Perspective.” Manuscript, Rutgers University.

Powell, Jerome (2017). “Innovation, Technology, and the Payments System.” Available at: https://www.federalreserve.gov/newsevents/speech/powell20170303a.htm.

Antonio Requena.(2019) Redes de Blockchain permisionadas. https://ideas.pwc.es/archivos/20190913/redes-blockchain-permisionadas-banca/

Arthur Gervais (2019) Blockchain scalability, interoperability and sustainability’ an academic research paper prepared by the Lucerne University of Applied Sciences and Arts – an academic partner of the EU Blockchain Observatory & Forum.

FAO (2020), Respuestas ante la COVID-19 y el riesgo para las cadenas de suministro de alimentos http://www.fao.org/3/ca8388es/CA8388ES.pdf

CAC (2017) Resumen ejecutivo Costo Argentino CAC. Cámara Argentina de Comercio y Servicios.

Economic Forum (2018) The Future of Trust and Integrity

Michael H. Goldhaber (1997) The Attention Economy and the Net by *First Monday*, Volume 2, Number 4 - 7 April 1997 https://firstmonday.org/ojs/index.php/fm/article/view/519/440