ESTRATEGIA TECNOLÓGICA

Tres **pilares fundamentales** sustentan el proyecto a nivel tecnológico:

- Seguridad. Llevar el nivel de seguridad al límite, no solo para mantener transacciones seguras, sino que también para estructurar un sistema de privacidad y anonimato.
- Privacidad. La privacidad es la esencia del código fuente, usando distintas técnicas tales como SHA-3 y Ring-Signature.
- Descentralización. ProsusMoney no tiene dueño. El desarrollo es gestionado voluntariamente por programadores de distintos proyectos Cryptonote que interactúan entre sí.

Especificaciones técnicas.

- Cantidad total de "prosus": ~18.5 millones
- Fraccionado: 12 decimales
- Tiempo de validación entre bloques: 120 segundos (*target*)
- Tiempo para registrar transacción: instantáneo (menor a 4 segundos).
- Protocolo: Cryptonote (application layer)
- Consenso: *egalitarian proof of work*
- Algoritmo de hashing: Cryptonight v1 + CV7_antiasic
- Cálculo de dificultad: Media Móvil Ponderada Lineal (Linear Weighted Moving Average, LWMA)
- Recompensa: disminución gradual.
- Pre-minado: primeros 100000 bloques, convocatoria abierta y anónima, más de 10 mineros.
- Integración: multiplataforma, portable.
- Control de versiones: desarrollado en paralelo con proyectos sucesores de Bytecoin (Monero, Karbowanec, Turtlecoin).

Acerca de la emisión.

Una vez emitido el bloque génesis de blockchain ProsusMoney, la recompensa partió en ~70 prosus (valor actual con 12 decimales) la cual iría gradualmente disminuyendo de acuerdo a la siguiente función:

$$\text{Recompensa} = (\text{Total\_Supply} - \text{Current\_Supply}) >> 18$$

Donde...

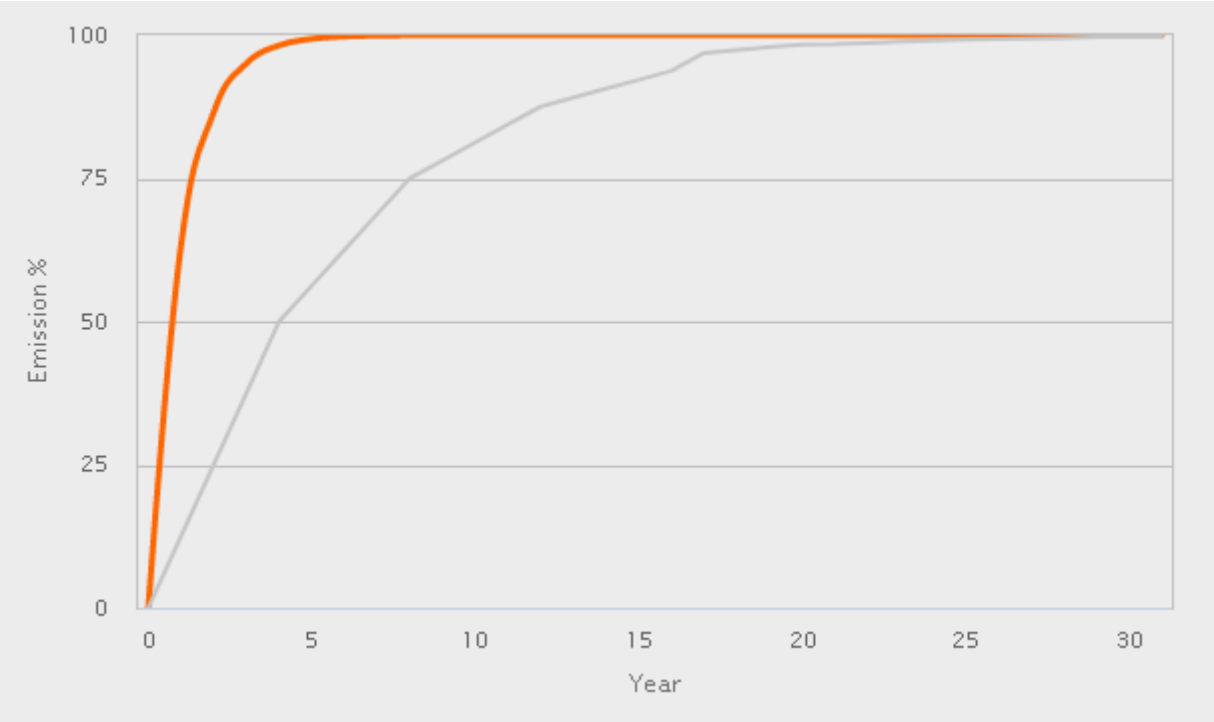
Total_Supply = $2^{64} - 1$ (unidades atómicas)

Current_Supply = cantidad de *prosus* emitidos hasta el momento.

>> 18 = factor de crecimiento

La anterior función está ajustada a un "nivel de recompensa diaria" (y otras variables), las cuales son seteadas en el código fuente (archivo CryptoNoteConfig.h)

Si graficamos *Current_Supply*, veremos la diferencia de crecimiento de la recompensa respecto al *halving* de Bitcoin. Destacando que, después de 4 años de funcionamiento ininterrumpido, ya se ha emitido un ~85% del Total_Supply de ProsusMoney .



ProsusMoney Bitcoin

Esta velocidad de emisión es muy importante para planificar un roadmap, considerando la disparidad con Bitcoin y otras criptomonedas.

Algoritmo de hashing, para minería.

El algoritmo Cryptonight es lo que determina que la minería de ProsusMoney esté orientada a ser exclusiva para CPU. Tiene 3 etapas principales basadas en SHA-3, cuyo funcionamiento detallado está descrito en los comentarios al código fuente disponible en el repositorio Github. A continuación, un breve resumen.

- **Preparar el scratchpad.**

  Se parte tomando los bytes 0-31 del *state* (bloque inicial de datos) y se expanden a 10 keys de AES.

  Se aplican 14 rondas usando los pasos de AES llamados *SubBytes*, *ShiftRows* y *MixColumns*

  El scratchpad resultante es un array de 2097152 bytes.

- **El loop principal.**

  Dos variables, a & b, se trabajan mediante operaciones lógicas XOR y usando las funciones *toScratchpadAddress*, *8ByteAdd* y *8ByteMultiply*

  Con lo anterior se obtiene un bloque de código llamado *memory-hard loop* que se repite 524288 veces.

- **Calcular el resultado.**

  Se expanden los bytes 32-63 del *state* para obtener 10 keys y se usan los bytes 64-191 del *state* como bloque inicial. A este bloque inicial se aplica una operación lógica XOR con los primeros 128 bytes del *scratchpad* y se crea el *modified-state*.

  Se aplica una permutación keccak-f y se obtienen dos bits significativos para elegir una de estas cuatro funciones de hash…

  00 Blake-256

  01 Groestl-256

  10 Jh-256

  11 Skein-256

  Se aplica la función de hash al *modified-state* creándose así el resultado final: un hash de Cryptonight.

Ring Signature

En criptografía, una "firma circular" (*ring signature*) es un tipo de firma digital que puede ser creada por cualquier miembro de un grupo de usuarios (en el que cada usuario tiene su propia clave). Una de las propiedades de seguridad que debe cumplir, es que no debe ser posible averiguar qué clave concreta del grupo fue utilizada para calcular la firma.

(Ver diagrama en páginas siguientes)

Checkpoints

Debido a que ProsusMoney fue desarrollado inicialmente como "laboratorio blockchain" hay algunos registros (*checkpoints* o sucesos) que se pueden examinar en el *Block-Explorer* y que vale la pena describir.

- **Bloque 1626, hash 55c456b87abc26b4ff62ad53b75c6f1033536507f60d7f7f1aed22950f4994bd**

  Ocurre un cambio de *factor de crecimiento*. En el *bloque génesis* fue 21 y a partir de este bloque es 18 (definitivo).

- **Bloque 3150, hash 6571b301402d7b677c53333cdb59f811dc902ac63ab5262ece30a4f66940f8f6**

  Se simula un "secuestro de blockchain" al encontrar un bug en una *función de curva elíptica* (Elliptic curve cryptography, ECC). Por lo anterior, los primeros bloques de la sincronización aparecen "incrustados" en la blockchain ProsusMoney, lo cual fortalece la integridad de toda la red al evitar las compilaciones maliciosas.

- **Bloque 164520, hash b41826f1c6411d6e31fae5b887020d33324996e28415941c73a9a00737a468c1**

  Algunos mineros comienzan a usar "hash-power rental" llevando la dificultad a niveles muy altos para que un computador convencional pueda resolver los bloques dentro del *tiempo_de_validación*, provocando un "stuck". Se solucionó arrendando hash-power para competir con otros mineros.

- **Bloque 230106, hash fcdd9a8a6753c2c046dfe6b961c713a4e4da57377b6be1e3ad5b5273f57bdef0**

  Otro "stuck" provocado por la misma causa del bloque 164520. Se intenta la misma solución y en la Comunidad Cryptonote se comienza a desarrollar un nuevo algoritmo para evitar el uso de hardware ASIC.

- **Bloque 400001, hash 3cd4816ccda60076271cb9aa37f254d16a6b656279399bf94531222994b8ab26**

  Comienza la versión 2 de la blockchain ProsusMoney con la característica LWMA (cálculo de dificultad con Media Móvil Ponderada Lineal). Esta modificación se planificó como una transición hacia la versión 3 de la blockchain ProsusMoney

- **Bloque 405401, hash 940d52285b06f6a359da39689c75d8b5124e2f3c01325a607ab2afc4607f63d2**

  Comienza la versión 3 de la blockchain ProsusMoney cuya principal característica es el algoritmo de minado anti-ASIC

Tamaño de las transacciones.

La cantidad máxima en cada transacción lo calcula el software cliente (Monedero o "wallet") mediante variables *equivalentes* al UTXO de Bitcoin. *Unspent Transaction Output* (UTXO) fue diseñado así en Bitcoin para evitar el doble gasto. Una transacción de salida en *prosus* es en promedio 10 "trozos" compuesto por las entradas.

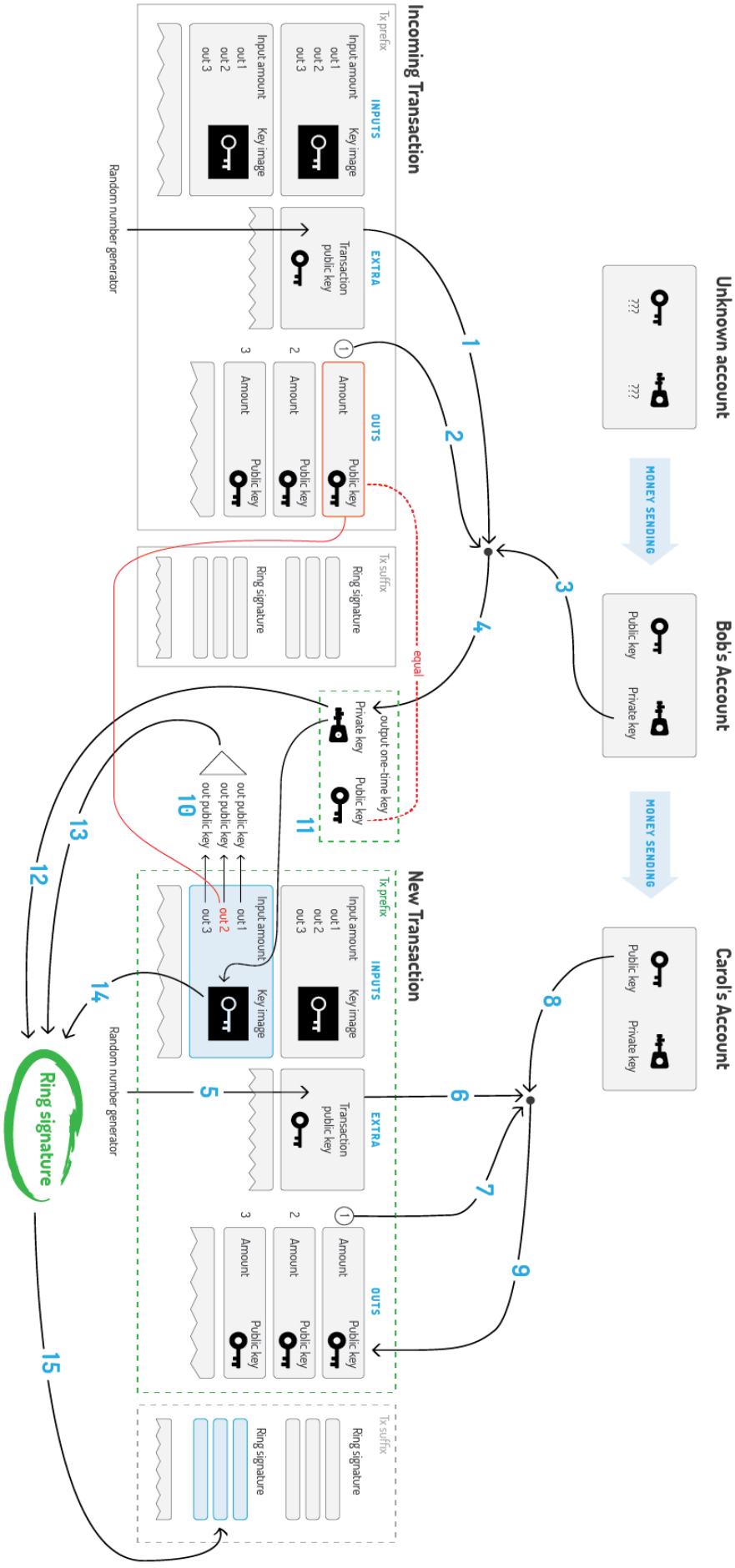
En síntesis, mientras más grande son las transacciones que ha recibido una wallet, más grande serán las transacciones que se pueden enviar. Esta técnica previene el *double spending* y el *dusting attack*.

Seguridad a nivel usuario.

- Frase memorizable: 25 palabras en lenguaje natural para rescatar la *wallet* del usuario desde la blockchain.
- Llave privada (o "clave" privada): string en formato *base58* para rescatar la información desde la blockchain (versión "máquina" de la frase memorizable)
- Llave de seguimiento: string que permite a un tercero tener acceso a una wallet, en modo solo lectura (no puede enviar *prosus* pero sí ver las transacciones).
- Contraseña: clave de usuario (palabra) para encriptar el archivo local (**.wallet*)

Desarrollo del código fuente

ProsusMoney sigue la filosofía *Open Source* mediante licencias de software MIT/X11 y GNU-GPL. Esto significa que existe una "obligación moral" de participar en proyectos similares aportando y usando el código fuente como si fuera patrimonio de una Comunidad. En definitiva, apoyando a otros se obtiene un beneficio que es compartido entre todos los participantes.


Unknown account
???
???
MONEY SENDING
Bob's Account
Public key
Private key
MONEY SENDING
Carol's Account
Public key
Private key
Incoming Transaction
Tx prefix
INPUTS
Input amount
Key image
EXTRA
Transaction public key
OUTS
Amount
Public key
Tx suffix
Ring signature
Random number generator
equal
output one-time key
Private key
Public key
out public key
New Transaction
Ring signature
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

ESTRATEGIA FINANCIERA

Especificaciones comerciales

- Nombre/marca: ProsusMoney
- Ticker: xPR ó PROSUS
- Adquisición: minería, compra P2P, compra en exchange.
- Precio: variable, por oferta y demanda.

Misión

- Desarrollar una criptomoneda de fácil uso para el usuario sin conocimientos técnicos en informática.
- Usar la blockchain de ProsusMoney para experimentar con nuevos usos y aplicaciones.
- Ser sinónimo de *confianza y rentabilidad* para inversionistas.
- Ser una reserva de valor para el inversionista.
- Aumentar actividad en los exchanges donde la criptomoneda esté listada.

Visión

- Llegar a ser uno de los referentes del desarrollo tecnológico en Chile.
- Acercar a las personas a un paradigma de *Economía Basada en Recursos*.

Breve análisis: Rentabilidad en dinero fiat

En los cuatro años de funcionamiento de ProsusMoney, después de varios ensayos y al observar la interacción de los usuarios en nuestros canales de redes sociales, se llega a la conclusión que **el inversionista busca hacer crecer su patrimonio en dinero fiat usando a las criptomonedas como herramienta.**

Según testimonio de los usuarios, lo anterior es preferente a las intenciones iniciales de las criptomonedas en general, cuando pretendían ser medio de pago. También es preferente a la implementación de la tecnología blockchain en otros contextos industriales (por ejemplo en la trazabilidad logística). En síntesis, las ventajas tecnológicas de las criptomonedas en general se convierten en argumentos (marketing) para hacer subir su valor con respecto al dinero fiat.

No obstante, esta cualidad de intercambiabilidad de las criptomonedas a dinero fiat, hace que el mismo dinero fiat evolucione a un nuevo sustrato, de la misma manera en que de la sal se pasó al metal y del metal al papel. Actualmente estamos presenciando el traspaso de valor del dinero de banco central (físico o digital) a un dinero sin banco central. En concreto, del "dinero de papel" se evoluciona al algoritmo.

Propuesta de valor: criptomoneda multipropósito

- Plusvalía tecnológica: Una de las principales características de ProsusMoney es su constante evolución y adaptación a las necesidades de sus usuarios. Como parte de esta evolución está la depuración de código, lo cual lo hace ser compatible con otras tecnologías de gran proyección. Por ejemplo, la compatibilidad con ARM permite usos en IoT, la API (JSON-RPC) permite la comunicación con sistemas de inteligencia artificial.
- Compatibilidad: Tener similitudes con otras criptomonedas no constituye una desventaja, sino que garantiza una futura integración.

Exchange

Varios usuarios de criptomonedas en Chile estuvieron al tanto que una de las mayores preocupaciones de ProsusMoney fue no caer en el "fantasma" del *pump-and-dump* (tal como ocurrió con miles de criptomonedas en los años 2017-2018).

Por eso y, para lograr el ya mencionado traspaso de valor, se necesita estar preparado antes de entrar a un mercado de intercambios fiat-criptomoneda. Así pues, aparte de la compra y venta persona a persona (P2P), existen los intermediarios de confianza (o *escrow*) y principalmente los exchange.

Según lo observado en los canales de redes sociales, la preferencia que tienen los usuarios para elegir un exchange se resume en dos variables:

- Bajas comisiones y rapidez para retirar las ganancias.
- Mayor dinamismo y volumen del mercado.

ProsusMoney no puede intervenir en el primer punto pero sí puede hacerlo en lo segundo. Las siguientes ideas ejemplifican maniobras que se pueden ejecutar (para fomentar compras o ventas según sea el caso) para beneficiar al exchange donde esté listado.

- Calendarizar los momentos de la compra de *prosus*, imitando el sistema de reparto de utilidades de las empresas tradicionales (dividendos). Así se crean expectativas reales entre los usuarios.
- Sorteos (lotería) de cantidades determinadas de *prosus* (u otros premios), para quienes cumplen ciertas condiciones (por ejemplo, una cantidad mínima de Prosus para participar).

Conclusión

La criptomoneda ProsusMoney después de 4 años ha logrado una madurez tecnológica, gracias a sus voluntarios colaboradores, siendo capaz de adaptarse a las exigencias de los nuevos mercados.

Y al igual como ha sido el ya mencionado trabajo colaborativo de los programadores *Open Source*, los beneficios económicos de esta criptomoneda pueden ser compartidos justamente entre sus usuarios (inversionistas) y los intermediarios (exchanges).

ROADMAP

2021

- Campaña masiva en redes sociales.
- Listar criptomoneda ProsusMoney en nuevo exchange.
- Desarrollo orientado a dispositivos portátiles (ej: botón de pago).
- Piloto de *pago automático en comercio usando QR*, en local físico (tal como ya lo hacen en China con Wechat o Alipay).

2022

- Campaña de expansión internacional, al observar que hay muchos chilenos poseedores de *prosus* listos para comerciar con personas del extranjero.

2023

- Publicación científica (en formato *paper* o mini-documental), para mostrar resultados de la investigación de Prosus Corp a la tecnología blockchain.
- Tener presencia en Coinmarketcap.

2024

- Integración ("tandem") con alguna criptomoneda PoS (ejs: Cardano, Ethereum-2, Gridcoin).

2025-2029

- Desarrollo de nuevo cripto-activo y/o DLT, según *estado del arte*, intercambiable (swap) por ProsusMoney

BIBLIOGRAFÍA

- **Ferdous**, Md. Sadek & **Chowdhury**, Mohammad & **Hoque**, Mohammad & **Colman**, Alan. (2020). Blockchain Consensus Algorithms: A Survey.

  www.researchgate.net/publication/338738073_Blockchain_Consensus_Algorithms_A_Survey

- **Github – ProsusMoney** . Repositorio de código fuente, *issues* and *testing*.

  https://github.com/prosuscorp/prosus.money

- **Nicolas van Saberhagen**. (2013), Cryptonote Whitepaper

  https://web.archive.org/web/20200617033118/https://cryptonote.org/whitepaper.pdf

- **Nicolas van Saberhagen, et al.** (2014), Cryptonote Standar (technical details)

  https://web.archive.org/web/20200512035055/https://cryptonote.org/standards/

- **Stack Exchange – Monero Beta**. Comunidad de preguntas y respuestas.

  https://monero.stackexchange.com