Sistemas de pago electrónico y Criptomonedas

Blockchain - Tokens - GNU Taler

Javier Sepúlveda

Presidente de GNU/Linux Valencia

presidencia@gnulinuxvalencia.org

Asociación de Usuarios GNU/Linux de Valencia

April 30, 2022

INDICE

1. SISTEMAS DE PAGO ELECTRONICO
   - PAYPAL
   - Samsung Pay
   - Google Pay
   - Apple Pay
   - GNU Taler
2. CRIPTOMONEDAS !
   - Bitcoin - BTC
   - Ethereum - ETH
   - Cardano - ADA
   - ...Miles de alt-coins.

Sistemas de pago electrónico - IMAGEN

Comparativa sistemas de pago basados en cuenta y basados en TOKENS

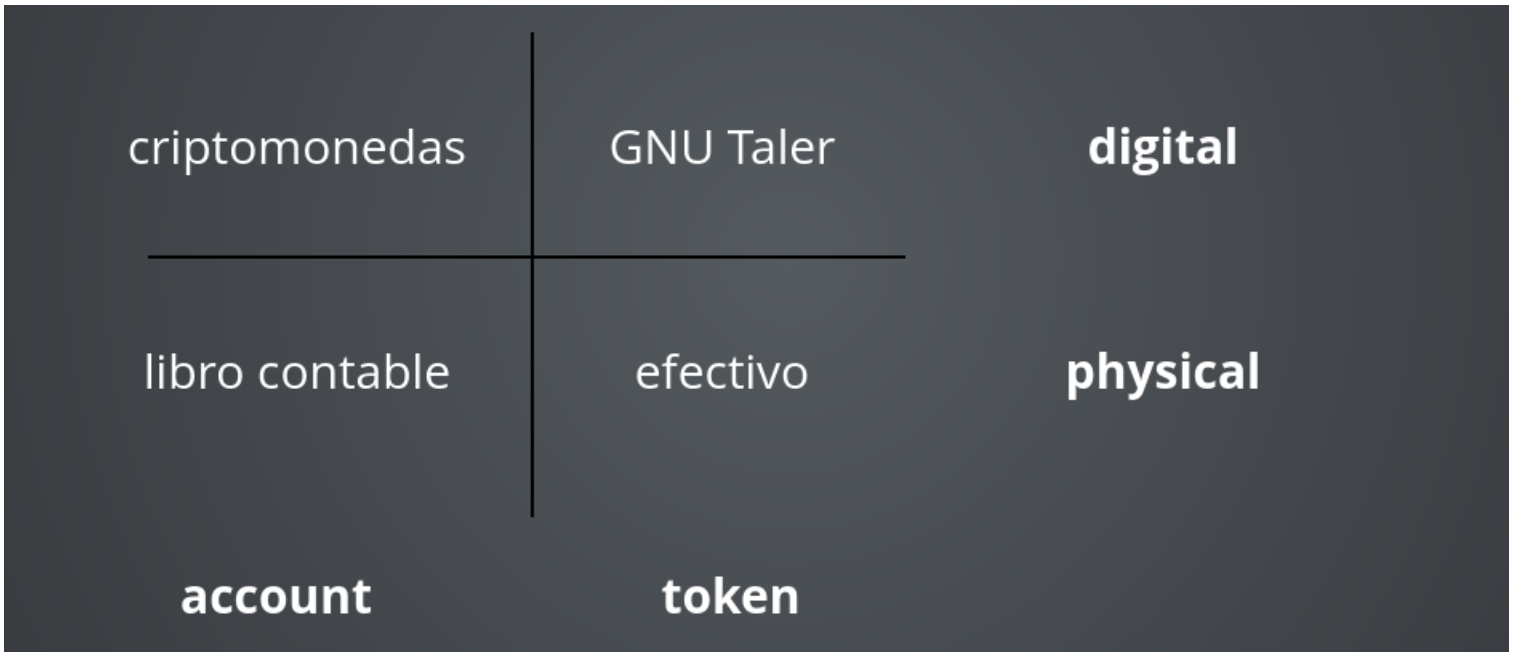


Figure: Sebastian Marchano @taler

Sistemas de pago: Cuentas vs. Tokens

Existen dos sistemas de pago:

1. **sistemas basados en cuentas**: la transferencia ocurre cobrando al comprador y dando crédito al vendedor. (ej: depósitos bancarios)
2. **basado en tokens**: la transferencia ocurre pasando el valor en sí mismo. El token representa el valor físico, como el billete.

La diferencia esencial, reside en la información que porta el activo:

- cuenta (activos): asociado al histórico de transacciones
- token (activos): porta la información sobre el valor nominal y la entidad que emitió el token

Bitcoin y las tecnologías de libro mayor distribuido (DLT), en general son sistemas basados en cuentas! La novedad es que el libro mayor es distribuido (descentralizado).

Que es GNU Taler?

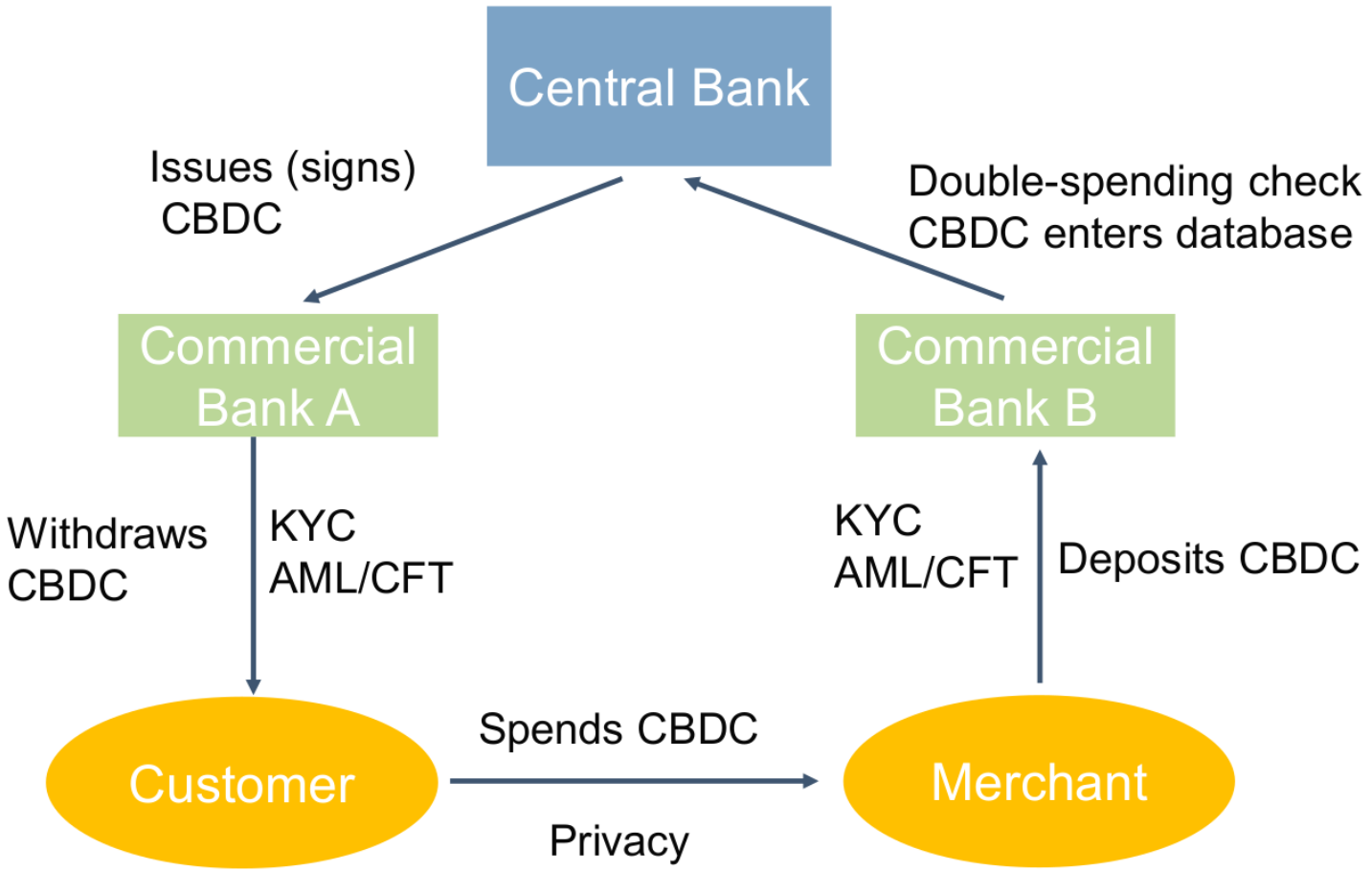
Taler es un sistema de pago electrónico
(**T**axable **A**nonymous **L**ibre **E**lectronic **R**eserve)

- Usa monedas(saldo) guardadas en el**carteras** del dispositivo del comprador
- Tal y como si fuera **efectivo**
- Permite pagar en **divisas existentes** (i.e. EUR, USD, BTC)

Que NO es GNU Taler

- *no es* una cripto-moneda
- *no* hace uso de la tecnología blockchain
- *no* está basado en proof-of-work
- *no* está pensado para almacenar valor a largo plazo
- *no* tiene volatilidad
- *no es* un activo especulativo
- *no es* una red o una instancia de un sistema
- *no es* descentralizado
- *no* está basado en hardware
- *no* pretende ser un reemplazo al dinero físico

Esquema de funcionamiento



Razones para adoptar GNU Taler

- **Consumidor/Usuario:** Privacidad en la compra
  - Pagos en instantáneos en 1 clic
  - Micro-pagos - Como artículos de prensa
  - Uso del dinero desde cualquier lugar del mundo
- **Vendedor:** Ventas en 1 clic, con cobro garantizado
  - Sencilla integración en paginas Web
  - Evita los falsos positivos y la devolución de carritos de compra
- **Bancos** Usar la infraestructura bancaria existente
  - Control sobre la moneda emitida BC
  - KYC, AML/CFT - Banco comercial
- **Gobierno:** Cobro de impuestos
- **Sociedad:** Población en **riesgo de exclusión financiera**
  - Evitar el oligopolio. Pocas empresas controlan hoy en día todo el sistema de pagos (comisiones altas).
  - División y gestión del dinero **earmarking**

ESTADO DE GNU TALER

1. Estado del proyecto
   - Presentado ya a Banco de España y otros bancos europeos.
   - 5 millones de euros invertidos
   - Complemento para navegador
   - APP para teléfonos
   - URL: https://taler.net
   - White paper en español: https://taler.net/papers/cbdc2021es.pdf
   - Demo: https://demo.taler.net

BITCOIN

1. BTC (criptomonedas) afectarán a las banca, como la imprenta afecto a la iglesia.
2. Jefferson separó la **iglesia y el estado**. BTC separa **dinero del estado**.
3. BTC no es un sistema de pago es mucho mas. Es un concepto disruptivo.
4. Base de datos o libro mayor. publico, inviolable, red distribuida, registra, valida y verifica
5. Su unidad mínima es el satoshi.
6. Escasez, duradera, fungible,transmisible, trackeable.
7. La blockchain no es alterable, cada bloque apunta al siguiente.

BITCOIN

1. Creada por Satoshi Nakamoto en 2009
2. Escasez solo 21 millones de unidades
3. Halving cada 4 años, cada vez un 50% menos de recompensa.
4. basado en PoW
5. ¿Calentamiento global? Datacenters en países nórdicos.
6. el dinero se crea, se guarda, y se transfiere. Siempre disponible.
7. Que resuelve BTC
   - El problema del general Bizantino (consenso)
   - Doble gasto (libro mayor / ledger)

Características de Bitcoin

1. cuando al menos 3 nodos validan la transacción avisan al resto de nodos.
2. la base de datos o libro mayor, es completamente distribuido
3. no es anónimo, se pueden consultar todas las transacciones (blockchain.com)
4. rastreo forense se puede conocer sobre las carteras.
5. Es divisible hasta 8 dígitos (100 millones)
6. Cada 4 años se produce un halving
7. Cada 10 minutos se genera un bloque de 1MB
8. Cada 210.000 bloques de 1MB, halving. (cada 4 años)
9. No es posible acabar con BTC, se necesitarían el 51% de los pc que lo sustentan.
10. Todos los ordenadores de Google son el 1% de la red BTC
11. La blockchain ya existe en satélites

Los costos de mantener la blockchain

1. 2012 se recompensaba a la red con 50 BTC
2. 2016 con 25 BTC
3. 2020 con 12,5
4. 2024 sera la mitad. Compensará? Dependerá del precio de BTC.
5. Cada vez hay más datacenters, más compentencia, solo 1 gana el premio cada 10 min.
6. En España no se mina BTC, pero si ETH
7. Cada 10 minutos se genera un bloque de 1MB
8. Cada 210.000 bloques de 1MB, halving. (cada 4 años)
9. No es posible acabar con BTC, se necesitarían el 51% de los pc que lo sustentan.
10. Todos los ordenadores de Google son el 1% de la red BTC
11. La blockchain ya existe en satélites

Imagen blockchain

LIBRO MAYOR DISTRIBUIDO POR MILES DE DATACENTERS

Figure: **Pixabay License**

Criptomoneda

1. Una moneda digital, con un valor comparable con otras monedas o el dinero fiat como el EURO o Dolar.
   - Bajo licencias de software libre como la licencia MIT
   - Alt-coins - Derivaciones de criptomonedas existentes
   - Blochain permisionada o no.
   - PoW o PoS
   - Basadas en cuentas (blockchain (distribuida))
2. ADA:Licencia Apache
3. LTC:Licencia MIT
4. Dogecoin:Licencia MIT
5. Clave publica / Clave privada
6. La clave privada puede almacenarse en un exchange
7. La cartera fria (almacenamiento de la clave privada)

Mineria

- Minado y costes de electricidad.
- Rig
- Pool de mineria
- Minado con CPU o GPU
- hashes/segundo

Agradecimientos

Las Naves

- Ana Melchor
- David Rosa
- Maria Jesús Sánchez

GNU

- Richard Stallman
- Christian Grothoff

GNU Linux Valencia

- Julian Moyano
- José Mico
- Jose Mira (latex)

GRACIAS

¿Preguntas, Comentarios?

Descarga esta presentacion - CC SA 4.0

- Transparencias en LaTEX
  https://valenciatech.com/flisol-2022-javier-sepulveda.tar
- Realizadas con Latex, bajo GNU/Linux Debian 11