GNU Taler

DIGITAL CASH MADE SOCIALLY RESPONSIBLE

⟨Taler⟩

< **T**axable >
< **A**nonymous >
< **L**ibre >
< **E**lectronic >
< **R**eserve >

< **Javier Sepulveda – GNU Speaker** >

Patrocinadores y apoyos

- Inria
- Universidad de Berna de Ciencias Aplicadas
- Asoka
- Pretty Good Privacy
- The GNU Project

Sistemas actuales

- **Pago en efectivo o contra-reembolso**
  - No permite pagos digitales
- **Transferencia bancaria**
  - Es lento y no inmediato
- **Pago con tarjeta de débito o crédito**
  - Visa, MasterCard – Alta vigilancia al comprador
- **Pago a través de pasarelas de pago**
  - Paypal, Apple Pay, Ali Pay, …
  - Pocas empresas muy grandes = Oligopolio
- **Pago a través de cripto-monedas como Bitcoin**
  - Sistema no-regulado

Nuestras opciones

- **Sufrir vigilancia masiva** usando sistemas de pago con tarjeta como VISA o MasterCard
- **Usar pasarelas de pago como Paypal**
  - El mercado está repartido entre muy poca empresas
- **Usar cripto-monedas inestables** y **des-reguladas** que fomentan las actividades ilegales
  - Moneda des-regulada
  - Sin garantías
- **Usar GNU Taler**
  - Usa la infraestructura bancaria existente

Pagos con tarjeta

- Cuando pagas con tarjeta esta incluye tu **nombre**
- Cuando pagas con tarjeta en persona, tu **ubicación** es conocida
- Los **datos de tus compras**, son compartidos con empresas asociadas.
- Muchas veces no dispones de otros medios de pago
- Casi nunca puedes usar la tarjeta de otra persona
- Las tarjetas de pre-pago anónimas son caras y complicadas de conseguir
- La información de cada transacción es almacenada por unos 6 años

Pasarelas de pago

PayPal

SAMSUNG pay

Alipay

Pay with Amazon

pay

Pay

Predicciones

- Google, Facebook o Amazon quieren ser tu sistema de pago
- Estas empresas conocen tu historial de búsquedas, gustos y compras
- Ellas te proveerán de sistemas de pago más usables, rápidos y conocidos, el sistema bancario tradicional será historia.
- Cuando dominen el sector de los pagos on-line, empezarán a cobrar comisiones, acorde con el tamaño de su oligopolio.
- Los competidores y vendedores que no se alineen con sus valores corporativos, serán excluidos por sus términos de servicio y se irán a la bancarrota

Bitcoin - BTC

- Es una cripto-moneda programada por Satoshi Nakamoto
- Basada en un **libro mayor público descentralizado**
- Cada usuario debe contar con la copia de este libro mayor
- Es público y no gobernado por ninguna empresa o entidad
- Solo cuenta con un número limitado de monedas
- Desde su aparición, su valor ha sido muy volátil

Transacciones en Bitcoin

- Cada transacción es difundida por toda la red
- Un sistema de consenso distribuido confirma cada transacción y la incluye como un nuevo bloque en la blockchain (libro mayor)
- A este proceso de consenso computacional se le llama minería
- Confirmar cada transacción tarda entre 10 y 20 minutos
- Tiene un alto gasto energético
  - Tanto como el gasto diario eléctrico de un hogar norteamericano
  - Si existiera comisión por transacción, esta sería de unos 100 dólares

Los defectos de Bitcoin

- Valor inestable
- Transacciones lentas
- Alto coste energético por transacción
- Su alta descentralización fomenta la anarquía del sistema
- Bitcoin solo ofrece pseudo-anonimato pero no el anonimato completo

Algoritmo proof-of-work

- Algoritmo de consenso
- 1993 creado para evitar ataque por denegación de servicio y spam
- 2009 usado por BTC para confirmar nuevos bloques (transacciones)
-

Como funciona proof-of-work

- Un problema complicado es dado a los mineros
- La solución a este problema es fácil de comprobar
- Una vez un minero ha llegado a la solución, esta es comprobada por el resto.
- El nuevo bloque se añade al libro mayor (blockchain)
- El resultado se difunde por toda la red
- Este proceso es muy costoso a nivel computacional y de consumo de energía.

⟨Taler⟩

Que es GNU Taler

- Es un **sistema de pago**
- **No es un cripto-moneda**
- Solo usa la cuantía digital que tiene almacenada cada usuario en su cartera electrónica en su propio dispositivo
- Es como **dinero efectivo electrónico**
- Puedes recargar tu cartera con cualquier divisa actual a través de un banco
  - EUR, USD o incluso BTC

GNU Taler la moneda

- Identificada por clave pública
  - Solo el propietario cuenta con la clave privada
  - El banco firma ciegamente la moneda
  - El banco firma la moneda electrónica con su propia clave publica, para garantizar la moneda.

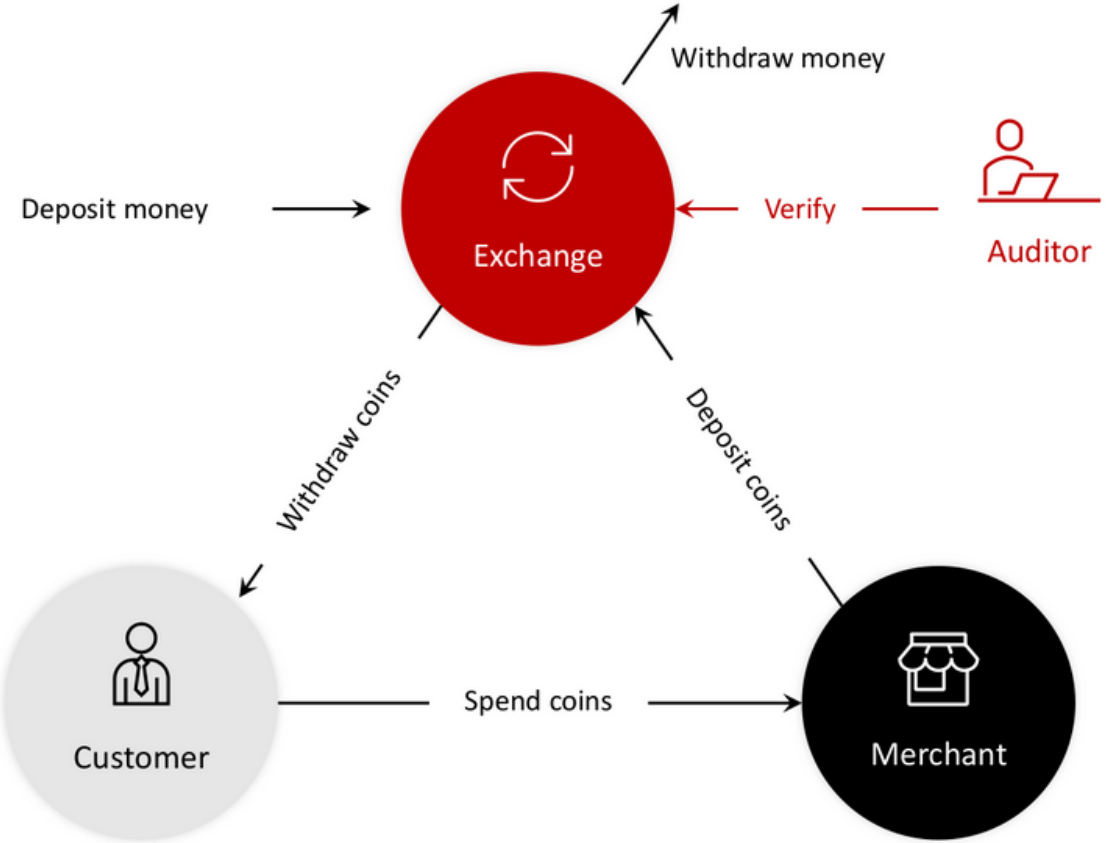
Metas de diseño I

- Debe ser programado en **Software Libre**
- **Proteger la privacidad del comprador**
  - Compras 100% anónimas
- **Permitir al autoridad fiscal conocer los ingresos de los vendedores**
- Poner fin a los negocios ilegales
- Prevenir el fraude en los pagos
- **Ser rápido**
- Usar la infraestructura bancaria existente
- Evitar los oligopolios

Metas de diseño II

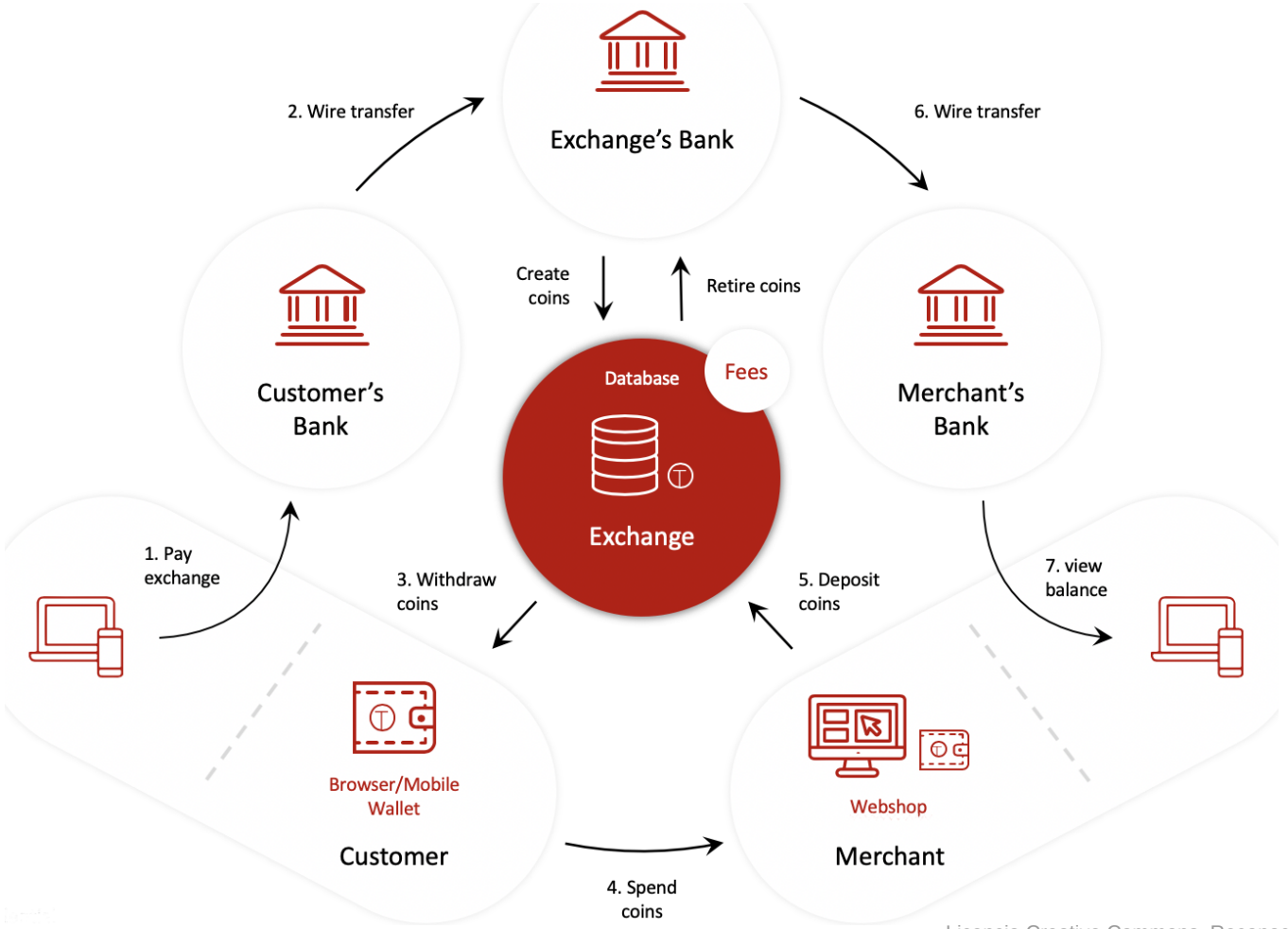
- Ser respetuoso con medio ambiente
  - Evitar el alto consumo de electricidad como hace Bitcoin
- Solo revelar la información necesaria mínima
- Ser usable
- Evitar puntos de fallo
- Fomentar la competitividad
- Ser intrazable para garantizar el anonimato

La arquitectura



Source : https://taler.net/it/features.html

Como funciona



Las transacciones en GNU Taler

- No se basan en tecnología blockchain
- No requieren minería
  - No se basan en proof-of-work
- No se basan en ningún otro mecanismo de consenso distribuido
- Se basan en el **algoritmo de firma ciega**

GNU Taler Wallet

- **Tu cartera (wallet) almacena tu saldo**
  - Se llaman Kudos en la demo de GNU Taler, pero serán en la realidad euros, dólares o la divisa que compres directamente a tu banco.
- **¿ Donde se guarda mi balance ?**
  - Tu PC guarda tu balance
  - El exchange mantendrá el balance de tus fondos no gastados en un cuenta de garantía de depósito
- **¿ Y si pierdo mi cartera electrónica GNU Taler ?**
  - Es lo mismo como tu cartera física en el mundo real
  - Para evitar esto puedes hacer copias de seguridad
  - Para minimizar riesgos puedes mantener un saldo bajo

Lo bueno de GNU Taler

- Es Software Libre
- Evita el lavado de dinero
- Evita mercados y actividades ilegales
- Obliga a los vendedores a ser transparentes con sus ingresos
- Previene la inflación y la volatilidad
  - No se genera más moneda
  - El valor del contenido de la cartera no sube o baja de valor como tal
- Programa licencia bajo licencia General Public License GPL v.3

Ventajas para el comprador

- Es muy fácil de instalar
- Pagos en un solo clic
- Sin necesidad de registrarse en la página de venta
  - Si existirá registro para la compra en tu banco de fondos anónimos para tu cartera
- Sin necesidad de proporcionar datos personales
- Es Software Libre, lo que es garantía de calidad y seguridad.
- Posibilidad de transferir dinero a familiares y amigos
- Sin falsos positivos en la detección de fraude de tarjetas
- Posibilidad de realizar copia de seguridad de tu cartera electrónica

Ventajas para vendedor

- Es un sistema de pago rápido
- Es software libre
  - Esto garantiza buen soporte
  - Y precios competitivos
- Cumple con la regulación europea GPDR

Casos de uso

1) Campos de refugiados
2) Periodismo más independiente
3) Recibir dinero por correo electrónico
   - Ganar dinero por leer publicidad o correo electrónico no-deseado (spam)

1) Campos de refugiados

- **Ahora :**
  - Distribución directa de bienes a la población
  - Actividad económica limitada
  - Alto nivel de dependencia económica
- **Con GNU Taler :**
  - Divisa local emitida asegurada por la cantidad de ayuda recibida
  - Aplicación de impuestos proporcionales basado en el estatus económico
  - Gobierno local habilitado para impuestos locales
  - Incremento de la independencia económica y participación local

2) Periodismo

- **HOY**
- Estructura corporativa
- Ingresos principales por anunciantes
- Rastrear la actividad de los lectores, es la clave del éxito económico
- Periodismo y marketing, difíciles de diferenciar.
- **Con GNU Taler**
- Micro-pagos en un solo clic por artículo
- El hospedador no requiere de experiencia
- La información financiada por el lector, queda separada de la publicidad
- Los lectores pueden permanecer anónimos

Métodos de encriptación

- Funcion hash criptografica (1989)
- Firma ciega (1983)
- Firma Schnorr (1989)
- Diffie-Hellman intercambio de llaves (1976)
- Cortar y elegir prueba de conocimiento-cero (1985)

Visiones futuras

- Recibir pagos por leer anuncios
- Recibir pagos por recibir spam
- Dar bienestar a los usuarios sin altas comisiones
- Eliminar la corrupción haciendo todos los ingresos visibles
- Parar la minería que inutilizada las cripto-monedas

Que necesitamos para empezar

- Instalar el programa GNU Taler
  - Complemento de navegador (Firefox, Chrome)
  - Aplicación para Android

Más información

- **URL :** Taler. Net
- **Lista de correo :** taler@gnu.org
- **Api:** Api.taler.net
- **Git:** Git.taler.net
- **Demo :** Demo.taler.net
- **Twitter:** @taler

Dejemos que el dinero facilite el comercio, pero asegurémonos, de que el capital sirva a la sociedad

Equipo de GNU Taler

Agradecimientos

- Equipo de GNU Taler – Taler SA
- Patrocinadores de GNU Taler
- Proyecto GNU.org
- Asociación de Usuarios GNU Linux Valencia
- Fundación Las Naves Valencia