



Aplicaciones de DLT (Blockchain) en seguros



16 de noviembre, 2017

@aaramburu
aaramburu@kayum.mx

Bitcoin: A Peer-to-Peer Electronic Cash System

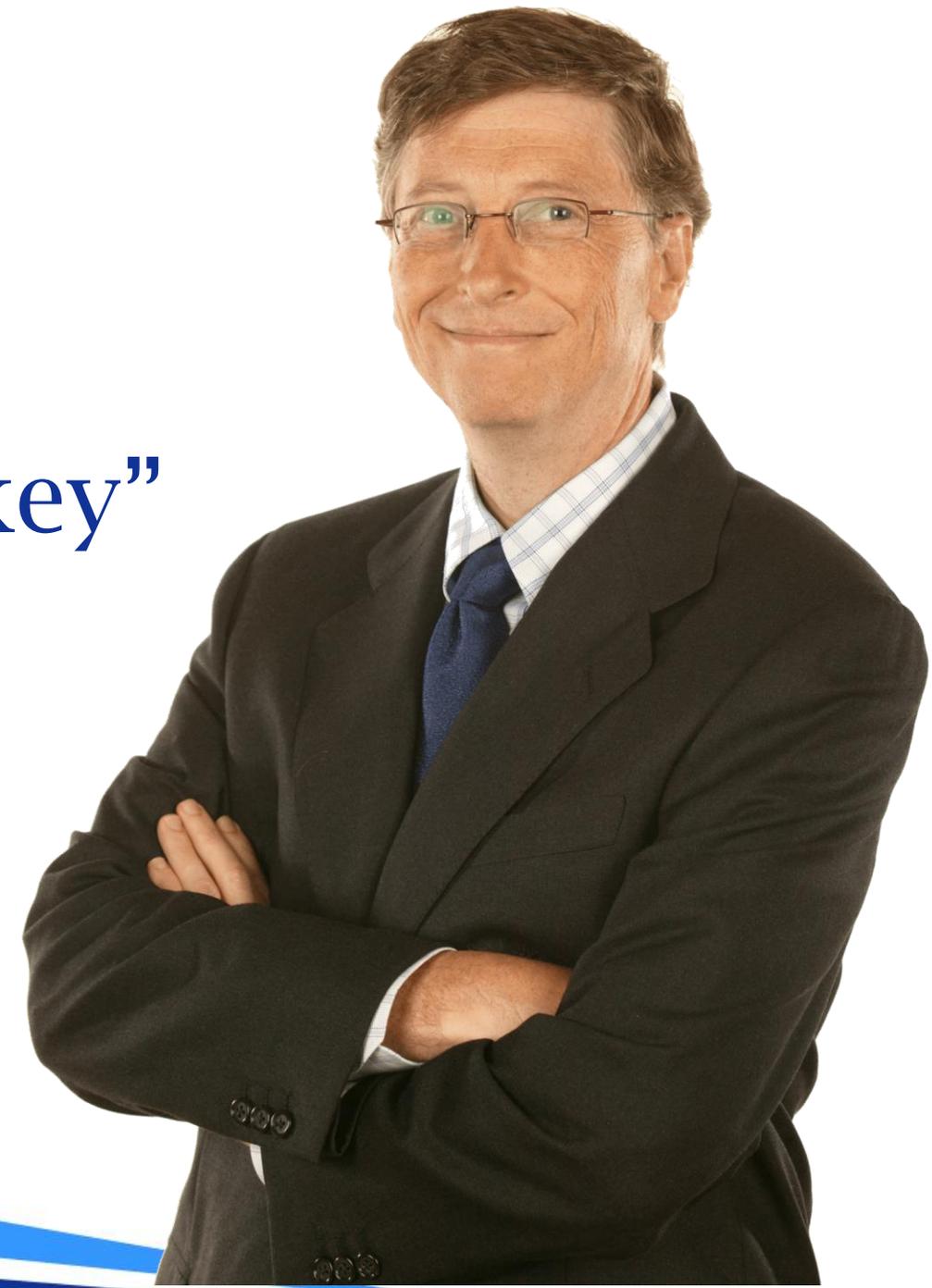
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As more nodes join the network, the proof-of-work required to create a new block increases, making it computationally infeasible for any one person to control the network. To attack the network, they would have to generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

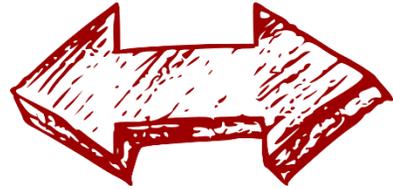
Satoshi Nakamoto, 1° de noviembre, 2008

“The bitcoin technology is key”

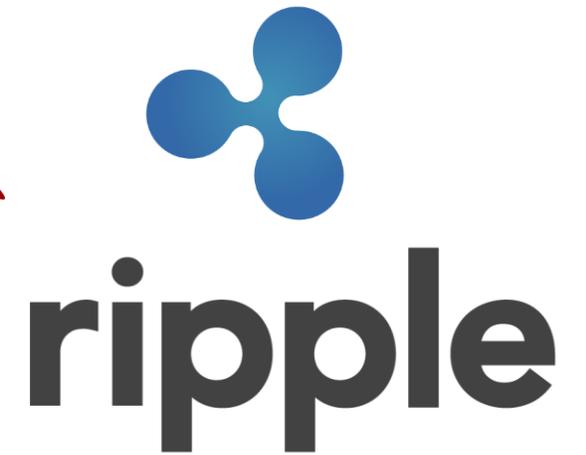
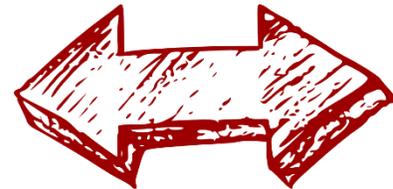
Bill Gates, 2014



Blockchain facilita coordinación

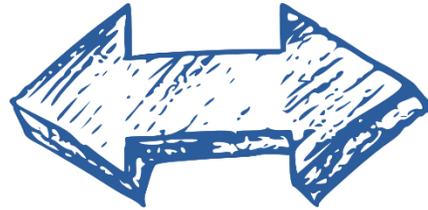


HOY



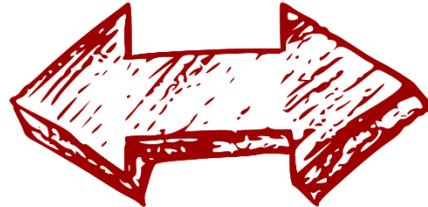
Propiedades de blockchain

**Transacciones
irreversibles**



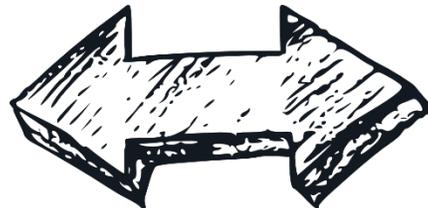
Registro inmutable

**Plataforma
descentralizada**



**Reglas comunes entre
participantes**

**Registro
compartido**



**Conciliación común de
transacciones, con historia
de movimientos**

Ejemplo: inmutabilidad

❑ El abuelo Juan asegura su cosecha

- Envía a la aseguradora la superficie y el valor a asegurar y fotos iniciales
- Registro en un blockchain

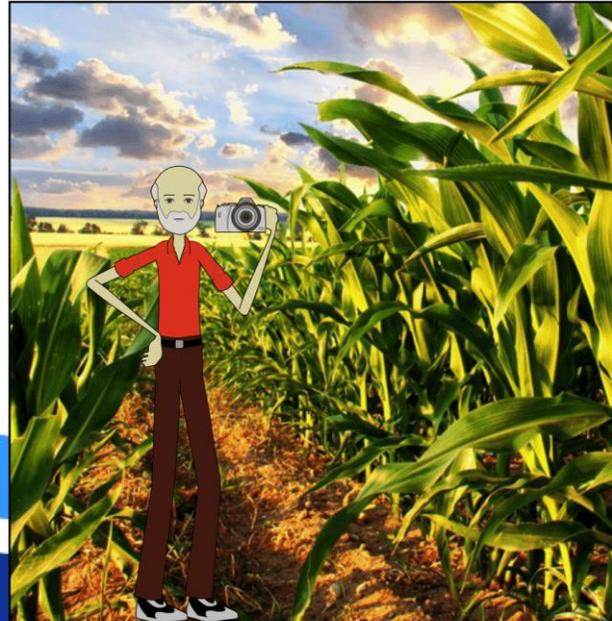
❑ Cada semana toma fotos a la cosecha

- Envío de fotografías geo-localizadas, con timestamp
- Registro en un blockchain

❑ Si hay siniestro

- Envío de nueva foto a la aseguradora
- El ajustador usa historia inmutable y registro meteorológico para decidir pago

Asegura la cosecha



by aaramburu

Aplicaciones de Blockchain en Seguros: inmutabilidad

Pruebas de existencia compartidas



Existencia de pólizas

Existencia de eventos

Existencia de siniestros

Ejemplo: inmutabilidad y reglas comunes

Historia de Siniestros en un blockchain

- Firmada por cada aseguradora
- Disponible a otras aseguradoras de forma anónima

Asegurar mi auto



Prueba de identidad e interés asegurable

- Comprueba género, edad, código postal e historia de siniestros
- Recibe ofertas de aseguramiento firmadas

Pruebo quien soy



Contrata el seguro

- Elije oferta ganadora
- Revela identidad y propiedad de vehículo
- Paga póliza
- Prueba de aseguramiento al Blockchain

Revelar, contratar y pagar



Aplicaciones de Blockchain en Seguros: inmutabilidad y reglas comunes

**Pruebas de
existencia
compartidas**



**Historia de siniestros
Propiedad del vehículo**

Reglas comunes



**Historia de siniestros
Protección de datos
personales**

Ajuste a través de terceros

Ejemplo: reglas comunes y registro compartido

- ❑ Juan desea cobertura para una enfermedad catastrófica
 - Desea asegurarse al menor costo posible

- ❑ Forma una mutualidad bajo reglas vigentes
 - Invita a personas similares en todo el país a participar en la mutualidad
 - Mutualistas aportan al fondo social

- ❑ El seguro se paga
 - Las reglas de la mutualidad se ejecutan desde un "Smart contract"
 - Los siniestros se ajustan vía un tercero certificado

Enfermedad catastrófica



Aplicaciones de Blockchain en Seguros: reglas comunes y registro compartido

**Registro
compartido**



**Historia de pagos de primas
Registro de riesgos asegurados**

Reglas comunes



**Reglas ejecutadas a través de
“Smart contracts”
Menores costos de coordinación
Ajuste a través de terceros**

- Prueba de aseguramiento
- Grupo de trabajo blockchain en la AMIS

Mexico



Prueba de aseguramiento

1



Cada póliza tendrá un QR CODE con los datos de la misma

2



Para comprobar que la póliza esta vigente, se escanea el QR-CODE en los puntos de controles definidos

3



La solución comprueba que la póliza existe, y muestra todos los datos de la misma

Oportunidad

- Seguros masivos
- Nuevos mercados
- Reducción de costos

- Personalidad jurídica
- Accionistas
- Industria Regulada
 - Requisitos de Solvencia
 - Registro de Productos
 - Reportes
- Función social

- Descentralizado
- Sin censura
- Inmutable
- Pública
- Verificable
- No falsificable
- Programable

Realidad

Blockchain

**Probar
Aprender
Errores
Crecer
Gran futuro**



@aaramburu
aaramburu@kayum.mx