SMART CONTRACTS

Universidad del Rosario

TIC TANK

1. EL CONTRATO ELECTRÓNICO

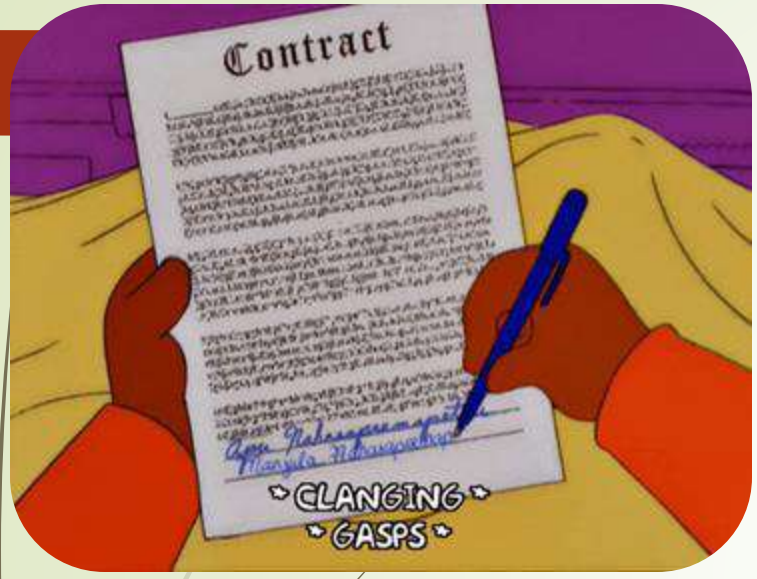
a. La equivalencia funcional de la Ley 527

b. La Libertad de forma y la aplicación de las normas sustanciales

c. Los Acuerdos Marco en el B2B

d. Los Términos y Condiciones de Uso en el B2C

e. El consentimiento electrónico y la firma



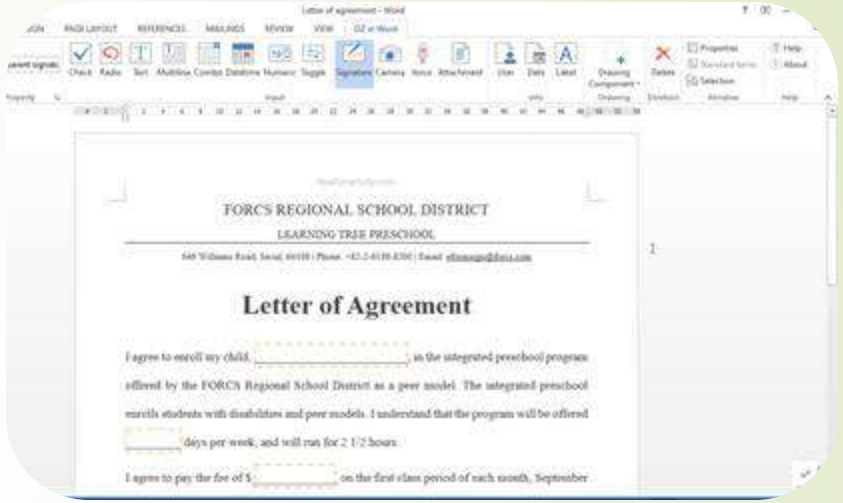
"En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos."

Validez de los contratos formados mediante mensajes de datos

Ley 527 de 1999, artículo 14

Elaboración del contrato

Chinomatic:



FORCS REGIONAL SCHOOL DISTRICT

LEARNING TREE PRESCHOOL

Letter of Agreement

I agree to enroll my child, _____, in the integrated preschool program offered by the FORCS Regional School District as a peer model. The integrated preschool enrolls students with disabilities and peer models. I understand that the program will be offered _____ days per week, and will run for 2 1/2 hours.

I agree to pay the fee of $_____ on the first class period of each month, September

Contract Legaltech Builders:

2. ¿QUÉ SON LOS SMART CONTRACTS?

El criptógrafo Nick Szabo creó el concepto de Smart Contracts como un grupo de promesas especificadas en forma digital con las cuales las partes ejecutan sus promesas (Nick Szabo, Smart Contracts: Build Blocks for Digital Markets, 1996).

En cambio un contrato inteligente es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores. Evitan el lastre de la interpretación al no ser verbal o escrito en los lenguajes que hablamos. Los *smart contracts* se tratan de "scripts" (códigos informáticos) escritos con lenguajes de programación, siendo los términos del contrato puras sentencias y comandos en el código que lo forma.

Por otro lado, un *smart contract* puede ser creado y llamado por personas naturales y/o jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma. Un *smart contract* tiene validez, sin depender de autoridades, debido a su naturaleza: es un código visible por todos y que no se puede cambiar al existir sobre la tecnología *blockchain*, la cual le da ese carácter descentralizado, inmutable y transparente.

2. ¿QUÉ SON LOS SMART CONTRACTS?

Esto significa que

- Se programan las condiciones;
- Se firman por ambas partes implicadas;
- Y se ‘coloca’ en una blockchain para que no pueda modificarse;

Y por otra parte, tienen como objetivo principal:

- Implementar una estado de seguridad mayor al del contrato tradicional;
- Reducir costes;
- Reducir el tiempo asociado a este tipo de interacciones.

3. ¿Qué es Blockchain?

Blockchain es un sistema de código abierto donde se registran, a través de un libro contable distribuido y descentralizado, transacciones o cualquier tipo de información digital. Estas transacciones se reproducen en miles de ordenadores alrededor del mundo, logrando toda la protección y seguridad de la información que ahí reposa, por ello no requiere de un intermediario que valide el registro.

3. ¿Qué es Blockchain?

Blockchain es un sistema de código abierto donde se registran, a través de un libro contable distribuido y descentralizado, transacciones o cualquier tipo de información digital. Estas transacciones se reproducen en miles de [illegible] mundo, logrando toda la protecció[illegible]n que ahí reposa, por ello [illegible] valide el registro.

La **información digital** es un conjunto organizado de datos procesados que constituyen un mensaje y cuya codificación se reduce a dos valores:

0 y 1

3. ¿Qué es Blockchain? - Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

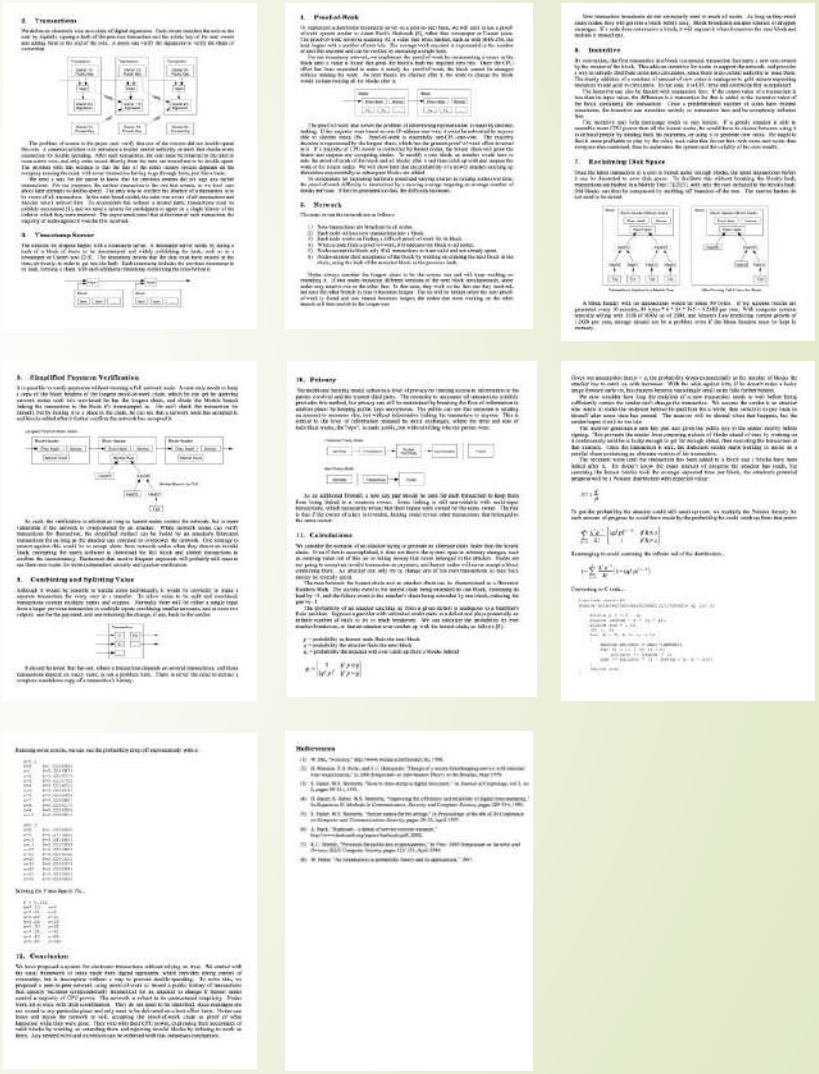
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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 long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.



3. ¿Qué es Blockchain?

Alicia

Dario

Bernardo

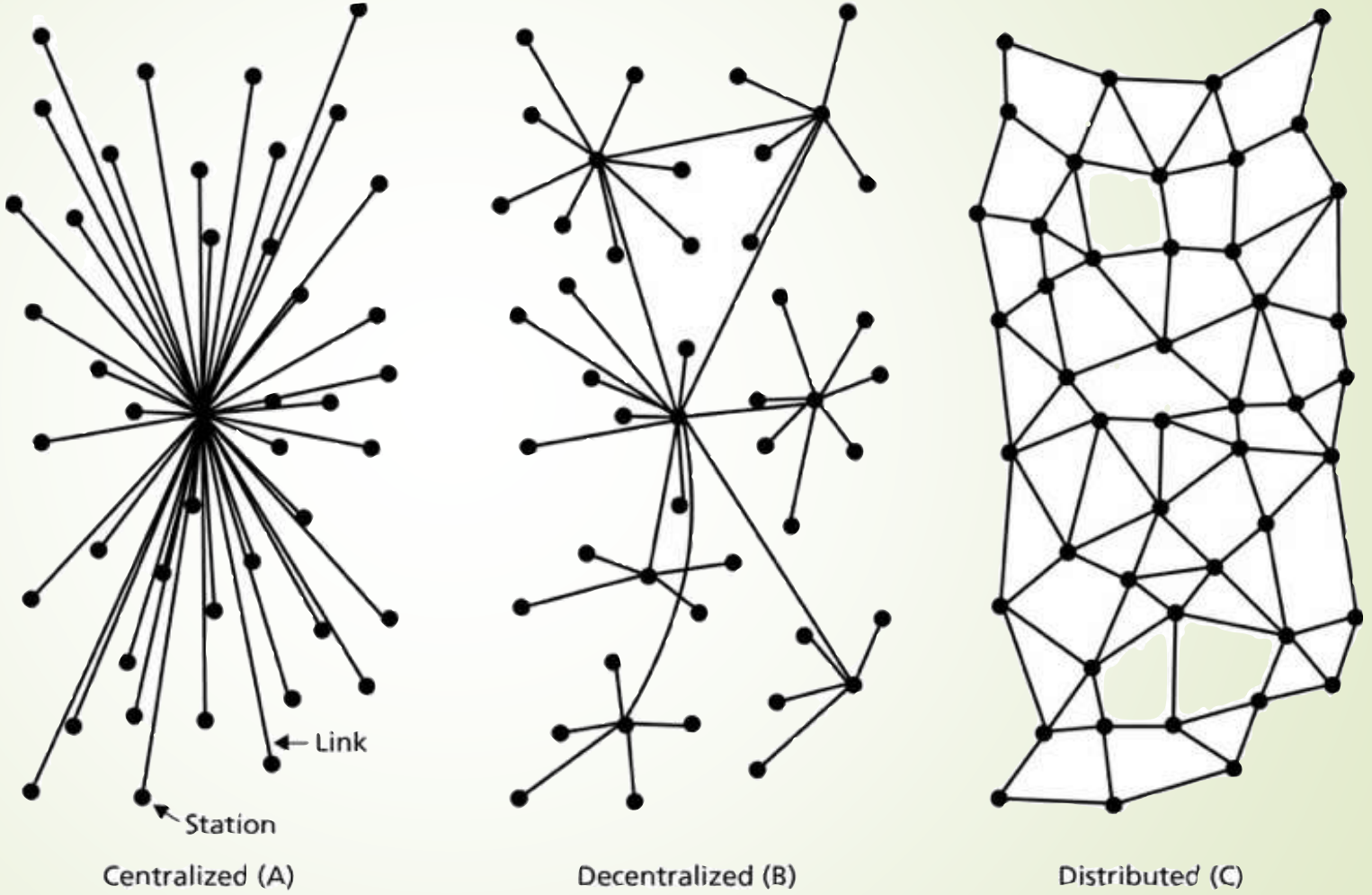
2 + 2 =?

Anonymous

Carlos

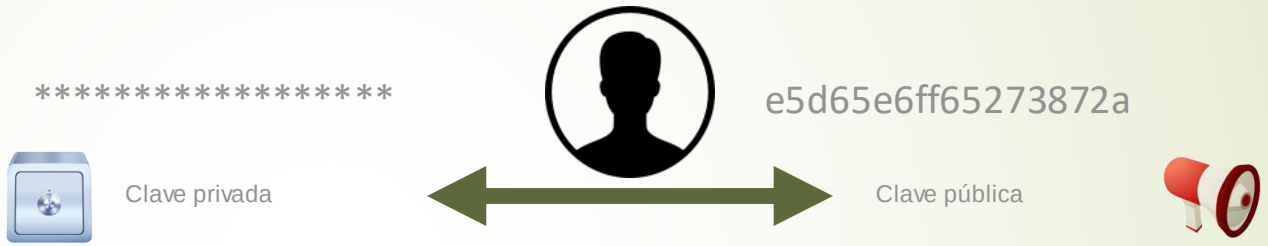
3. ¿Qué es Blockchain? - Consenso

3. ¿Qué es Blockchain? – BB DD

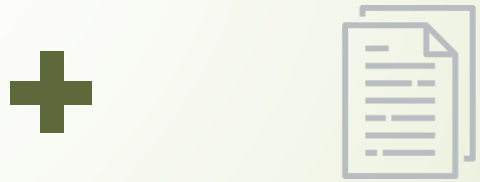


3. ¿Qué es Blockchain? – Criptografía

1. Cada persona tiene un par de claves relacionadas matemáticamente:



2. Usamos la clave privada para firmar



4b23c42dd43ee32951aa2dd

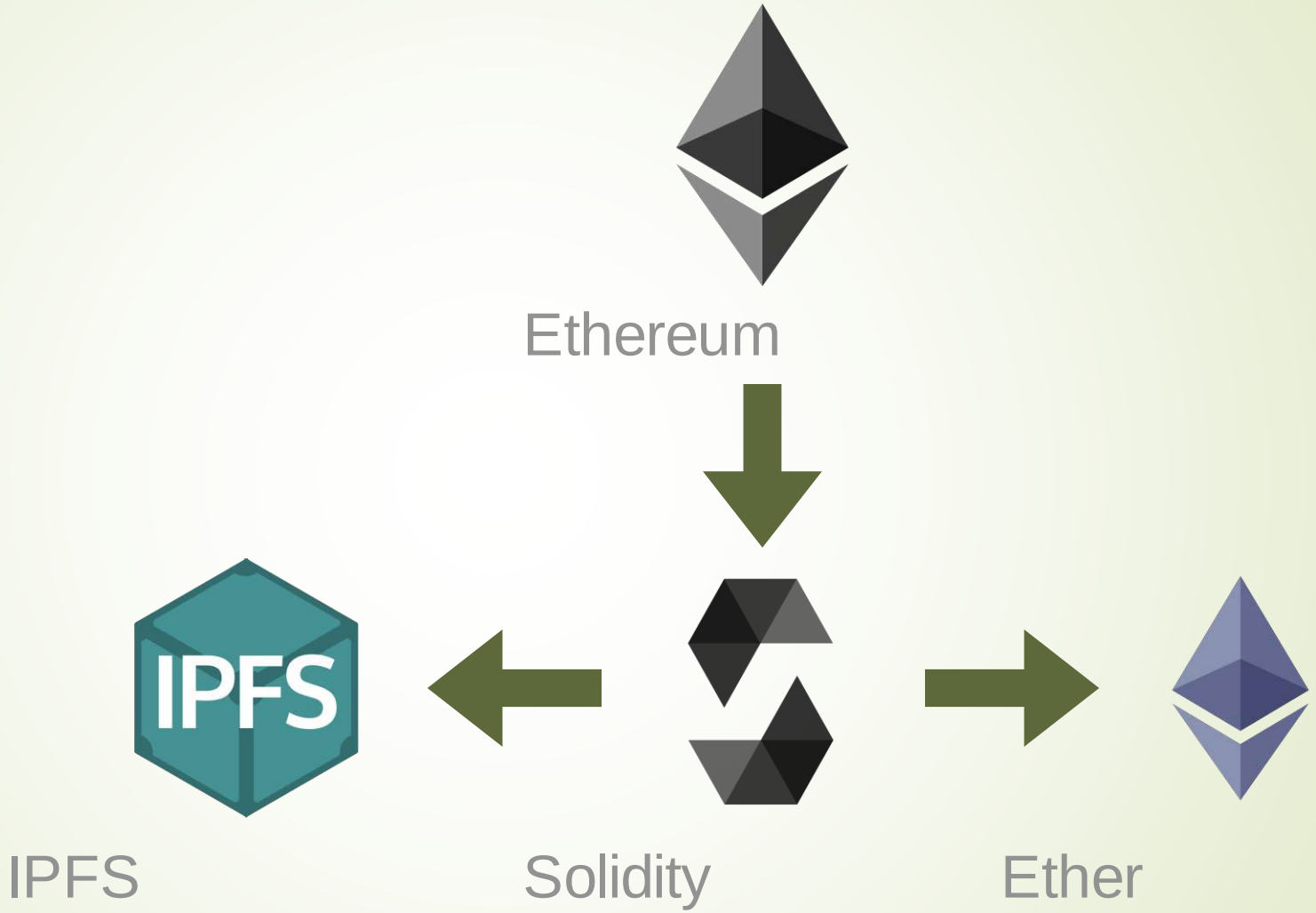
Firma

Criptografía asimétrica o de curva elíptica

3. ¿Qué es Blockchain? – Principios

- Integridad de la Red
- Poder distribuido
- El valor como incentivo
- Seguridad
- Privacidad
- Derechos preservados
- Inclusión

3. ¿Qué es Blockchain? – Ethereum



3. ¿Qué es Blockchain? – Ethereum

4. Aplicaciones - Servicios financieros

4. Aplicaciones - Servicios financieros

Préstamos: si la persona que contrata el préstamo no realiza el pago en el tiempo estipulado, se ejecutaría el contrato para retirarle las garantías.

Liquidación de operaciones: los contratos calculan importes de liquidación y transfiere fondos automáticamente.

Pagos de cupones y bonos: los contratos calculan y pagan automáticamente de forma periódica los cupones y devuelve el capital al vencimiento de los bonos.

Microseguros: Calculan y transfieren micropagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotriz de pago por uso)

Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor.

Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos.

Automatización de pagos y donaciones: se pueden acordar pagos o donaciones periódicas o puntuales a personas o entidades. El contrato inteligente lo que haría es verificar que se cumplen las reglas para realizar automáticamente la donación.

4. Aplicaciones - Servicios de la salud

Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores.

Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micropagos automáticamente al paciente para su participación.

Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos IoT -Internet of Things- (conectados a Internet). Los contratos generan automáticamente recompensas basadas en hechos específicos.

Servicios de propiedad intelectual

Distribución de royalties: el smart contract calcula y distribuye los pagos de royalties a artistas y otras partes asociadas según los términos acordados.

5. Algunas Conclusiones

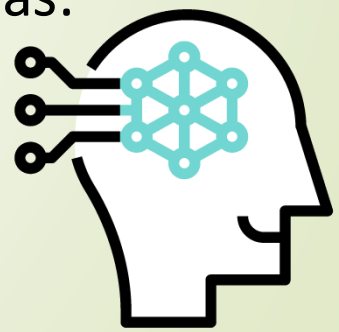
- ✓ Los operadores jurídicos deben reaprender, entender e implementar conceptos innovadores para gestionar y resolver conflictos, usando las nuevas tecnologías.
- ✓ Legaltech se basa en la optimización de procesos, lo cual puede evidenciarse mediante la automatización de los contratos, siendo esta automatización mediante minutas el principal antecedente de los Contratos inteligentes.
- ✓ Contratos mediante la automatización utilizando fuentes públicas o privadas de información.
- ✓ Los Smart Contracts se pueden evidenciar como una aplicación del principio de la autonomía de la voluntad, teniendo igual valor jurídico y probatorio que los contratos en papel.

- ✓ Los Smart contracts son verdaderos contratos con plena validez en el ordenamiento jurídico colombiano, no se modifica así su naturaleza jurídica ni sus elementos.

- ✓ Contribuyen a la seguridad de las partes al momento de la celebración de los contratos, ya que se tiene certeza del cumplimiento de las prestaciones.

- ✓ Otorga seguridad ya que no admite interpretaciones contrarias.

- ✓ Pero…no se pueden corregir errores de programación.



Universidad del Rosario

GRACIAS