



# Riesgo de LA/FT, criptomonedas y Blockchain

Luis Eduardo Daza Giraldo  
CP, MBA, CAMS, CIPLAD, Auditor Forense

# ¿Cómo y cuánto se lava?

**UNODC:**  
2 - 5% PIB [USD 800 billion – 2 trillion]



Negocios



Activos intangibles



Criptoactivos



Efectivo



Personas



Empresas

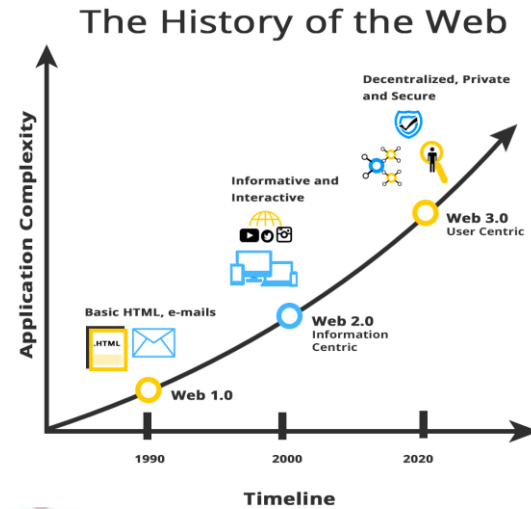


**IMF (Fondo Monetario Internacional):**  
USD 590 billion - 1.5 trillion

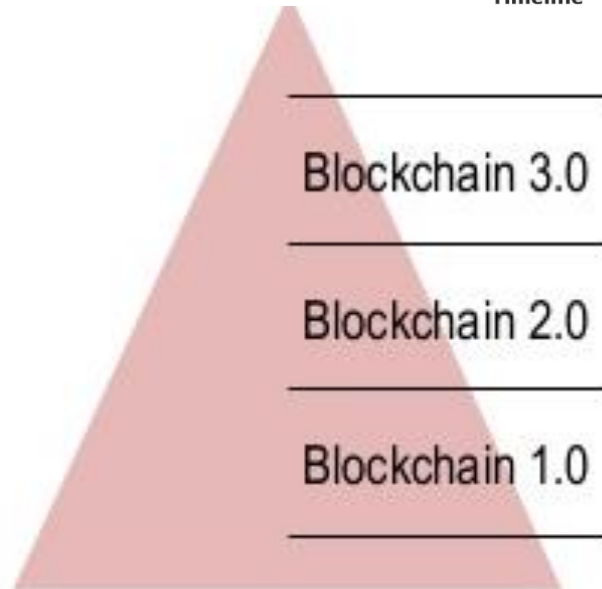




## ¿Qué son las criptomonedas?



CLOUD COMPUTING



Blockchain 3.0

*Applications*

"Beyond currency, finance, and markets"

Blockchain 2.0

*Contracts and Identities*

"The entire slate of economic, market, and financial applications using the blockchain that are more extensive than simple cash transactions"

Blockchain 1.0

*Bitcoin and other Crypto Currencies*

"The deployment of cryptocurrencies"



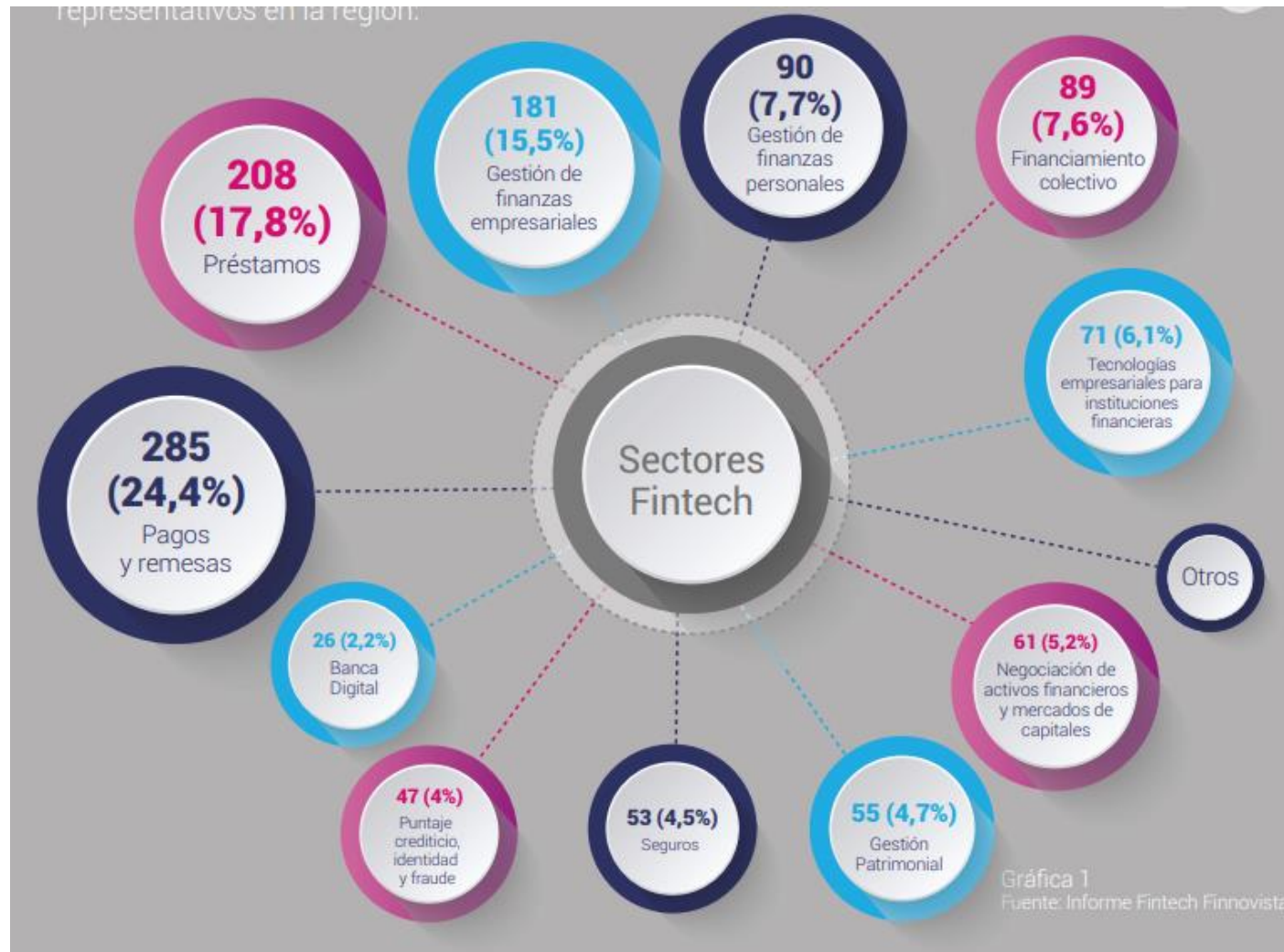


**Fintech**  
**Regtech**  
**Legaltech**  
**Insurtech**

# Ecosistema Fintech



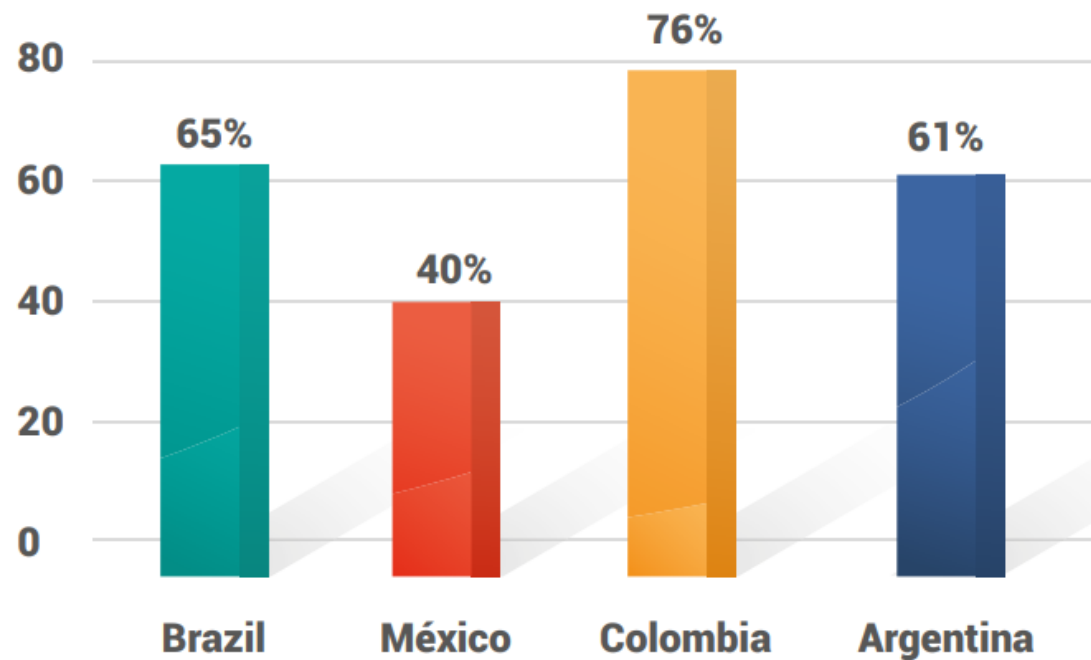
# Entorno de las Fintech - Latinoamérica



**Fuente:** Informe Vodanovic Legal 2018, actualizado junio 2019. *El panorama de la industria Fintech en Perú.*

# Entorno de las Fintech - Latinoamérica

## NIVEL DE CRECIMIENTO DE LOS PRINCIPALES MERCADOS FINTECH EN LATINOAMÉRICA



**4**

de los principales mercados Fintech en Latinoamérica han experimentado un crecimiento superior al 40% entre 2017 y 2018.

Source: Fintech in Latin America 2018: growth and Consolidation (Finnovista & IDB)

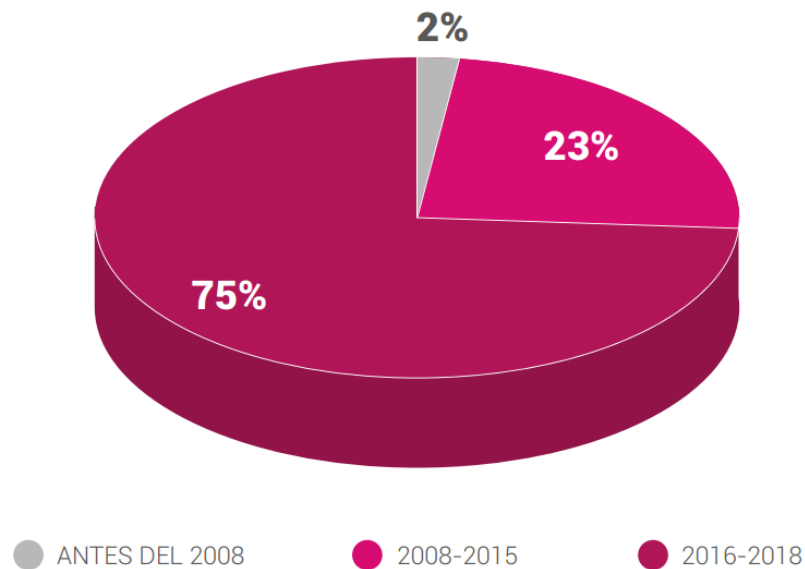
Fuente: Informe Vodanovic Legal 2018, actualizado junio 2019. *El panorama de la industria Fintech en Perú.*



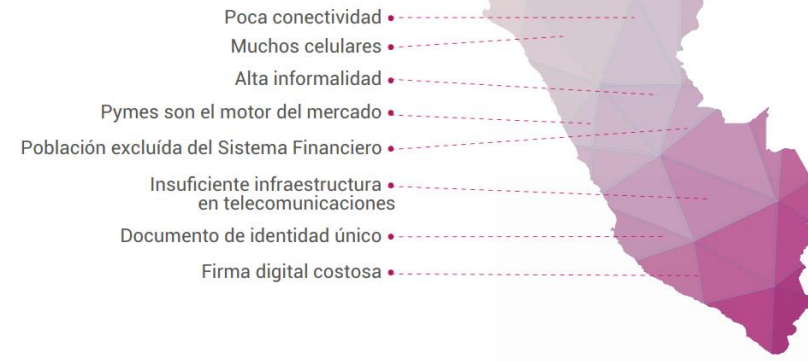


# Entorno de las Fintech - Perú

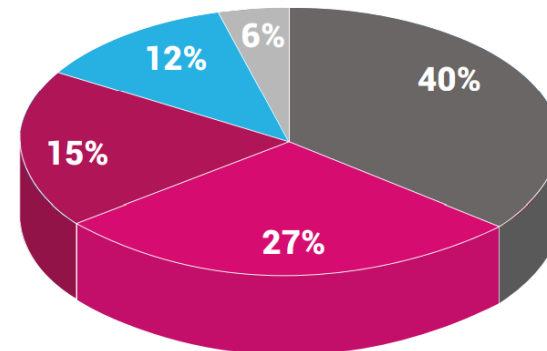
¿En qué años se fundaron las Fintech peruanas?



a. Infraestructura de mercado:



¿En qué etapa se encuentran las Fintech en Perú?

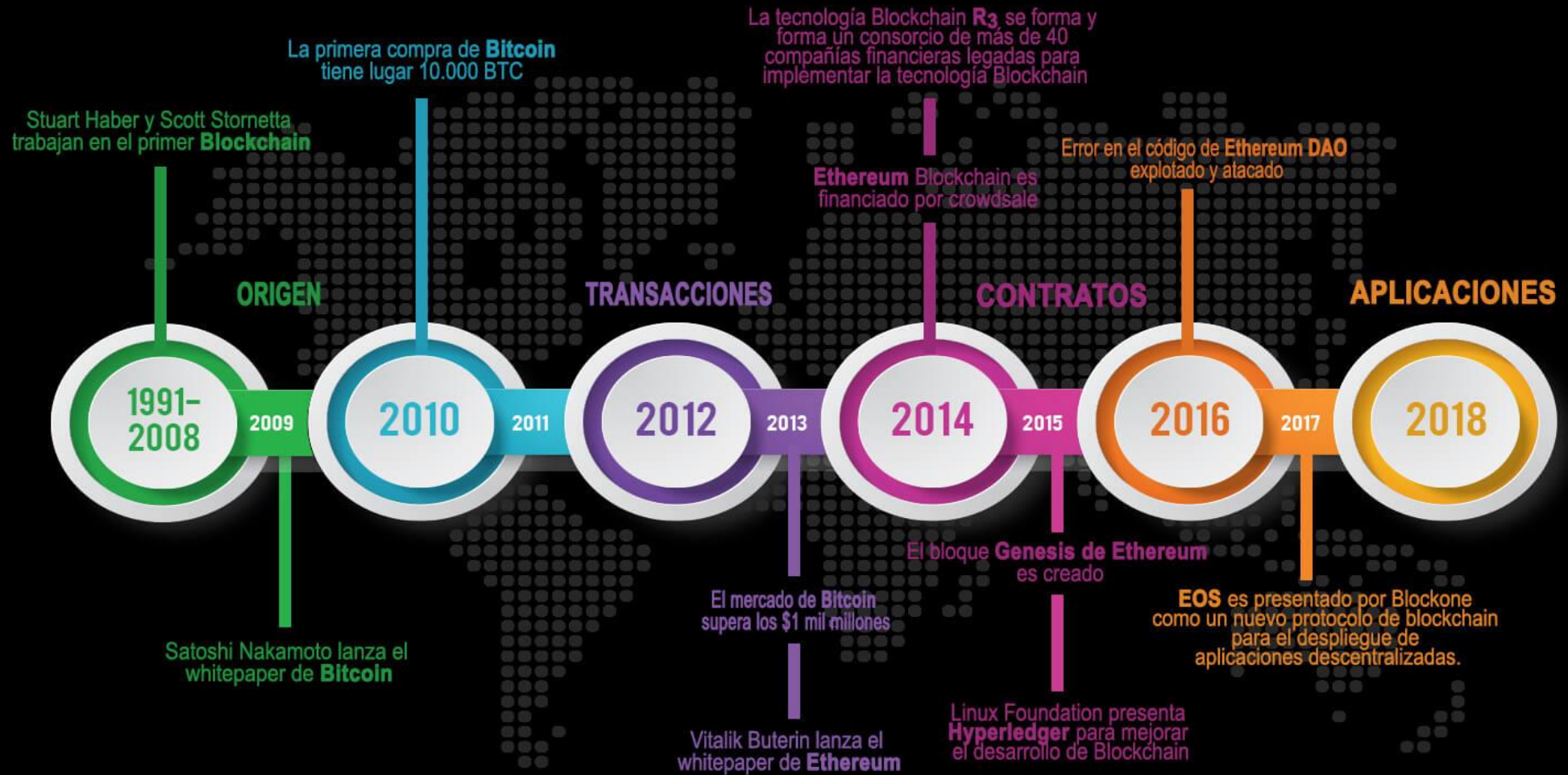


# Entorno de las Fintech - Perú

\* Principales obstáculos percibidos por los inversionistas:



# LA HISTORIA DE LA TECNOLOGÍA BLOCKCHAIN





# Bitcoin: Octubre de 2008 – Satoshi Nakamoto

## Bitcoin: A Peer-to-Peer Electronic Cash System

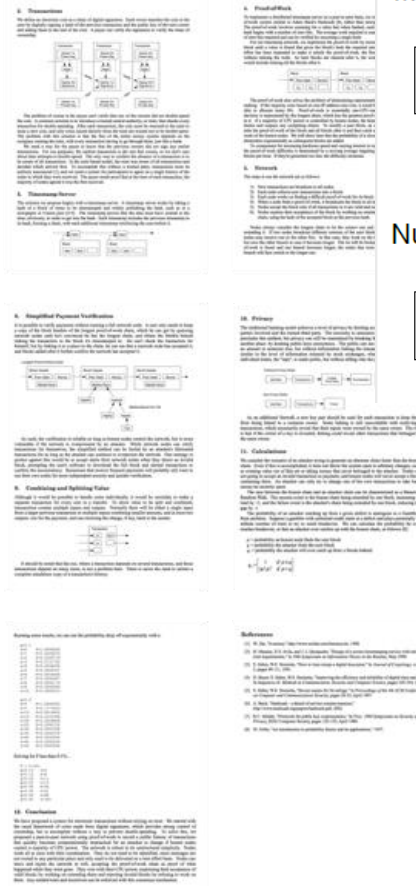
Satoshi Nakamoto  
satoshi@gmx.com  
www.bitcoin.org

**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.

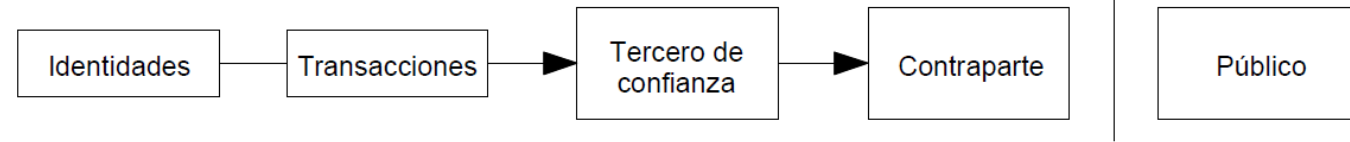
### 1. Introduction

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.

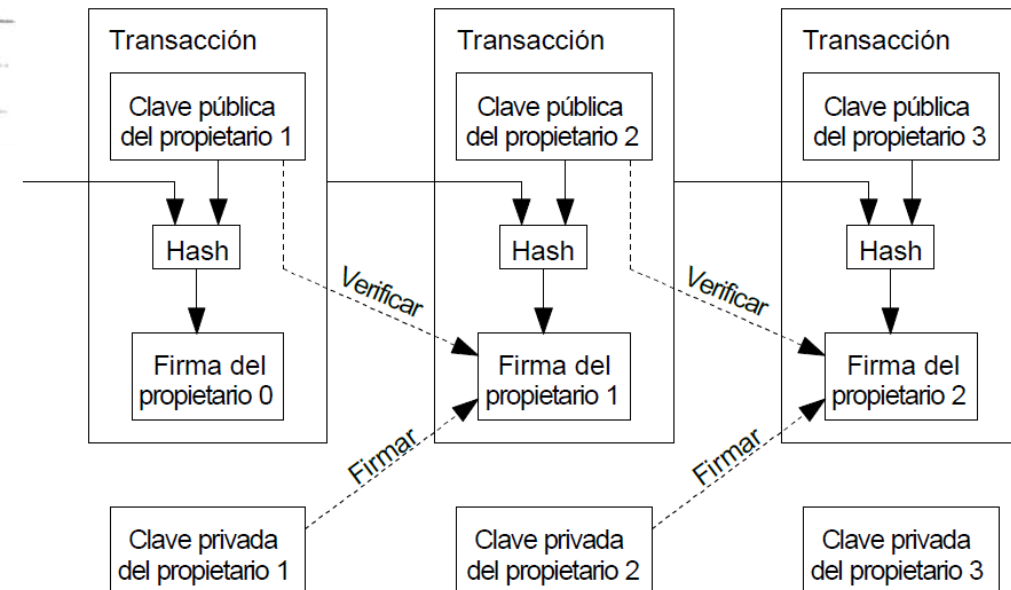
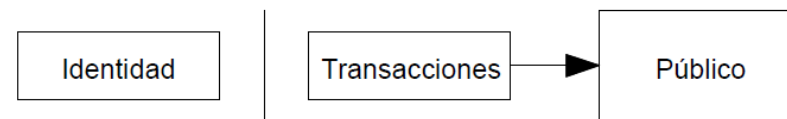
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, 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.



### Modelo tradicional de privacidad



### Nuevo modelo de privacidad



**Bitcoin: A Peer-to-Peer Electronic Cash System**

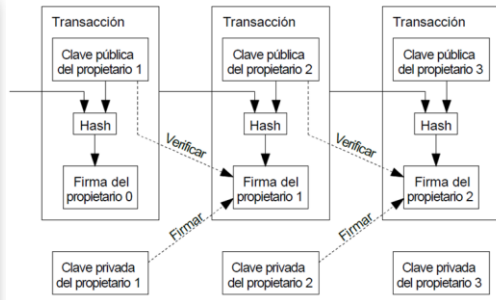
Satoshi Nakamoto  
satoshi@sigmas.com  
www.bitcoin.org

**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, handing them far 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 infeasible 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.



**2 + 2 = (?)**  
3bf7d3340c90ff62cd9a435f36ac1...



1. Problema –algoritmo (protocolo)
2. Registro de operaciones – libro contable (*ledger*)
3. Consenso del resultado (validación)
4. Base de datos distribuida y descentralizada
5. Verificación (aceptada o rechazada)
6. Protección ( firma digital y hash criptográfico)

**Bitcoin: A Peer-to-Peer Electronic Cash System**

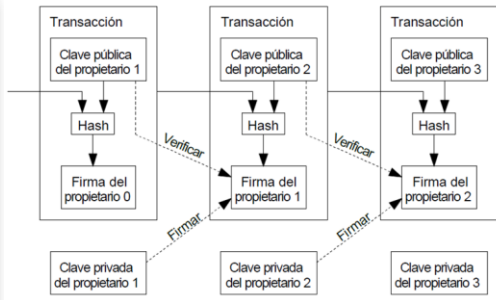
Satoshi Nakamoto  
satoshi@sigm.com  
www.bitcoin.org

**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 overpower 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, handing them far 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 infeasible 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.



4 ✓



4 ✓



4 ✓



4 ✓



3 ✗

**2 + 2 = (?)**

**3bf7d3340c90ff62cd9a435f36ac11d549a37744**

1. Problema –algoritmo (protocolo)
2. Registro de operaciones – libro contable (*ledger*)
3. Consenso del resultado (validación)
4. Base de datos distribuida y descentralizada
5. Verificación (aceptada o rechazada)
6. Protección ( firma digital y hash criptográfico)

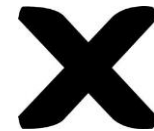


$2 + 2 = (4)$  ✓

3bf7d3340c90ff62cd9a435f36ac11d549a37744a9acc138271



3



1. Problema – algoritmo (protocolo)
2. Registro de operaciones – libro abierto
3. Consenso del resultado
4. Base de datos distribuida y descentralizada
5. Validación de operaciones (aceptada o rechazada)
6. Copia de la base de datos (descentralización)
7. Protección (criptografía)

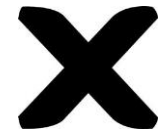




1. Problema – algoritmo (protocolo)
2. Registro de operaciones – libro abierto
3. Consenso del resultado
4. Base de datos distribuida y descentralizada
5. Validación de operaciones (aceptada o rechazada)
6. Copia de la base de datos (descentralización)
7. Protección (criptografía)



3

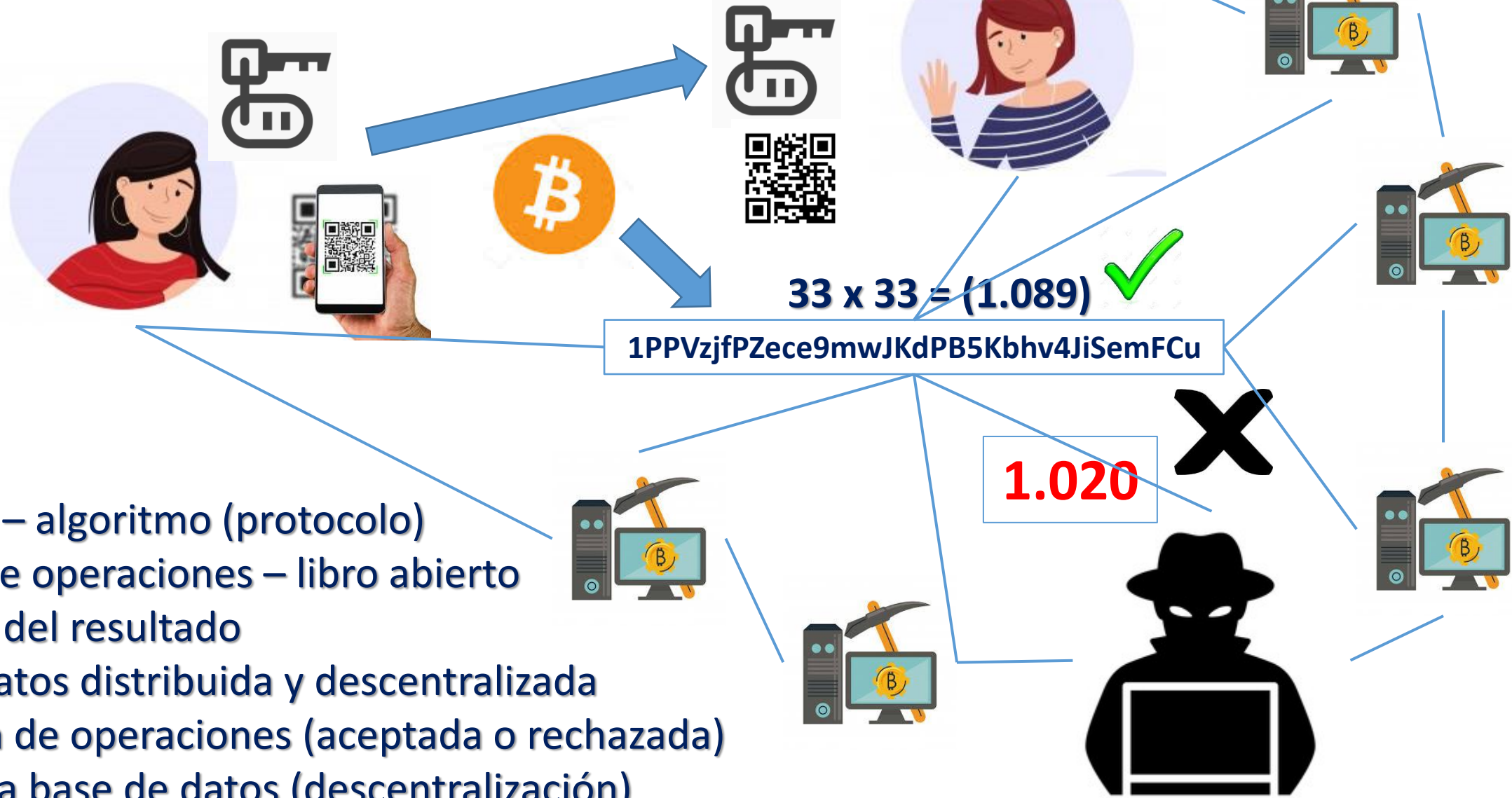




1PPVzjfPZece9mwJKdPB5Kbhv4JiSemFCu

$33 \times 33 = (?)$

1. Problema – algoritmo (protocolo)
2. Registro de operaciones – libro abierto
3. Consenso del resultado
4. Base de datos distribuida y descentralizada
5. Validación de operaciones (aceptada o rechazada)
6. Copia de la base de datos (descentralización)
7. Protección (criptografía)



1. Problema – algoritmo (protocolo)
2. Registro de operaciones – libro abierto
3. Consenso del resultado
4. Base de datos distribuida y descentralizada
5. Validación de operaciones (aceptada o rechazada)
6. Copia de la base de datos (descentralización)
7. Protección (criptografía)

**Bitcoin: A Peer-to-Peer Electronic Cash System**

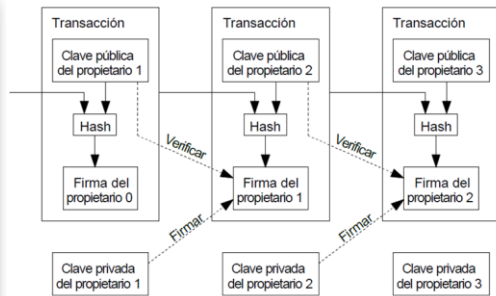
Satoshi Nakamoto  
satoshi@bitcointalk.org  
www.bitcoin.org

**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.

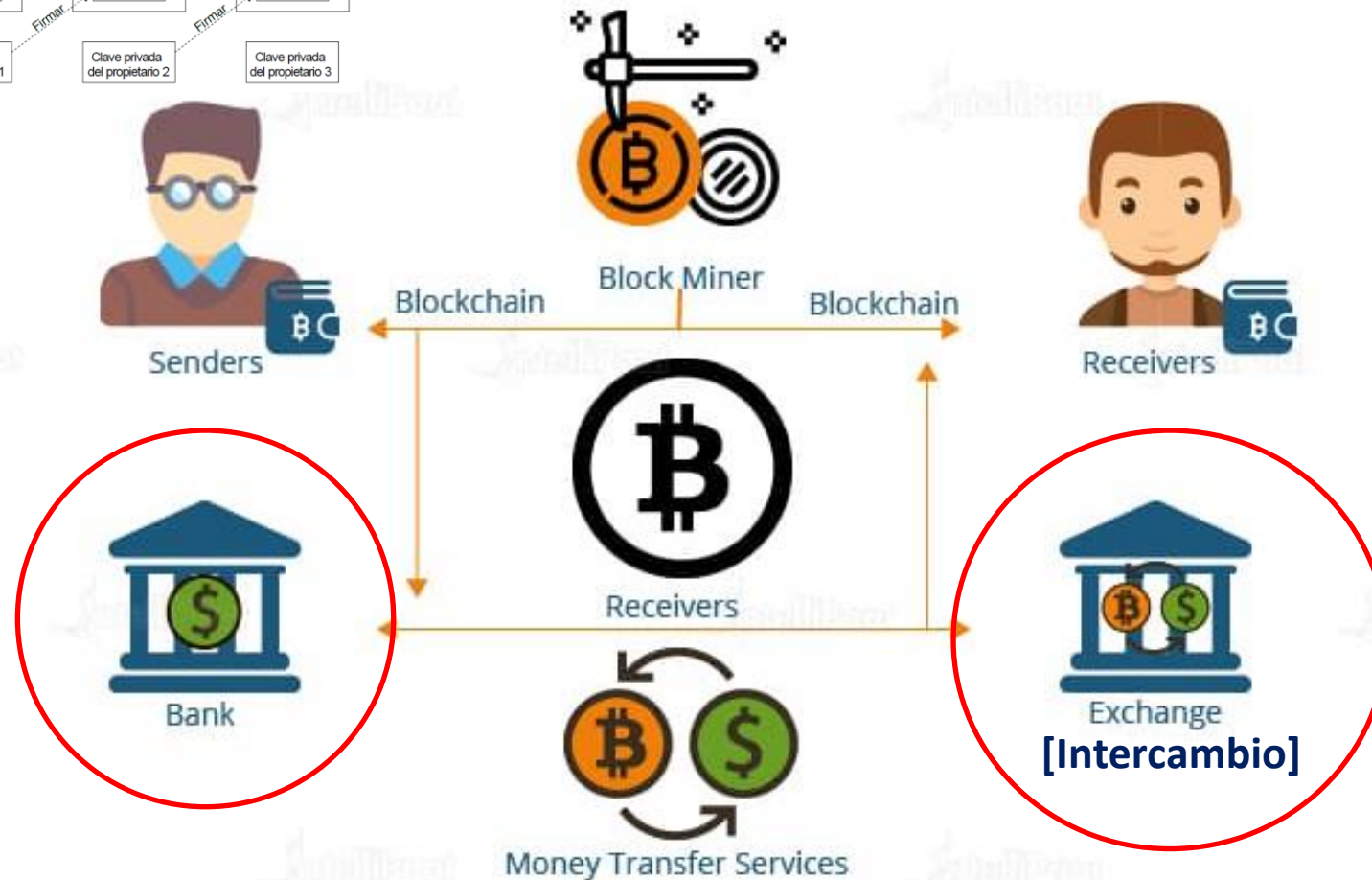
**1. Introduction**

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, handing them far 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.



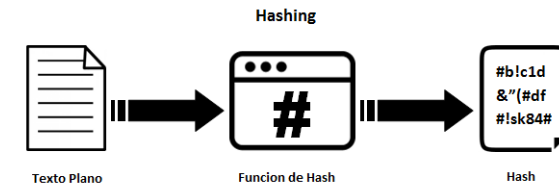
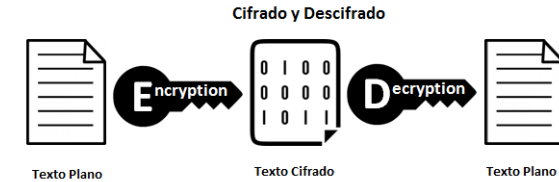
# Bitcoin funciona así:



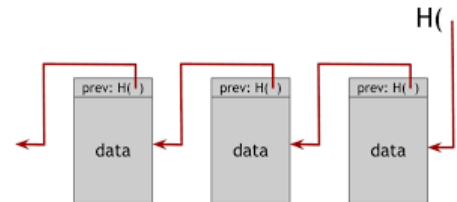


# Principales características [Blockchain]

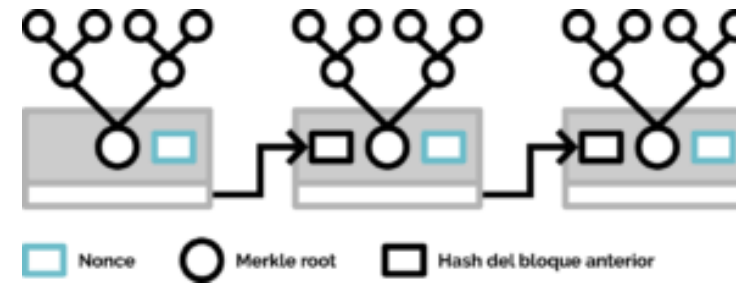
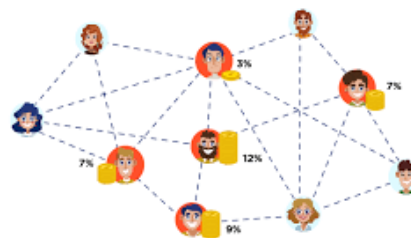
## 01. Seguridad - Criptografía



## 02. Cadena de Bloques

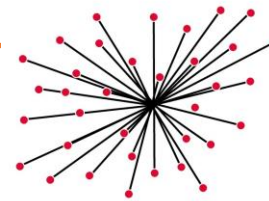


## 03. Consenso

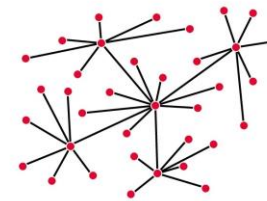


# Principales características [Blockchain]

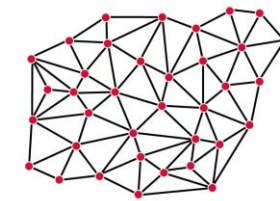
## 04. Descentralización



Centralizado



Descentralizado

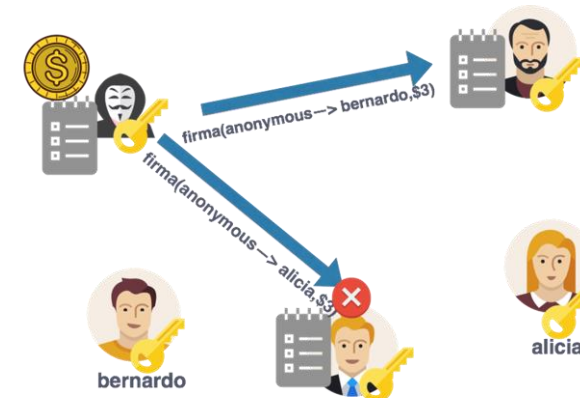


Distribuido

## 05. Validación en línea



## 06. Pseudo-anonimato



## 07. Transparencia

BLOCKCHAIN.COM Products Data Explorador Inicio de sesión Registrarse

BLOCKCHAIN THE #1 High-speed crypto trading built by the pros at blockchain.com Check it out

Explorador de bloques

Bitcoin 8724.11 USD

Últimos bloques

Bloques	Alte	Hash	Minuto	Mining	Tamaño
613763	0...e9632296c14a73a63a5a04633649527aa9f9187...		17 minutos	F2Pool	1,027,400 bytes
613762	0...8e9f756c4c5f3c3a3d08912b3c08f91278bdca...		28 minutos	BTC.com	38,332 bytes
613761	0...c30a05b20224ac0d0e0e433a380e79a0b3d...		28 minutos	Unknown	578,036 bytes
613760	0...af08f75a9e448c33342c01948810fe0b03ab...		32 minutos	AntPool	918,053 bytes
613759	0...6861e5e4433ac82097230e3a421d05864577a...		33 minutos	AntPool	1,235,691 bytes

# El Bitcoin, la moneda virtual

La e-moneda permite intercambiar o pagar a través de una red sin intermediarios en internet



  
 ↓  
  
 ↓  
**Bitcoins**  
  
 Creados en 2009 por Satoshi Nakamoto (seudónimo)

Máximo de  
**21 millones**   
 de bitcoins en el mundo  
  
 Un sistema **sin supervisión** de una autoridad monetaria  
  
 Una moneda de **gran volatilidad**



# A partir de Bitcoin...



...más de 5.580 Altcoins -criptomonedas y tokens-  
(junio 15 de 2020)



Cryptocurrencies: [5,583](#) • Markets: [22,646](#) • Market Cap: [\\$266,211,779,218](#) • 24h Vol: [\\$89,856,870,087](#) • BTC Dominance: [65.2%](#)











[Rankings](#) [Tools](#) [Resources](#) [Blog](#) [...](#)

[Se](#)

## Top 100 Cryptocurrencies by Market Capitalization

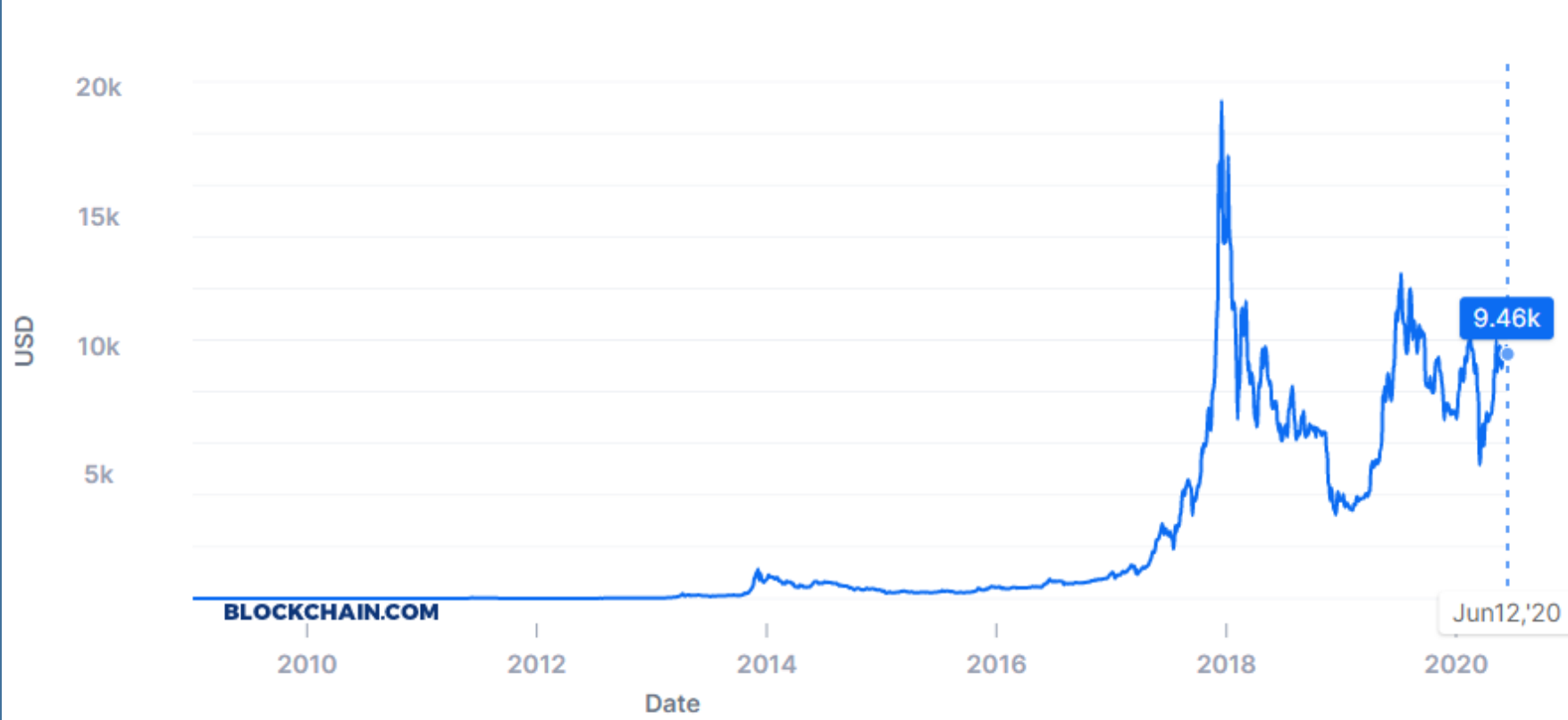
Cryptocurrencies ▾ [Exchanges](#) [Watchlist](#) [Filters](#) [USD ▾](#) [Next 100 →](#) [View All](#)

Rank	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 <b>Bitcoin</b>	\$173,630,605,134	\$9,433.43	\$26,657,015,843	18,405,887 BTC	0.68%	
2	 <b>Ethereum</b>	\$25,618,736,379	\$230.04	\$10,354,295,607	111,366,269 ETH	-1.21%	
3	 <b>Tether</b>	\$9,205,927,707	\$1.00	\$32,866,604,802	9,187,991,663 USDT *	-0.50%	
4	 <b>XRP</b>	\$8,443,786,715	\$0.190786	\$1,313,154,721	44,257,803,618 XRP *	-0.29%	



# Precio de mercado

Precio medio de mercado en USD a través de intercambios importantes de bitcoins.



**USD 9.463,43 BTC (Jun. 15 2020)**

30 días | 60 días | 180 días | 1 año | 3 años | **Todos**

**Valores brutos** | Promedio de 7 días | Promedio de 30 días

**Escala lineal** | Escala Logarítmica

Export Data ▼



## Top 10 Leaderboard

USD ▾

NAME	PRICE	24H CHG
BTC	\$9,411.67	▲ 1.67%
ETH	\$229.88	▲ 0.30%
XRP	\$0.19	▲ 2.29%
LINK	\$3.91	▲ 2.14%
BCH	\$235.57	▲ 0.46%
USDT	\$1.00	▲ 0.09%
LTC	\$43.59	▲ 0.46%
CRO	\$0.11	▼ -0.68%

HVN SCROLL FOR MORE -0.76%

### BITCOIN PRICE

\$9,411.67

▲ 1.67%

MKT CAP  
\$173.23B

CIRC SPLY  
18,405,900 BTC

24H VOL  
\$3.98B

24H HIGH/LOW  
\$9,505.54 / \$8,903.53

1HR 1D 1W 1M 1Y

CHART TYPE





# Total de circulación de Bitcoin

El número total de bitcoin minados que circulan actualmente en la red.



## Bitcoin Rich List



Share:     

### Bitcoin distribution

Balance, BTC	Addresses	% Addresses (Total)	Coins	\$USD	% Coins (Total)
(0 - 0.001)	14532446	48.04% (100%)	2,873 BTC	27,033,333 USD	0.02% (100%)
[0.001 - 0.01)	7307379	24.16% (51.96%)	29,458 BTC	277,141,270 USD	0.16% (99.98%)
[0.01 - 0.1)	5347872	17.68% (27.8%)	173,243 BTC	1,629,891,689 USD	0.94% (99.82%)
[0.1 - 1)	2244204	7.42% (10.12%)	711,924 BTC	6,697,856,452 USD	3.87% (98.88%)
[1 - 10)	663939	2.19% (2.7%)	1,729,106 BTC	16,267,604,860 USD	9.4% (95.01%)
[10 - 100)	138067	0.46% (0.51%)	4,456,974 BTC	41,931,665,085 USD	24.22% (85.62%)
[100 - 1,000)	13946	0.05% (0.05%)	3,502,543 BTC	32,952,285,422 USD	19.03% (61.4%)
[1,000 - 10,000)	2049	0.01% (0.01%)	5,041,352 BTC	47,429,559,116 USD	27.39% (42.37%)
[10,000 - 100,000)	103	0% (0%)	2,398,260 BTC	22,563,072,772 USD	13.03% (14.97%)
[100,000 - 1,000,000)	2	0% (0%)	357,359 BTC	3,362,073,788 USD	1.94% (1.94%)

### Addresses richer than

1 USD	100 USD	1,000 USD	10,000 USD	100,000 USD	1,000,000 USD	10,000,000 USD
22,083,798	7,667,354	2,859,848	674,211	138,167	13,340	1,560

[Bitcoin UTXO | Top Dormant for 5 years Bitcoin Addresses](#)

### Top 100 Richest Bitcoin Addresses

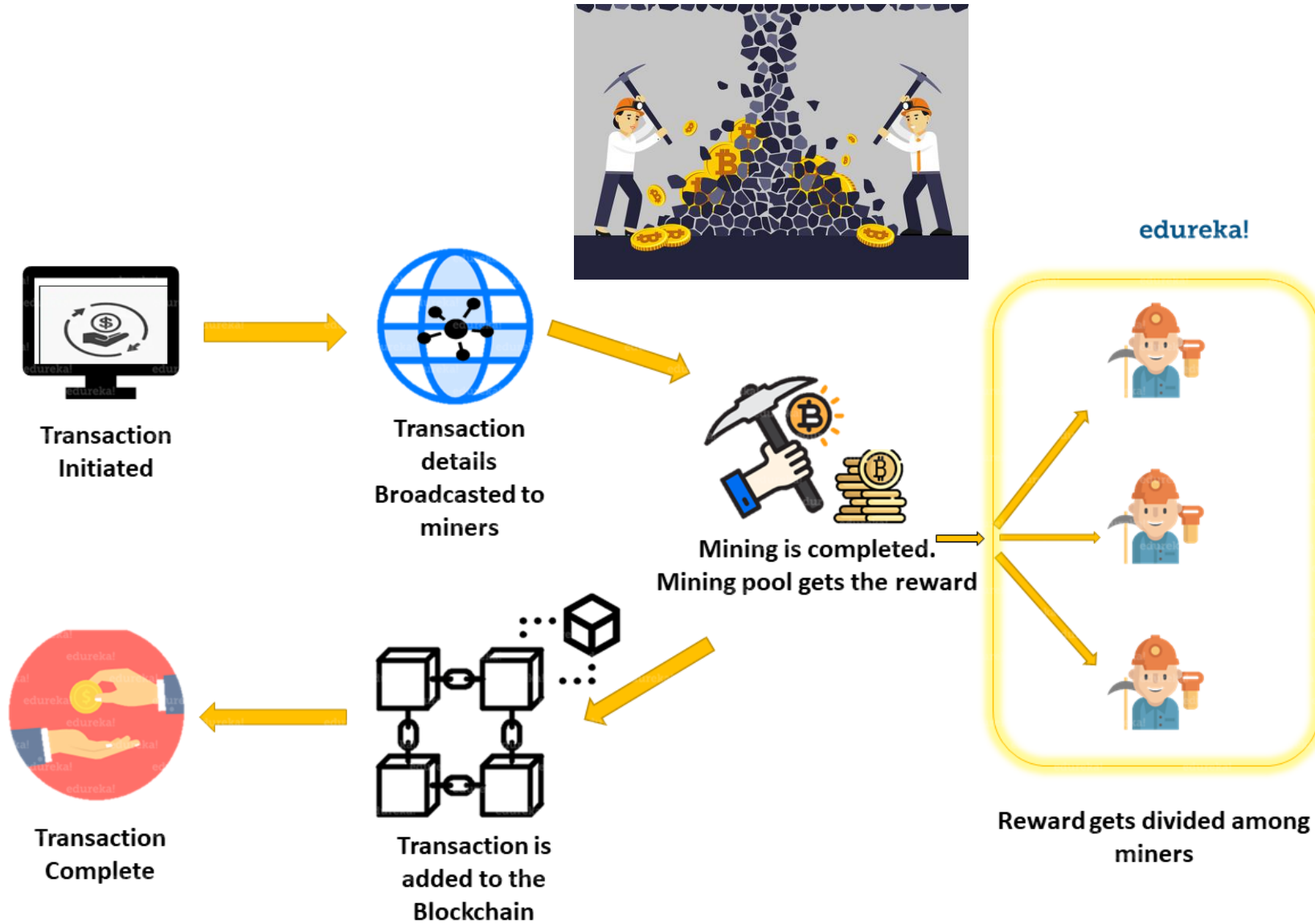
Address	Balance $\Delta 1w/\Delta 1m$	% of coins	First In	Last In	Number Of Ins	First Out	Last Out	Number Of Outs
1 <a href="#">35hK24tcLEWcgNA4JxpvbkNkoAcDGqQPSP</a> <sup>3-of-7</sup> wallet: Huobi-coldwallet	255,502 BTC (\$2,403,790,399 USD)	1.39%	2019-01-25 04:43:53	2020-06-12 04:50:12	364	2019-01-25 04:58:54	2020-05-25 03:18:56	13
2 <a href="#">3KZ526NxCVXbKwwP66RgM3pte6zW4gY1tD</a>	101,857 BTC (\$958,283,389 USD)	0.5534%	2020-04-01 13:55:54	2020-05-04 14:06:08	10			
3 <a href="#">37XuVSEpWW4trkfmvWzegTHQt7BdktSKUs</a>	94,506 BTC (\$889,119,962 USD)	0.5135%	2019-09-05 22:30:05	2020-06-07 11:33:54	58			
4 <a href="#">37do5d3pKeCuozjNCApGT153GJ8oNmKYbB</a>	88,990 BTC (\$837,222,939 USD)	0.4835%	2020-04-29 14:07:22	2020-06-11 13:13:12	5			
5 <a href="#">1FeexV6bAHb8ybZjqQMjJrcCrHGw9sb6uF</a>	79,957 BTC (\$752,245,538 USD)	0.4344%	2011-03-01 05:26:19	2020-05-21 17:04:15	328			
6 <a href="#">3NnGcxybgm3drht65hRucr23Ya4ZmQqz4w</a>	76,125 BTC (\$716,189,079 USD)	0.4136%	2020-03-19 22:45:16	2020-05-08 16:42:02	8			
7 <a href="#">3D8qAoMkZ8F1b42btt2Mn5TyN7sWfa434A</a> <sup>3-of-7</sup>	70,000 BTC (\$658,567,197 USD)	0.3803%	2019-09-27 02:26:31	2020-05-30 15:37:50	186	2019-10-10 22:51:24	2020-05-25 05:39:31	23
8 <a href="#">1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx</a>	69,370 BTC (\$652,642,120 USD)	0.3769%	2013-04-09 16:03:36	2020-06-13 13:46:12	196	2015-04-23 09:10:25	2015-04-23 09:10:25	1
9 <a href="#">385cR5DM96n1HvBDMzLHPYcw89fZAXULJP</a> wallet: Bittrex-coldwallet	61,302 BTC (\$576,734,539 USD)	0.3331%	2018-12-20 20:16:25	2020-04-21 16:13:33	84	2019-01-09 17:58:55	2020-02-20 15:38:19	49
10 <a href="#">bc1qqdjv0av3q56jvd82tkdjpy7gdp9ut8tlqmgrpmv24sq90ecnvqqjww97</a> wallet: Bitfinex-coldwallet	60,001 BTC (\$564,495,505 USD) <small>/-15000 BTC</small>	0.3260%	2019-08-16 05:00:29	2020-05-25 07:54:00	29	2020-02-02 12:43:14	2020-05-25 07:54:00	28
11 <a href="#">1P5ZEDWTKTFGxQjZphgWPQUpe554WKDFHQ</a>	55,482 BTC (\$521,977,091 USD) <small>/-897 BTC</small>	0.3014%	2019-02-05 21:18:39	2020-06-08 18:27:37	148	2019-02-10 16:58:57	2020-06-08 18:27:37	13

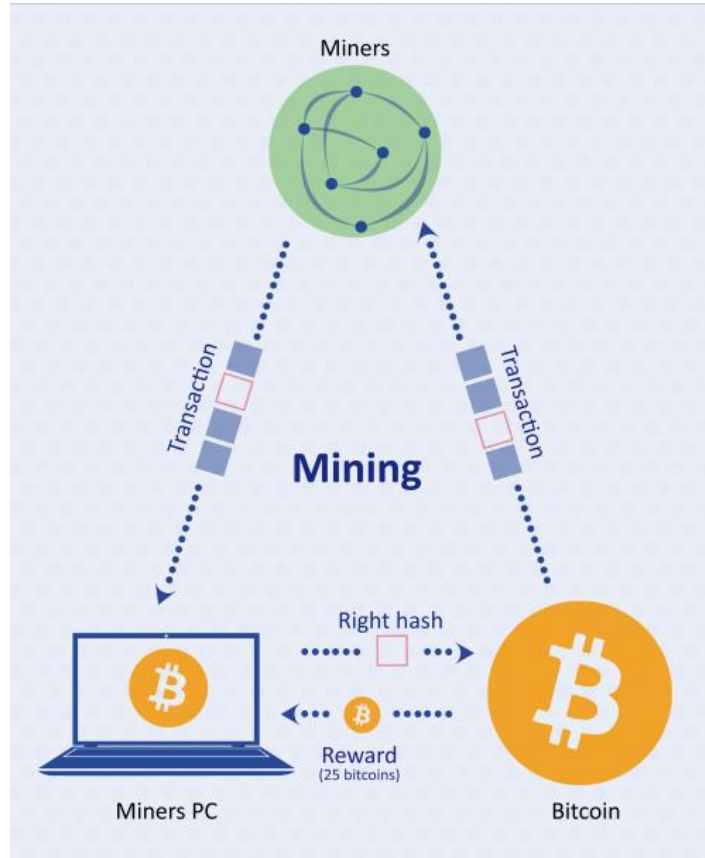




## ¿Qué es la minería?







Minero Bitcoin construido a partir de una tarjeta de video ATI Radeon



Minero Bitcoin construido a partir de tarjetas de video en paralelo



Minero Bitcoin construido a partir de (muchas) tarjetas de video



Granja de minería en Washington (Imagen de Coindesk)

## Información de Minería

Tarifa de hash total (TH/s)



El número estimado de terahashes por segundo en la red bitcoin se realiza en las últimas 24 horas.

Distribución de tasas de hash



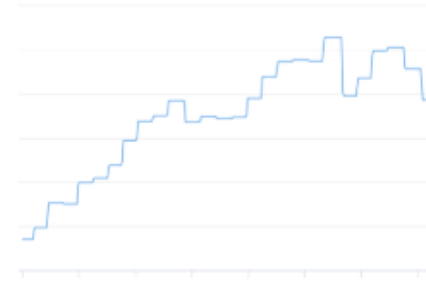
Una estimación de la distribución de las tasas de hash entre los pools de minería de mayor tamaño

Hashrate Distribution Over Time



An estimation of hashrate distribution over time amongst the largest mining pools

Dificultad de red



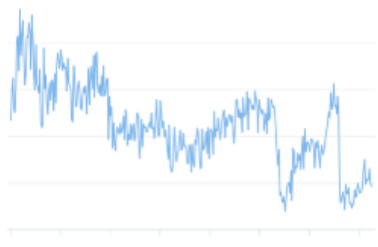
Una medida relativa de la dificultad de minar un nuevo bloque para blockchain.

Coste por transacción



Un gráfico que muestra los ingresos de los mineros divididos por el número de transacciones.

Beneficios de los Mineros (USD)



Valor total de recompensas del bloque de base de monedas y costos de transacción pagado a los mineros.

Comisiones totales de transacción (BTC)



El valor total en BTC de todas las comisiones de transacción pagadas a mineros. No incluye el valor de recompensas de bloque de base de monedas.

Comisiones totales de transacción (USD)



El valor total en USD de todas las comisiones de transacción pagadas a mineros. No incluye el valor de recompensas de bloque de base de monedas.

Comisiones por transacción (USD)



Comisiones promedio de transacción en USD por transacción.

Coste % del volumen de transacciones



Un gráfico que muestra los ingresos de los mineros como porcentaje del volumen de la transacción.



¿Cuáles son las criptomonedas más conocidas?



Cryptocurrencies: 5,583 • Markets: 22,646 • Market Cap: \$266,211,779,218 • 24h Vol: \$89,856,870,087 • BTC Dominance: 65.2%

**CoinMarketCap** Rankings Tools Resources Blog ...

**Top 100 Cryptocurrencies by Market Capitalization**

Rank	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	\$173,630,605,134	\$9,433.43	\$26,657,015,843	18,405,887 BTC	0.68%	
2	Ethereum	\$25,618,736,379	\$230.04	\$10,354,295,607	111,366,269 ETH	-1.21%	
3	Tether	\$9,205,927,707	\$1.00	\$32,866,604,802	9,187,991,663 USDT *	-0.50%	
4	XRP	\$8,443,786,715	\$0.190786	\$1,313,154,721	44,257,803,618 XRP *	-0.29%	



2009



**Litecoin**

2011



2012



2014



ethereum

2015



**BitcoinCash**

2017



2018



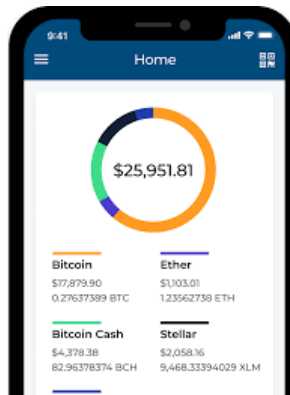
## ¿Cómo se almacenan las criptomonedas?

# Almacenamiento de Criptomonedas



**Hot Wallet**

**Cold Wallet**



**APP**



**WEB**



**USB**



**PAPEL**



¿Qué se puede hacer con las criptomonedas?



01. Guardar [riqueza]



02. Invertir [trading]

03. Usar – comprar [bs ss]



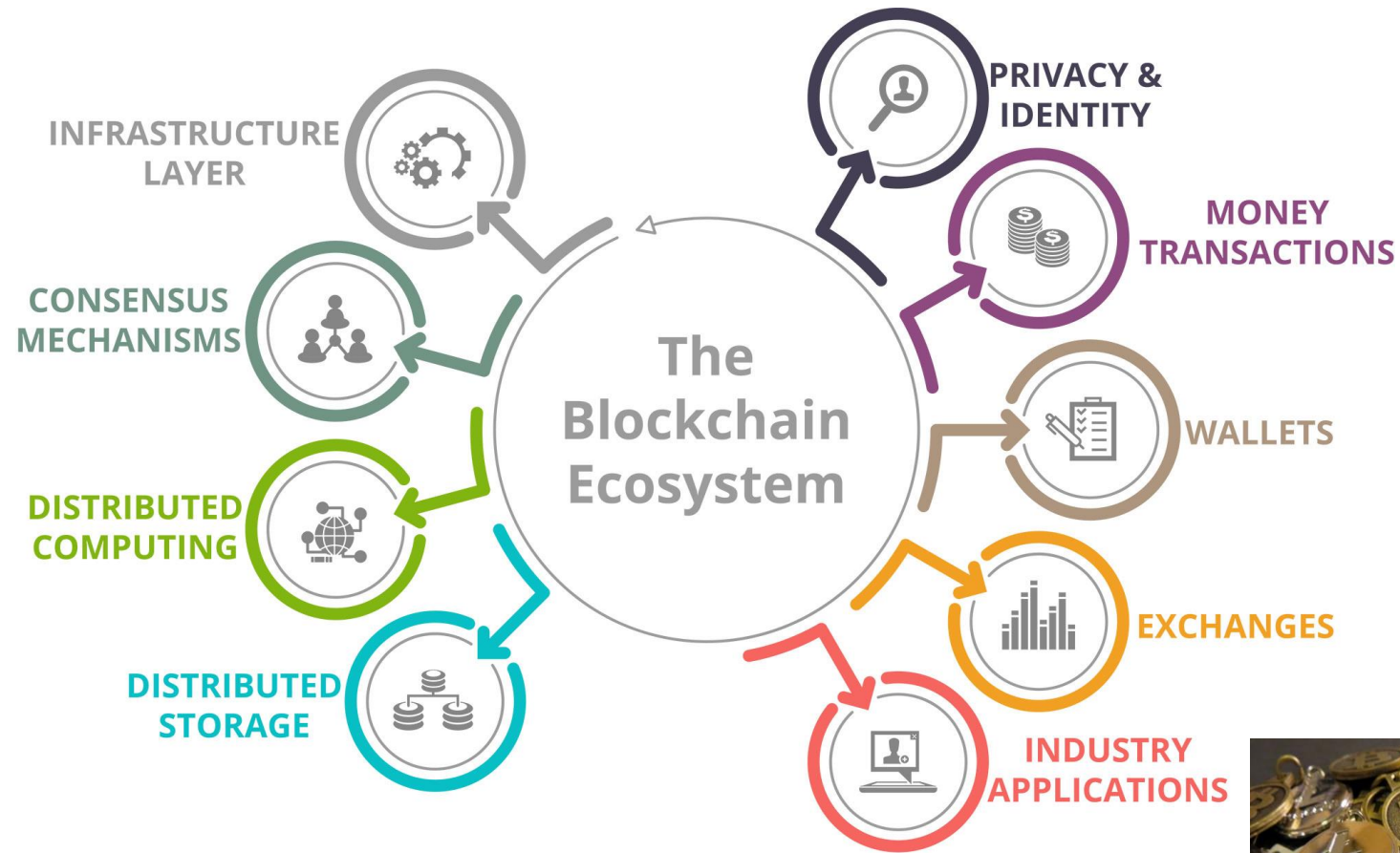
04. Transferir – pagar [pay]





¿Cómo funciona el ecosistema?

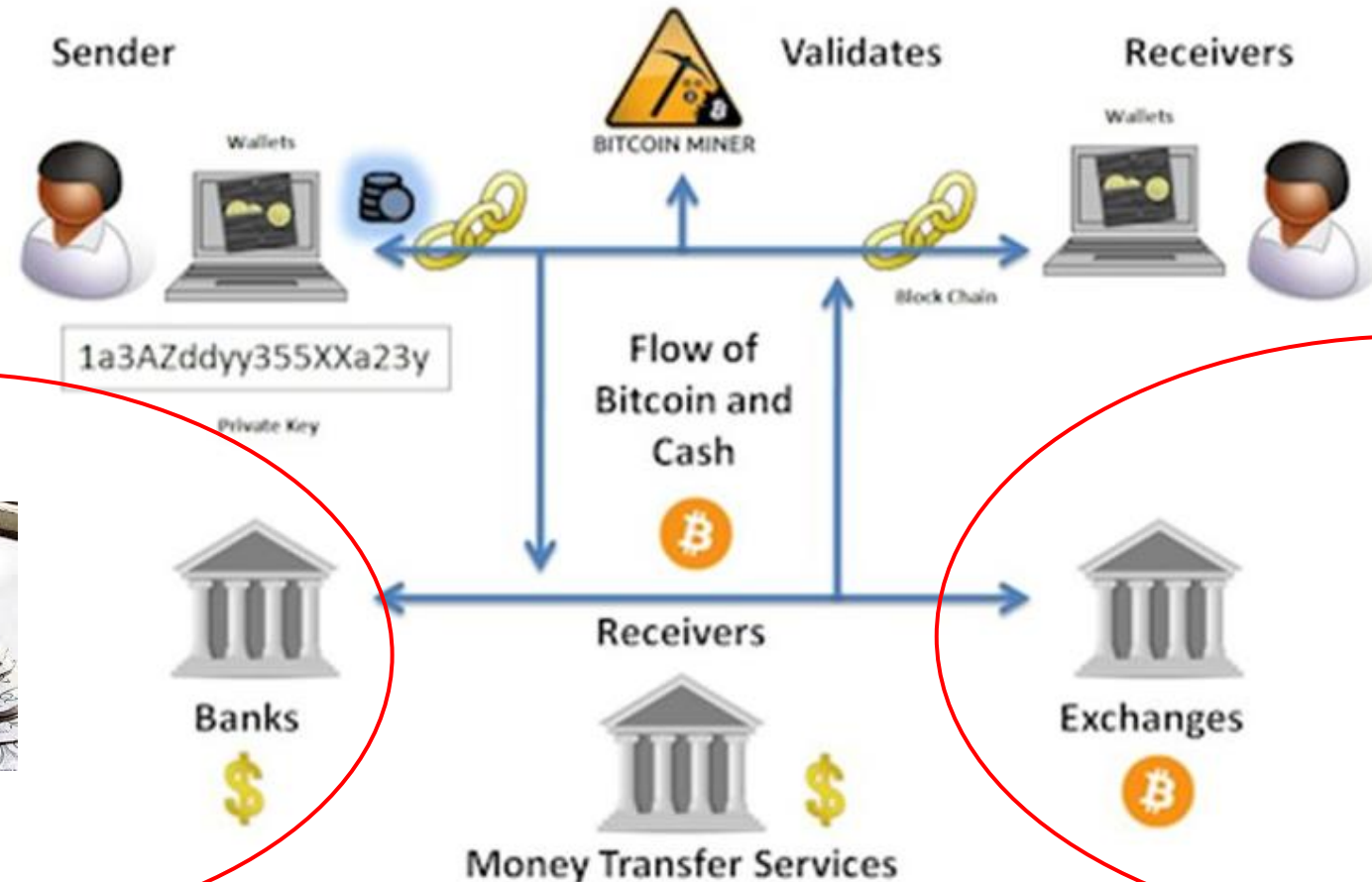
# Ecosistema de Blockchain



Mixer (Tumbler)



# Ecosistema de las Criptomonedas





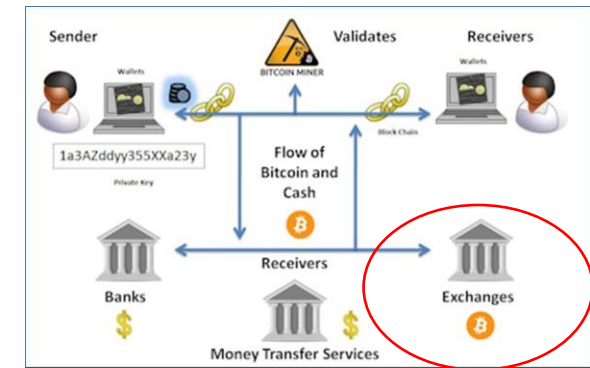
# Ecosistema de las Criptomonedas - Exchanges

## Top Cryptocurrency Exchanges

CoinMarketCap ranks the top cryptocurrency exchanges based on traffic, liquidity and trading volumes.

**314 Exchanges (Jun.15 2020)**

Rank	Name	Web Traffic Factor	Avg. Liquidity	Volume (24h)	No. Markets	Change (24h)	Vol. Graph (7d)	Laun
1	Binance	1000	434	\$6,635,373,651	598	105.38%		Jul
2	Huobi Global	752	507	\$6,444,447,594	551	130.40%		Sep
3	Coinbase Pro	972	418	\$389,366,855	65	89.80%		May
4	Kraken	856	357	\$346,261,562	155	192.59%		Jul
5	Bitfinex	781	424	\$163,403,854	274	109.14%		Oct
6	Bitstamp	729	270	\$191,205,283	25	179.39%		Jul
7	bitFlyer	746	150	\$86,412,160	5	141.69%		Jan
8	Bitbank	722	202	\$32,503,521	11	114.49%		May



# Ecosistema de las Criptomonedas - Localbitcoins

LocalBitcoins.com Buy bitcoins Sell bitcoins Post a trade Help ▾ ☑ Sign up free 👤 Log in

**QUICK BUY**   **QUICK SELL**

## Buy bitcoins online in Colombia

Seller	Payment method	Price / BTC	Limits	
erikah91 (100+; 100%) <span style="color: green;">●</span>	Transfers with specific bank: bancolombia	<b>33,899,000.00 COP</b>	300,000 - 8,575,981 COP	<input type="button" value="Buy"/>
DerCatala (15 000+; 100%) <span style="color: green;">●</span>	Transfers with specific bank: BANCOLOMBIA LIBERACION RAPIDA!	<b>33,950,000.00 COP</b>	1,000,000 - 18,000,000 COP	<input type="button" value="Buy"/>
DIOSCONTIGO (100+; 100%) <span style="color: green;">●</span>	Cash deposit: Bancolombia Rápido y SEGURO desde \$150.000♥	<b>33,950,000.00 COP</b>	150,000 - 15,000,000 COP	<input type="button" value="Buy"/>
Sernaventas (30+; 98%) <span style="color: grey;">●</span>	Transfers with specific bank: BANCOLOMBIA <input checked="" type="checkbox"/> CONFIABLE <input type="checkbox"/> LIBERO RÁPIDO <input type="checkbox"/> EN LINEA <input checked="" type="checkbox"/>	<b>33,950,000.00 COP</b>	100,000 - 3,000,000 COP	<input type="button" value="Buy"/>
clamar0831 (30+; 100%) <span style="color: grey;">●</span>	Transfers with specific bank: BANCOLOMBIA***CORRESPONSAL***APP***NEQUI	<b>34,000,000.00 COP</b>	200,000 - 3,188,755 COP	<input type="button" value="Buy"/>
andresint2 (70+; 100%) <span style="color: grey;">●</span>	Transfers with specific bank: Davivienda y Bancolombia	<b>34,000,569.69 COP</b>	100,000 - 30,822,087 COP	<input type="button" value="Buy"/>

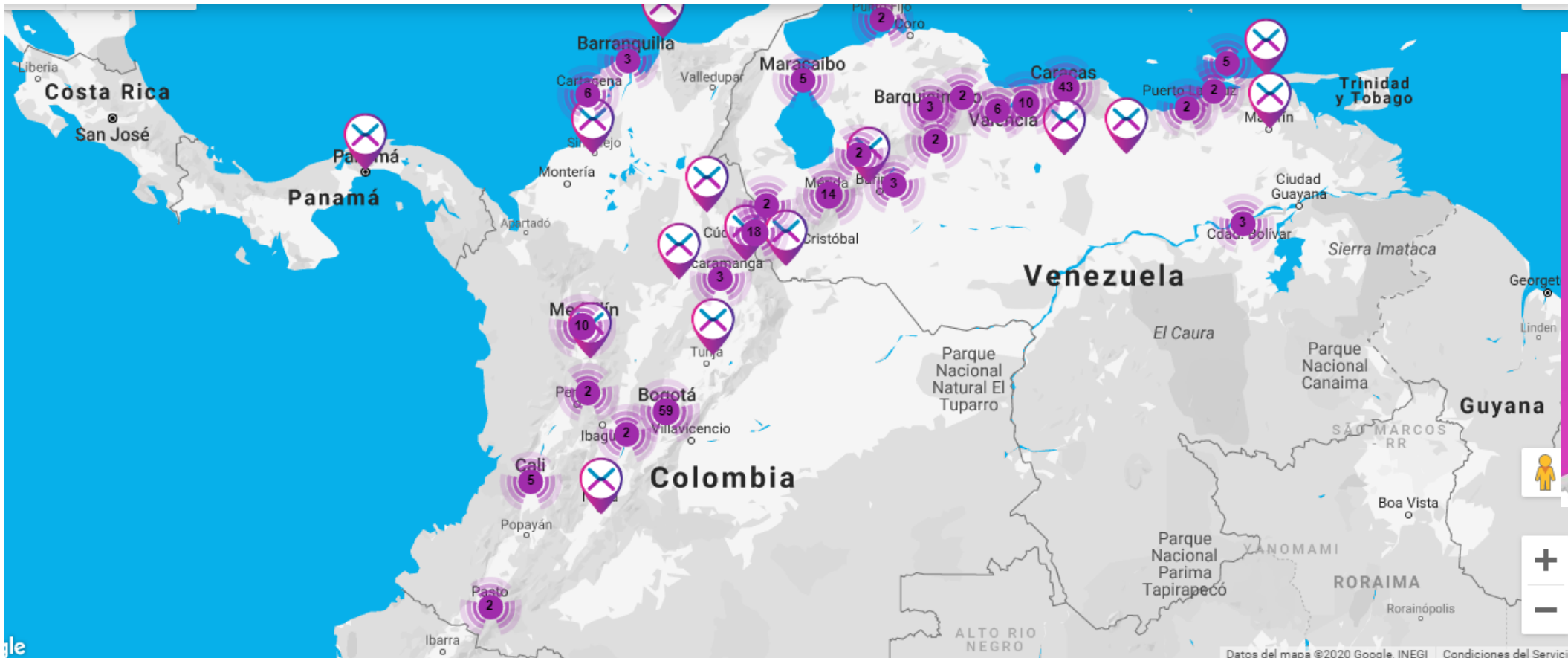
# Ecosistema de las Criptomonedas - BTMs



# Ecosistema de las Criptomonedas - Comercios

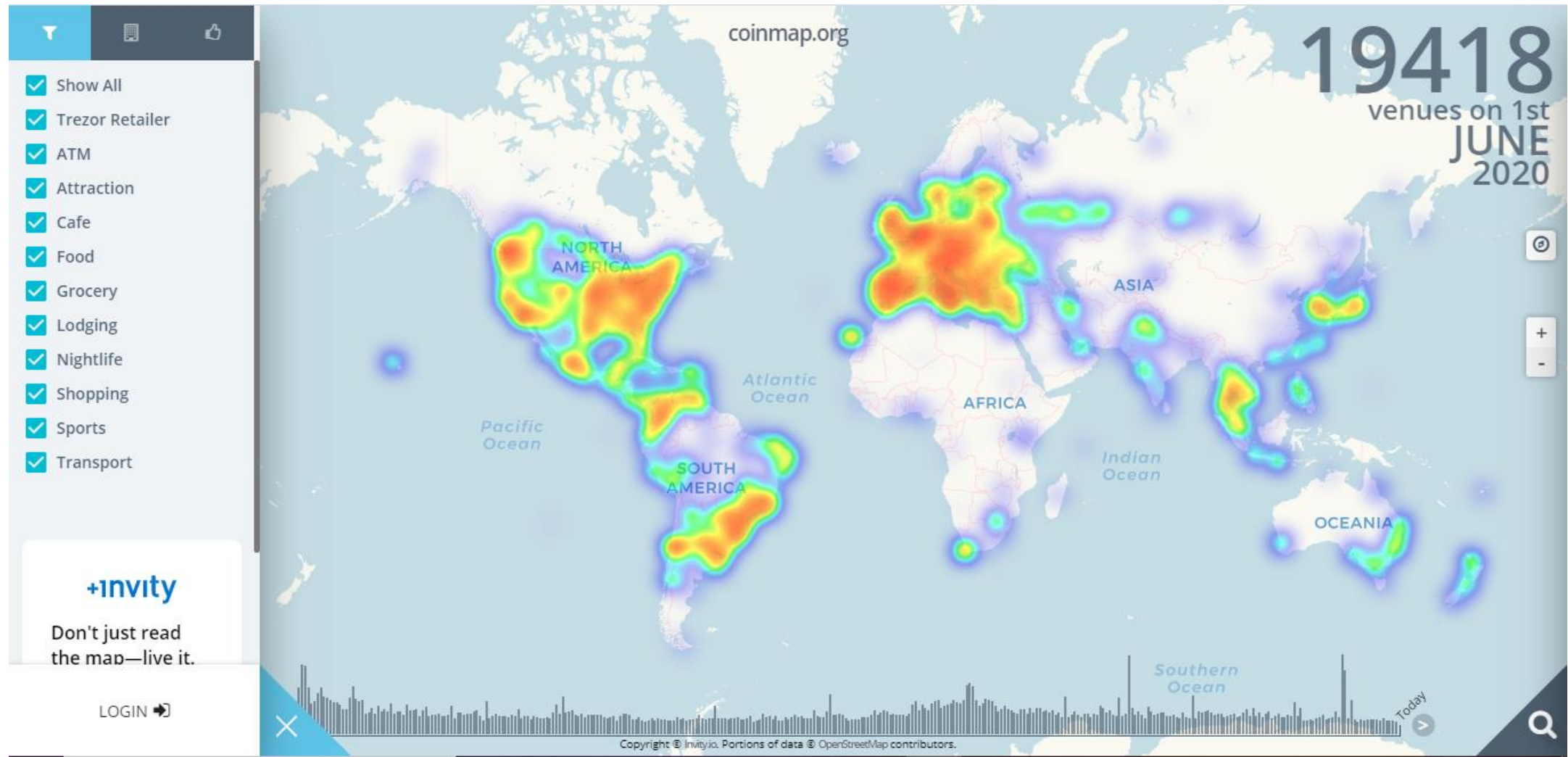
**XPAY**

- RECIBE PAGOS
- BILLETERA
- UBICACIONES
- BLOG
- DESARROLLADORES
- INGRESAR





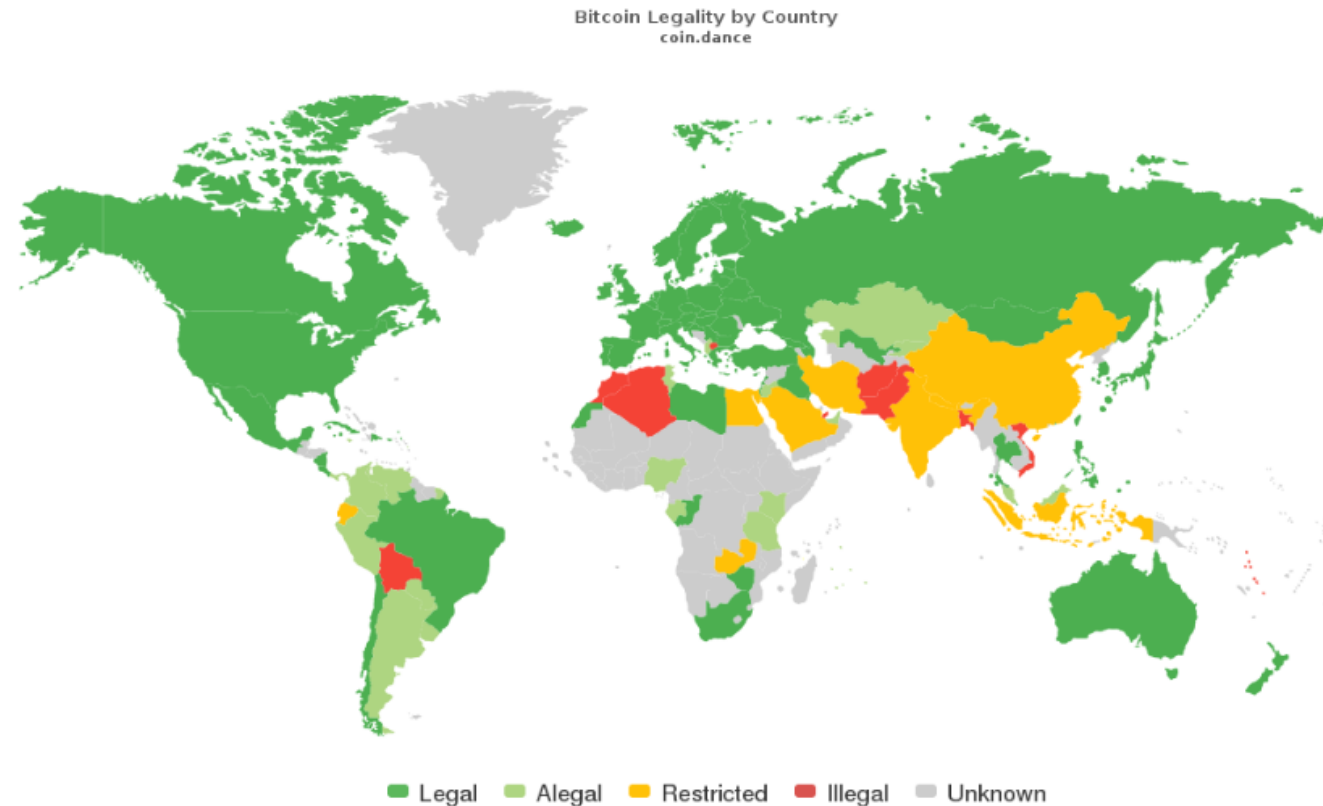
# Ecosistema de las Criptomonedas - Comercios





¿Las criptomonedas son legales o ilegales?

# ¿Legal, ilegal o alegal?





¿Cómo se pueden usar las criptomonedas para LA/FT?





## Virtual Assets

# *“wild west” of the finance industry*



The FATF's focus on virtual assets

How do the FATF Standards apply?

**Blockchain, bitcoin, crypto assets, virtual currencies...**a whole new vocabulary describing innovative technology to swiftly transfer value around the world. The fast-evolving blockchain and distributed ledger technologies have the potential to radically change the financial landscape. But, their speed, global reach and above all - anonymity - also attract those who want to escape authorities' scrutiny.

Blockchain originated just over 10 years ago. Since then, virtual assets have become widely available and have started to be used as payment products. However, without established regulation and oversight, the sector is often still referred to as the “wild west” of the finance industry.

Date	Meeting	FATF/FSRB/Other
08 June 2020	Virtual PDG Working Group meeting	FATF
10-11 June 2020	Virtual AGSR Meeting (Part II)	FATF
16 June 2020	Virtual ICRG Working Group meeting	FATF
18 June 2020	Virtual RTMG Working Group Meeting	FATF
19 June 2020	Virtual - 32nd Special EAG Plenary Meeting	EAG
24 June 2020	Virtual FATF Plenary	FATF
09-13 July 2020	Postponed - GAFILAT Plenary, Punta Cana, Dominican Republic	GAFILAT
15 August 2020	CFATF Council of Ministers, Miami, (dates & venue tbc)	CFATF
30 August-04 September 2020	ESAAMLG Task Force and Plenary meetings, Kampala, Uganda (location tbc)	ESAAMLG
01-02 September 2020	FATF Private Sector Consultative Forum (2-day event), UNODC Headquarters, Vienna (dates TBC)	FATF

# Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report

## EXECUTIVE SUMMARY

## MAJOR TRENDS AND DEVELOPMENTS

Proportion of Directly Illicit Funds Received by Exchanges Halves

LocalBitcoins Leads as Go-To for Direct Criminal Funds for Third Year in A Row

Cross-Border Exchanges Comprise Three Quarters of Exchange-to-Exchange Transfers

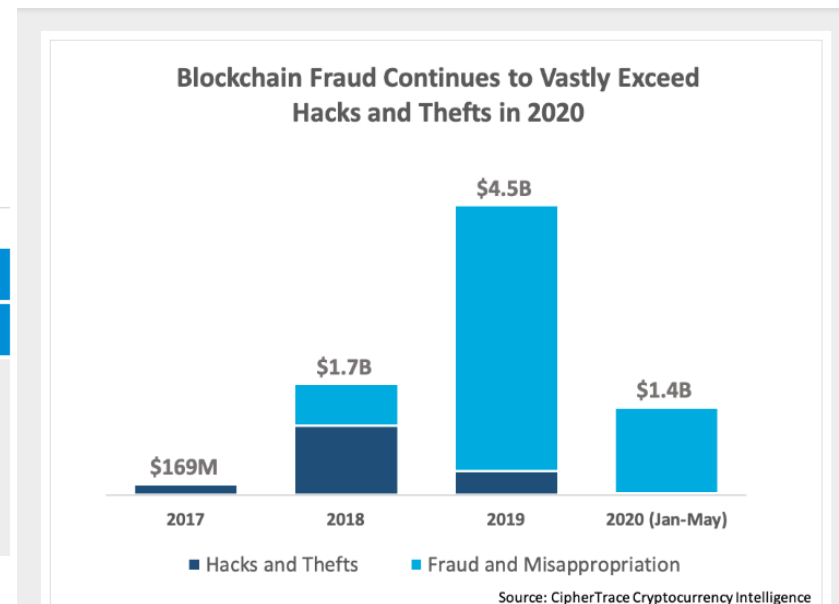
US Bitcoin ATM Users Increasingly Prefer High-Risk Exchanges

**Jun 2, 2020**

## Robos, piratas informáticos y fraude

En los primeros cinco meses de 2020, los robos de criptomonedas, los piratas informáticos y los fraudes suman USD 1,36 mil millones, lo que indica que 2020 podría ser el de mayor crypto delitos. En 2019 fue de USD 4,5 mil millones.

El fraude inspirado en el coronavirus se realiza a través de plataformas y salas de chat que exigen a sus víctimas el pago en bitcoin. Los sitios de phishing relacionados con COVID-19 son los más vendidos la web oscura.



## FATF focus on virtual assets

Virtual assets have many potential benefits. They could make payments easier, faster, and cheaper; and provide alternative methods for those without access to regular financial products. But without proper regulation, they risk becoming a virtual safe haven for the financial transactions of criminals and terrorists. The FATF has been closely monitoring the developments in the cryptosphere and in recent years has seen the first countries start to regulate the virtual asset sector, while others have prohibited virtual assets altogether. However, as yet, the majority of countries have not taken any action. These gaps in the global regulatory system have created significant loopholes for criminals and terrorists to abuse.

With support from the G20, the FATF has issued global, binding standards to prevent the misuse of virtual assets for money laundering and terrorist financing. The term 'virtual asset' refers to any digital representation of value that can be digitally traded, transferred or used for payment. It does not include the digital representation of fiat currencies.

The FATF standards ensure that virtual assets are treated fairly, applying the same safeguards as the financial sector. FATF's rules apply when virtual assets are exchanged for fiat currency, but also when they are transferred from one virtual asset to another.

- The FATF Standards: [FATF Recommendations](#)
- [FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#)

## Taking effective action

Countries need to implement the FATF's measures, and soon. This will ensure transparency of virtual asset transactions and keep funds wit

### Layering

Multiple transactions convert the payments from one virtual asset into another to remove all links to the crime.

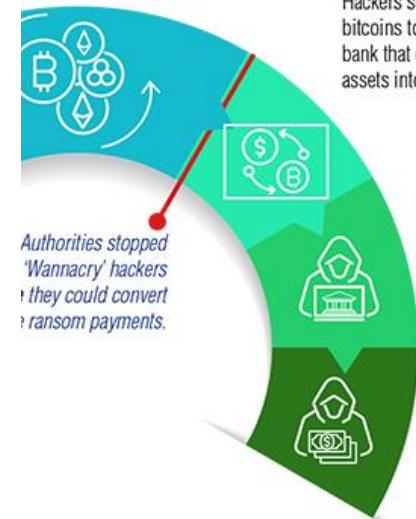
### Virtual Asset Service Provider

Hackers send the 'cleaned' bitcoins to a service provider or bank that converts the virtual assets into fiat money.

### Conversion into regulated currency

Hackers receive the bitcoins in the currency of their choice, ready to invest in a bank.

and spend.



Authorities stopped 'Wannacry' hackers they could convert to ransom payments.

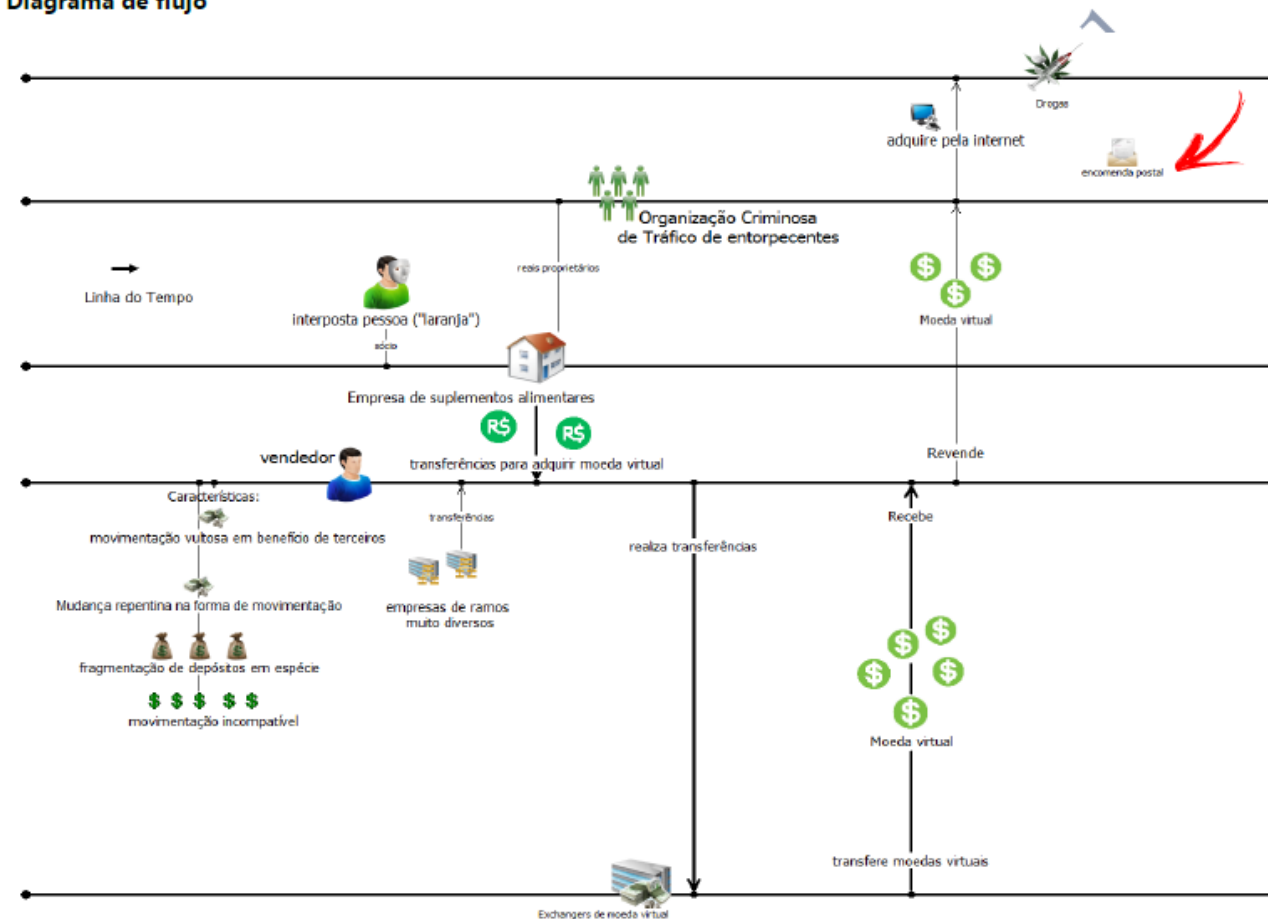
Had the hackers been successful, they would have received a fraction of the amount of damage they caused: **USD 100 million**

**"activo virtual"** se refiere a cualquier representación digital de valor que se pueda comercializar, transferir o usar digitalmente para el pago. Este no incluye la representación digital de monedas fiduciarias (fiat).

# Lavado de dinero proveniente del tráfico ilícito de drogas por medio de monedas virtuales



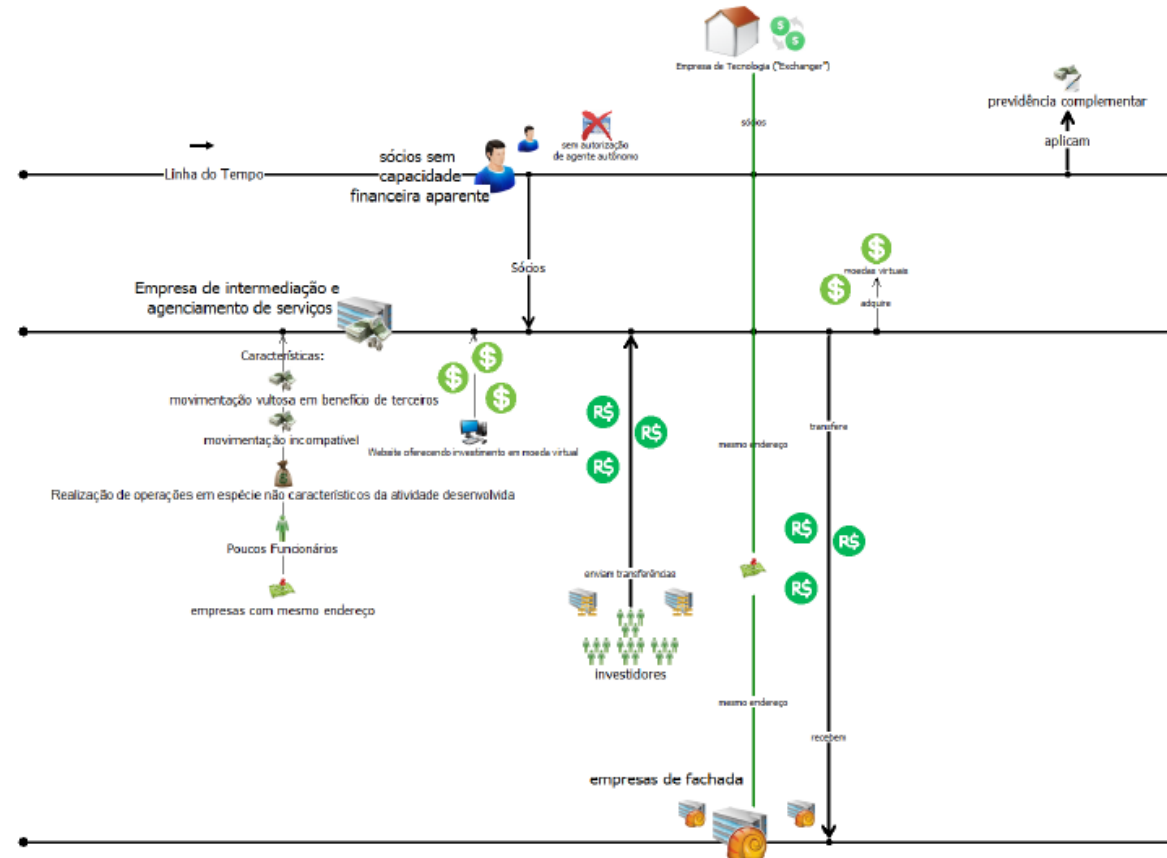
Diagrama de flujo





# Pirâmide Financiera (esquema Ponzi) basada en monedas virtuales

Diagrama de flujo



# Criptomonedas para actividades ilícitas

**Bitcoin SV entra en el Top 5 del trading de lavado, afirma un analista**

por Risk D. — Ene 17, 2020 @ 18:02 UTC — en Industria, Noticias, Noticias Afiliado, Noticias de Empresas



**Uso de criptomonedas para ocultar delitos**  
enero 20, 2020



El experto en prev lavado de activos y Explica que esta es recompensa o com la persecución del d

## Terroristas encuentran 'atajos' en las criptomonedas

- Los esquemas de financiamiento que usan los grupos terroristas son cada vez más sofisticados con el uso de este tipo de criptomonedas, como el bitcoin.

BLOOMBERG /OLGA KHARIF 20/01/2020



Por Daniel Jimenez 16 ENE 2020

**Chainalysis: USD 1.4 billones en Bitcoin fueron movidos por entidades criminales a Binance y Huobi en el 2019**

435 Vistas totales 7 Número total de compartidos

Un extracto del informe de Chainalysis sobre el Crísto (<https://es.cointelegraph.com/tags/crysto>) Crimen 2020 ha salido a la luz pública, mostrando cómo los corredores de OTC (<https://es.cointelegraph.com/tags/otc>) corruptos establecieron una infraestructura de blanqueo de dinero para mover mil millones de dólares en fondos ilícitos mediante criptomonedas (<https://es.cointelegraph.com/tags/cryptocurrencies>).

El extracto cubierto por la prestigiosa revista Fortune indica cómo los corredores anónimos de venta libre (OTC) se han convertido en el eje central de un nuevo tipo de lavado de dinero (<https://es.cointelegraph.com/tags/money-laundering>), ayudando a convertir al menos USD 2.8 mil millones en Bitcoin

20/1/2020

Los mercados de criptomonedas sorprendieron a muchos con ganancias masivas ayer. Con un aumento de alrededor del 140 por ciento, Bitcoin SV (BSV) lideró el mercado en general, pero algunos analistas sospechan que el enorme aumento de la presión de compra no fue el resultado de un interés genuino de los inversores.

# Criptomonedas para actividades ilícitas

## Quiso lavar dinero con Bitcoin, pero blockchain hizo su magia

Quiso lavar dinero con Bitcoin, pero blockchain hizo su magia

By Luis Mendoza — On Abr 3, 2020 — 2,661 — 0

NOTICIAS ESTAFAS

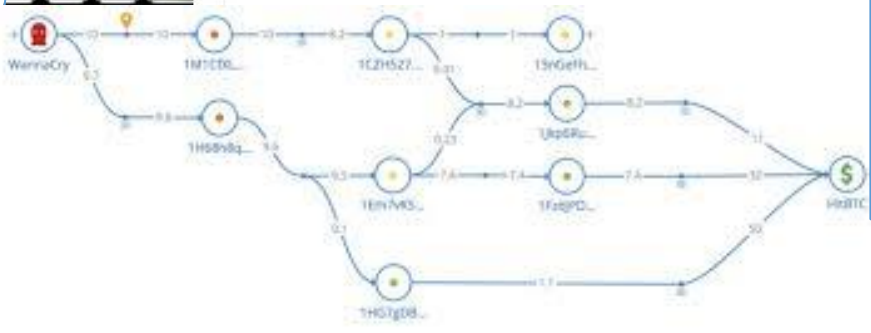
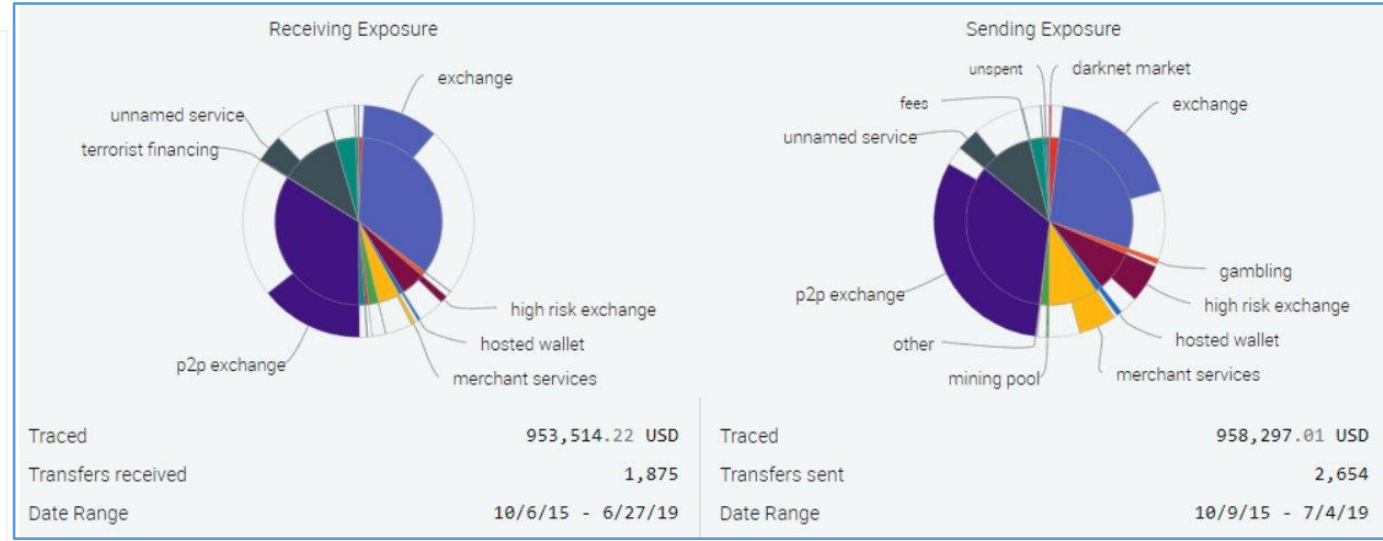
La Oficina Federal de Investigaciones (FBI) utilizó la actividad de billetera Bitcoin y una antigua cuenta de cambio, como evidencia clave para arrestar a un rapero ruso acusado de conspiración para cometer lavado de dinero.

En una declaración jurada revelada a principios de esta semana, la agente especial del FBI Samantha Shelnick dijo que ella y su equipo habían usado el rastro de papel digital para descubrir una importante operación de lavado de dinero, dirigida por una organización criminal oscura conocida como QAAZZ. Se cree que el rapero, Maksim Boiko, está estrechamente relacionado con los líderes de la pandilla, según conoció **CriptomonedaselCO**.

QAAZZ recibió y lavó dinero para los ciberdelincuentes al cambiar la moneda fiduciaria a criptografía. El grupo se había registrado para múltiples intercambios, incluidos **Coinbase** y **Bits1** con el nombre de usuario «Atrof95».

Como estos intercambios tienen cheques **KYC** (conozca a su cliente), los funcionarios del FBI vincularon las cuentas a una cuenta de correo electrónico controlada por un **Aleksejs Trofimovics** que, como afirma la declaración jurada, se comunicaba regularmente con los números de teléfono asociados con Boiko.

Los teléfonos de Boiko, utilizados para comunicarse con Trofimovics, incluían múltiples capturas de pantalla de direcciones de billetera Bitcoin y transacciones de hasta \$ 35.000. En una investigación adicional, muchas de estas imágenes se encontraron en conversaciones entre Boiko y otros miembros sospechosos de QAAZZ.





# Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services



**TABLE 7**

DISTRIBUTION OF LAUNDERED BITCOINS, BY CONVERSION SERVICE TYPE					
	2013	2014	2015	2016	All years
ATM	0.00%	0.00%	0.03%	0.05%	0.01%
Bitcoin Exchange	61.79%	23.22%	41.34%	59.40%	45.43%
Crypto-Exchange	0.17%	0.32%	0.64%	0.30%	0.37%
Gambling	10.86%	43.48%	31.56%	12.21%	25.79%
Mixer	24.97%	26.54%	19.27%	24.20%	23.40%
Multi-Service	2.20%	6.44%	7.16%	3.84%	5.00%
Grand Total	100.00%	100.00%	100.00%	100.00%	100.00%

**TABLE 10**

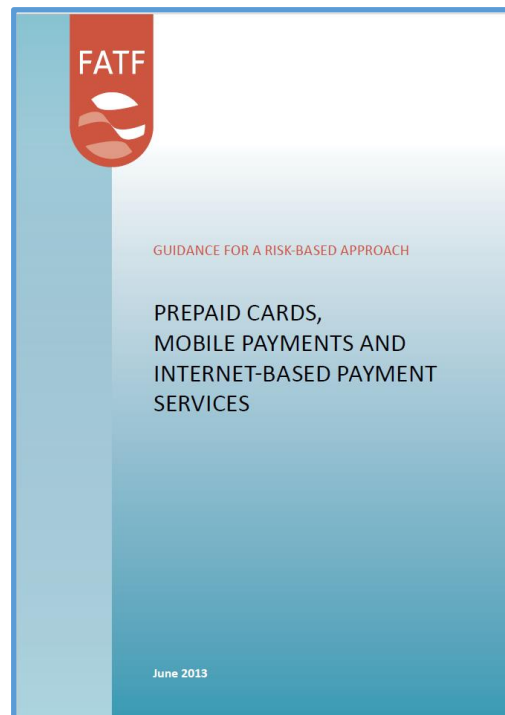
DISTRIBUTION OF TOTAL BITCOIN VOLUME INTO CONVERSION SERVICES, BY REGION					
	2013	2014	2015	2016	All years
Africa	0.00%	0.00%	0.09%	0.26%	0.11%
Asia	27.59%	21.95%	52.07%	52.56%	42.97%
Europe	34.37%	43.91%	27.81%	22.86%	29.76%
North America	17.27%	19.95%	12.85%	19.14%	16.88%
Oceania	0.00%	0.14%	0.22%	0.11%	0.13%
South America	0.13%	0.20%	0.24%	0.22%	0.20%
Unkown	20.64%	13.86%	6.72%	4.85%	9.94%
Grand Total	100.00%	100.00%	100.00%	100.00%	100.00%



# Lavado de dinero mediante el uso de nuevos métodos de pago



**2010**



**2013**



Tarjetas Prepagas



Pagos por Dispositivos Móviles

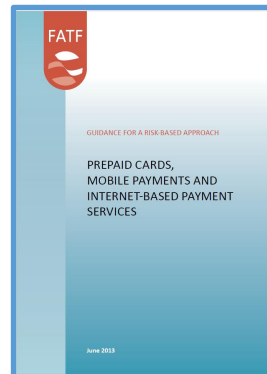


Pagos por Internet

# Lavado de dinero mediante el uso de nuevos métodos de pago



2010



2013



Tarjetas Prepagas



Pagos por Dispositivos Móviles



Pagos por Internet

El caso de Bitcoin es sin duda particular. No se trata de un método de pago por Internet de forma estricta, sino que representa un esquema de moneda virtual que opera a nivel mundial basado en una red de pares descentralizada (también conocida por su denominación en inglés como peer-to-peer) y que se ha convertido por el momento en el más exitoso y controvertido entre todos los esquemas virtuales existentes. Al igual que cualquier otra moneda oficial, el Bitcoin permite todo tipo de transacciones, ya sean transferencias a otras personas o compras de productos de forma anónima.

## Novedades

- Prepaid Cards
- ATMs
- Credit Cards

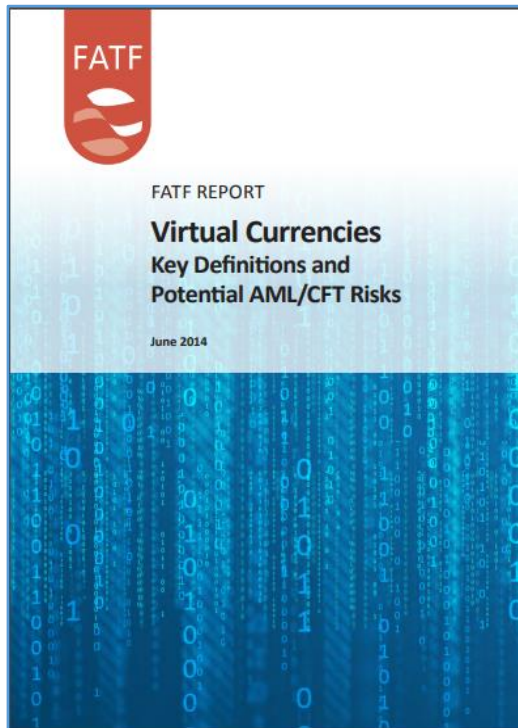
## Riesgos

- LA/FT
- Evasión
- Ponzi
- Ciberataques

## Regulación

- Unión Europea
- Estados Unidos
- Canadá

# Monedas Virtuales - Riesgo de LA/FT



2014

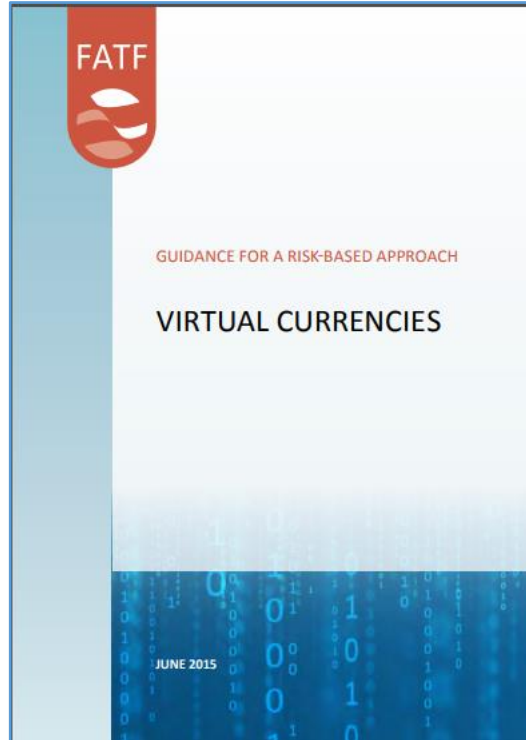
## Taxonomy of Virtual Currencies

	Centralised	Decentralised
<b>Convertible</b>	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
<b>Non-convertible</b>	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

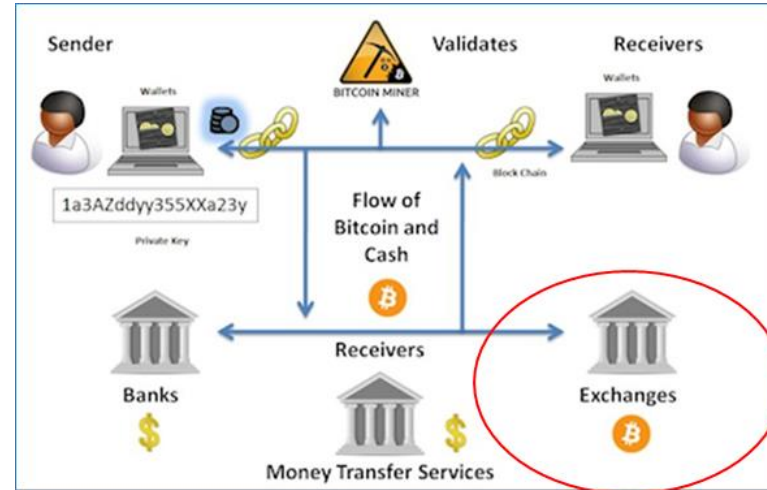


- Liberty Reserve – Costa Rica (2013) – USD 6 billion
- Silk Road (2013) – USD 1,2 billion
- Western Express International – Ucrania – USD 35 million

# Monedas Virtuales - Riesgo de LA/FT



2015

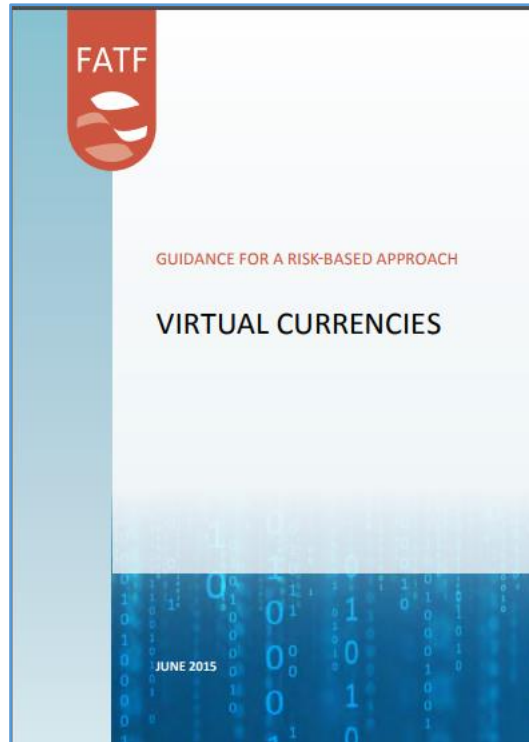


- RBA asociado a VCPPS\* [R1]
- Debida Diligencia – [R10]
- Mantenimiento de Registros y Reporte de Operaciones Sospechosas [R11] [R20] [R22]
- RBA Nuevas Tecnologías [R15] [R22]

\* VCPPS – Virtual Currency Payment Products and Services - Productos y Servicios de Pago de Moneda Virtual



# Monedas Virtuales - Riesgo de LA/FT



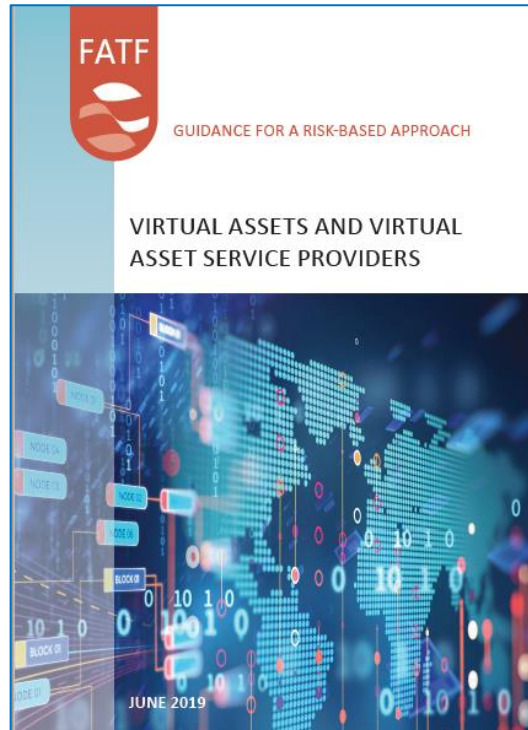
2015



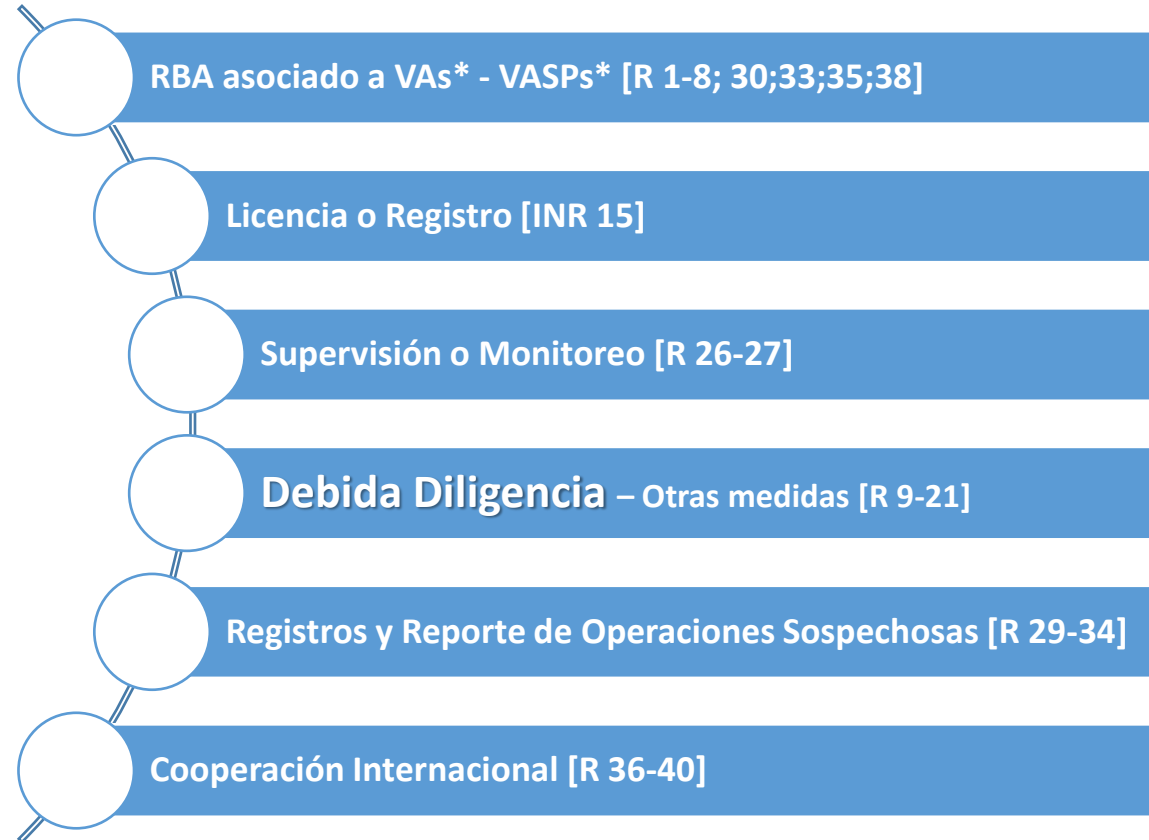
Canadá	• VCPSS como MSB (2014) – Intervención reguladora
China	• Medidas de supervisión mejoradas (2013) - Aviso
Francia	• Regulación ACPR y Recomendaciones TRACFIN (2014)
Alemania	• Instrumento Financiero
Hong Kong	• Delito no Revelar Transacciones Sospechosas (2013)
Italia	• Advertencia sobre el uso (2015)
Rusia	• Borrador de ley prohibición de sustitutos monetarios electrónicos (2014)
Singapur	• Conocimiento del cliente y ROS (2014)
Sudáfrica	• Advertencia. No regulación (2014)
Suiza	• DDC obligatorio y licencia (2014)
Reino Unido	• Regulación ALA
Estados Unidos	• Regulación ALA/CFT – “Bitlicenses” NY

\* VCPSS – Virtual Currency Payment Products and Services - Productos y Servicios de Pago de Moneda Virtual

# Activos Virtuales - Riesgo de LA/FT



2019



\* VA – Virtual Assets [Activos Virtuales]

\*\* VASP – Virtual Asset Service Provider [Proveedor de Servicios de Activos Virtuales]

# Activos Virtuales - Riesgo de LA/FT



**Table 1. Progress in implementing VASP AML/CFT regulatory regimes**

	FATF	FSRB	Total
<b>Regulation of VASPs</b>			
AML/CFT regime permitting VASPs is established	24	8	32
Regulations being developed / approved to regulate VASPs	9	4	13
<b>Prohibition of VASPs</b>			
VASPs prohibited with prohibition enforced	1	2	3
Regulations being developed / approved to prohibit VASPs	2	0	2
<b>Yet to decide</b>			
Approach to VASPs under consideration	2	2	4
<b>TOTAL</b>	<b>38</b>	<b>16</b>	<b>54</b>

2020 – jul 7

Un activo virtual es una **representación digital de valor** que puede comercializarse o transferirse digitalmente y puede utilizarse para fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI.

### Changes to FATF Standards

- New definitions of 'virtual asset' and 'virtual asset service provider'
- Revised R.15
- New INR.15

### Changes to FATF Methodology

- New definitions of 'virtual asset' and 'virtual asset service provider'
- Technical compliance - Revised R.15
- Effectiveness - Revised methodology, particularly Immediate Outcomes 3 and 4

### Changes to FATF Guidance

- Release of new FATF Guidance on a Risk-Based Approach for virtual assets and VASPs

\* VA – Virtual Assets [Activos Virtuales]

\*\* VASP – Virtual Asset Service Provider [Proveedor de Servicios de Activos Virtuales]

# Resumen

## Criptomonedas y sus principales riesgos de LA/FT

---



- 01.** Anonimato (Debida Diligencia)
- 02.** Mezcladores (Mixers – Tumblers)
- 03.** Intercambios (Exchanges) y plataformas descentralizadas
- 04.** ICOs y negocios poco transparentes



# Resumen

## Criptomonedas y sus principales riesgos de LA/FT

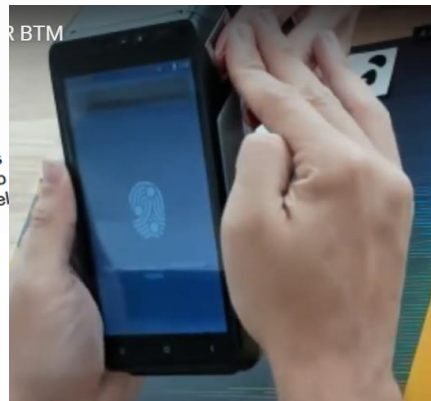
- Mantener contacto, acompañamiento y comunicación entre entidades y S.O.
- Fortalecer EBR.
- Monitoreo de las transacciones financieras (OSFL).
- Fomentar el uso de identidad digital.



Comunicado del GAFILAT sobre el COVID-19 y sus riesgos asociados de LA y FT

Buenos Aires, Argentina a 8 de abril de 2020.

Ante la presente situación que representa la pandemia de COVID-19, la comunidad internacional ha tomado medidas y ha aplicado recursos a fin de mitigar en lo posible el impacto de este fenómeno en la población. En este esfuerzo necesario, surge la posibilidad de que algunas medidas o controles encaminados a la prevención y combate al Lavado de Activos (LA) y el Financiamiento del Terrorismo (FT) y la proliferación (FP), se hayan visto afectadas y por lo tanto surjan posibles amenazas y/o vulnerabilidades en los sistemas Anti-Lavado de Activos y Contra el Financiamiento al Terrorismo (ALA/CFT) implementados por los diferentes actores en las distintas jurisdicciones en el mundo.





[gerenteproyectos@riskconsultingcolombia.com](mailto:gerenteproyectos@riskconsultingcolombia.com)

[ledaza@javeriana.edu.co](mailto:ledaza@javeriana.edu.co)

[ledaza@gmail.com](mailto:ledaza@gmail.com)