



San Francisco | March 4–8 | Moscone Center

A graphic element consisting of a large, stylized word "BETTER." in white. The letters have a complex, woven texture. Behind the letters is a background of many thin, colorful lines (blue, yellow, green) radiating from the bottom right corner, suggesting a network or a burst of energy.

BETTER.

SESSION ID:SEM-M03J

Bitcoin Por Favor: Cybercriminal Usage of Cryptocurrency in Latin America

Ian W. Gray

Director of Americas Analysis & Research
Flashpoint
@iw_gray

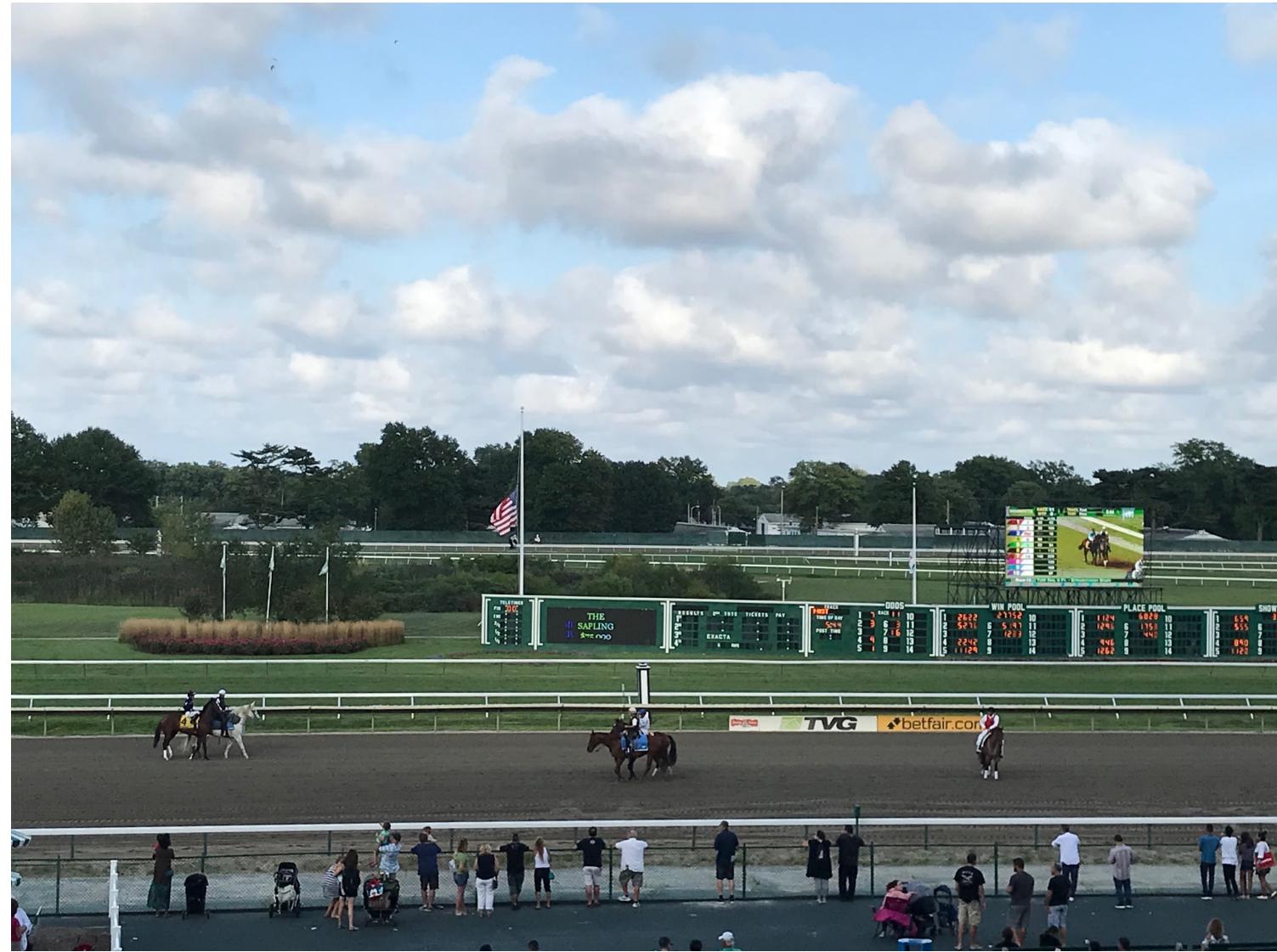
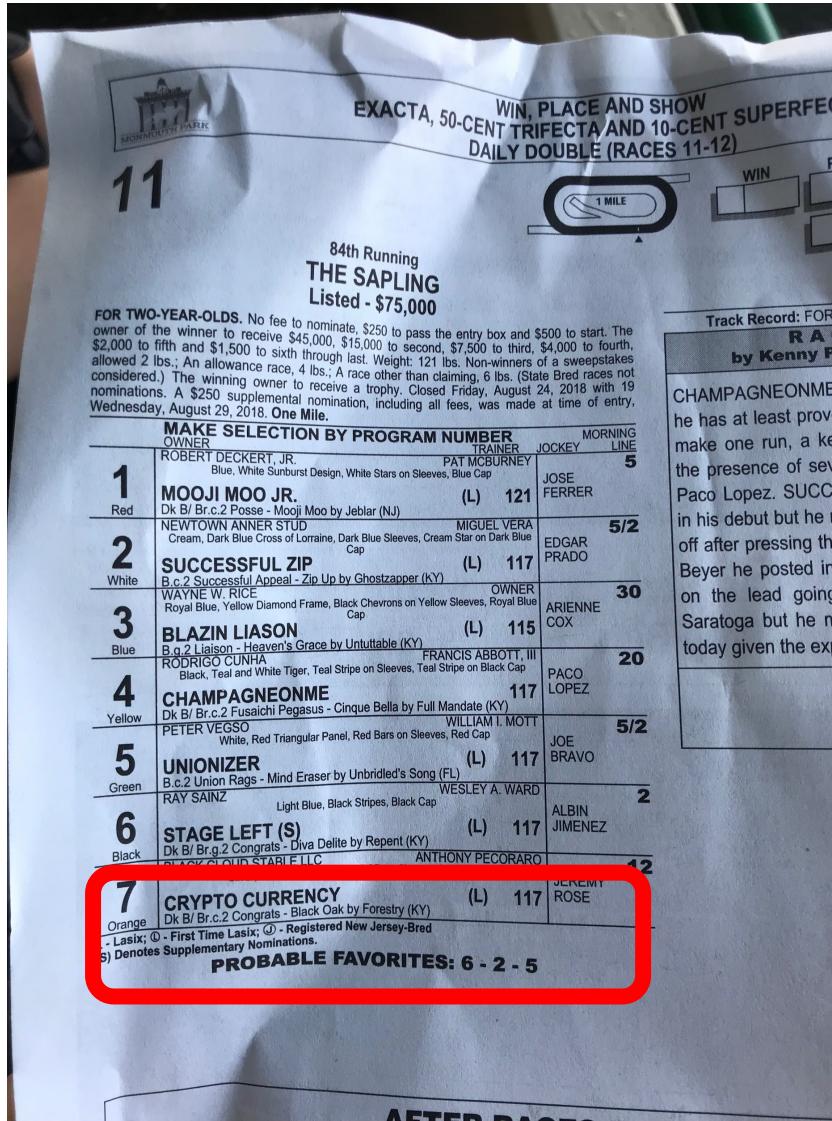
Carles Lopez-Peñalver

Cybercrime Analyst
Chainalysis
@carleslopezp

#RSAC



Always Bet on CRYPTO CURRENCY!



Presentation Summary

- Socioeconomic Issues Affecting Legitimate Adoption of Cryptocurrencies in Latin America
 - Case Study: Mexico, Colombia, Argentina, Venezuela
- Legitimate Payment Processors
 - Fraudulent Use of Payment Processors
- Deep and Dark Web Activity
 - Popular Cryptocurrencies
- The Future of Cryptocurrencies in Latin America

Primero, una clase en Español:

- Criptomoneda - Cryptocurrency
- Criptodivisa - Cryptocurrency
- Criptoactivo - Cryptoassets
- Bitcoin - Bitcoin



How do you acquire cryptocurrencies

- Alternative methods
 - Cryptomining
 - Ransomware
- Cryptocurrency Exchanges
- Peer-to-Peer (P2P) Exchanges
 - Local Bitcoins
- Forum Exchanges
 - Foro-PTC

Research Methods

- Deep and Dark Web Datasets
- Blockchain Research
- Firsthand Research (talking to bad guys)
- Research Gaps and Assumptions
 - Anonymity
 - Language

RSA®Conference2019

Socioeconomic Issues Affecting Adoption of Cryptocurrencies in Latin America

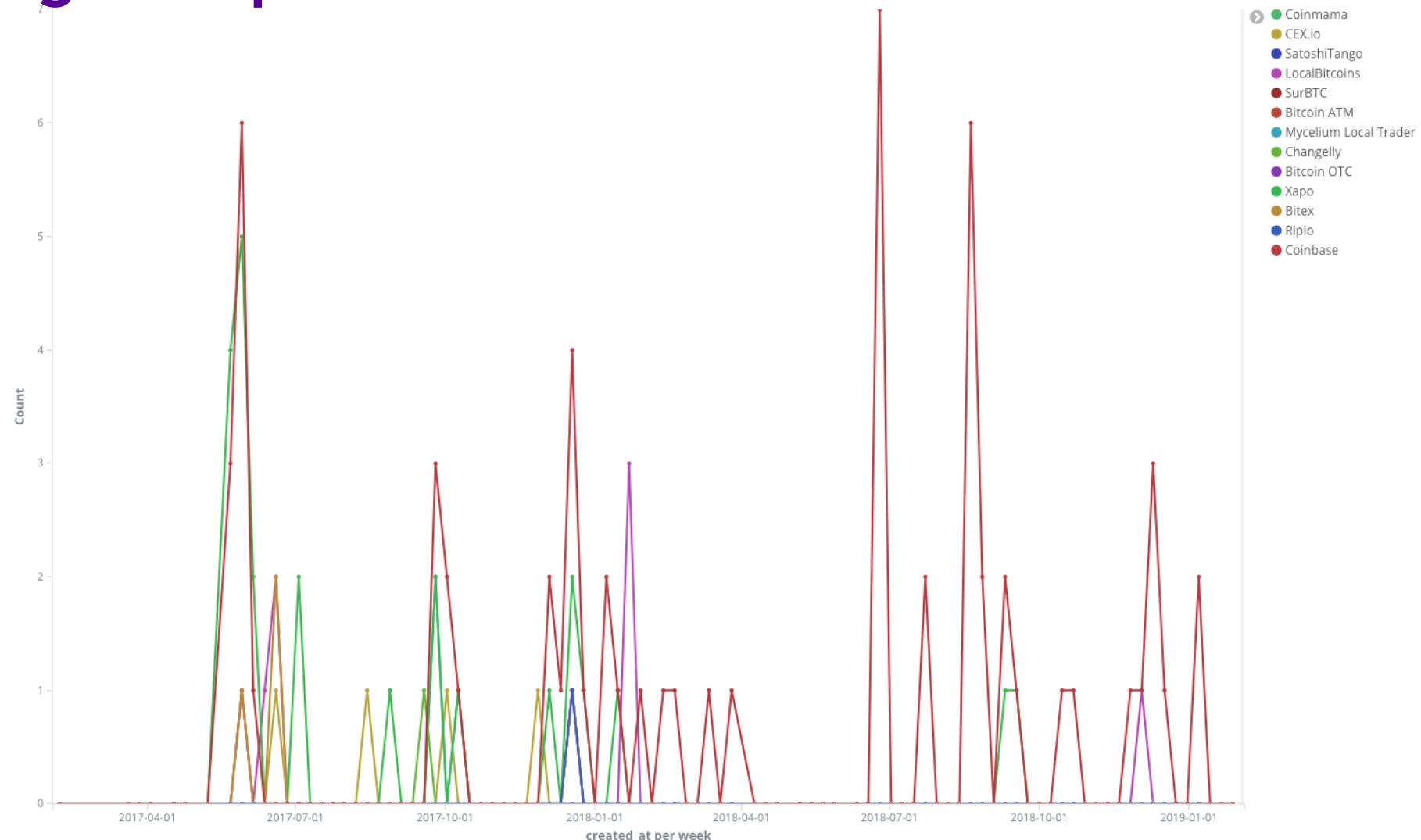
Case Study: Mexico, Colombia, Argentina,
Venezuela

Largest Cryptocurrency Exchanges in the Region

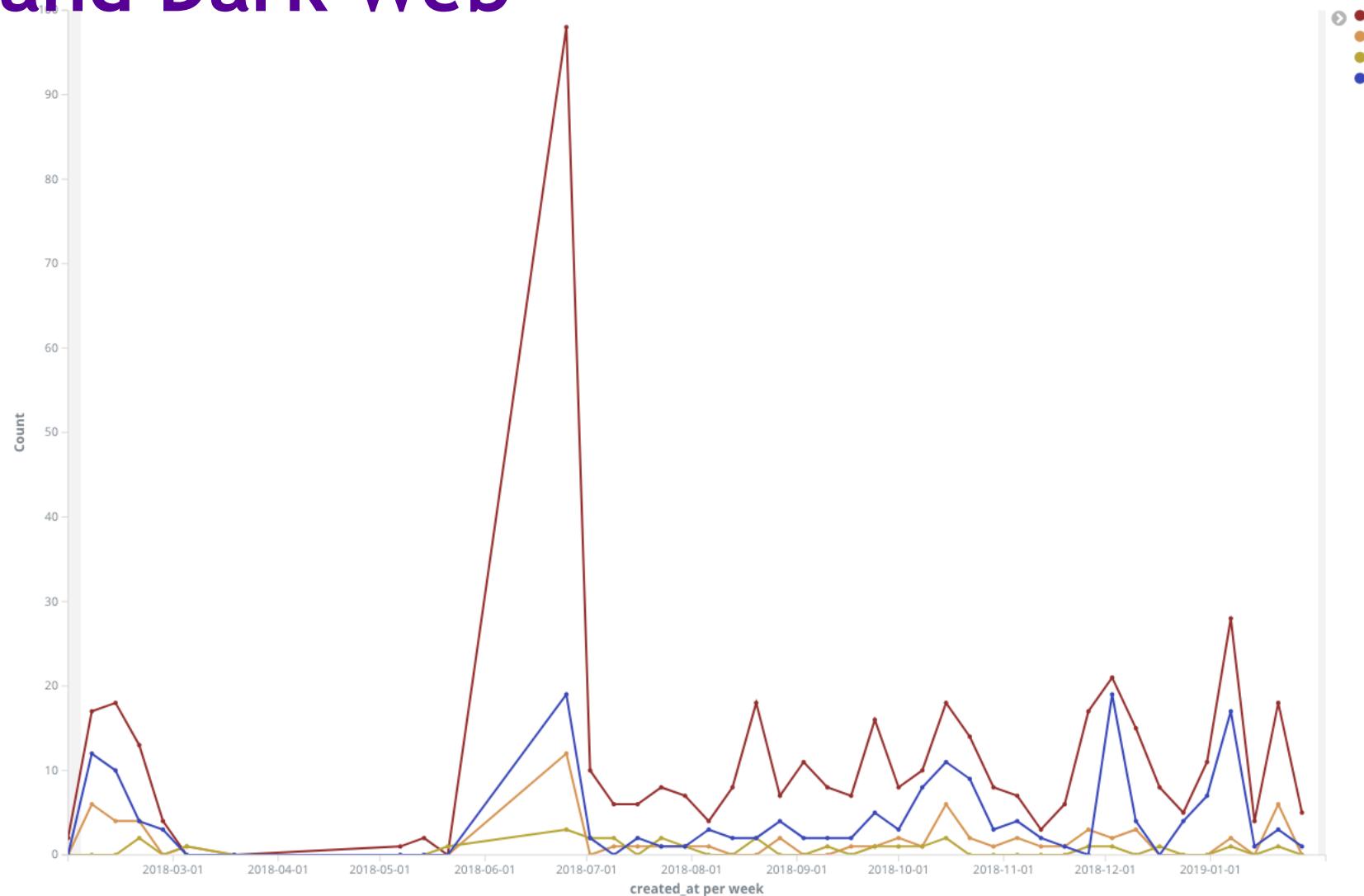
- Mexico
- Colombia
- Argentina
- Venezuela



Most Popular Cryptocurrency Exchanges in Spanish Language Deep and Dark Web Forums



Cryptocurrency Chatter on Spanish Language Deep and Dark Web



Mexico

- No dedicated cybercrime laws
- Cryptocurrencies are legal and FINTECH companies gain approval.
- The Central Bank has not announced which cryptocurrencies are legal

Colombia

- Cryptocurrencies do not constitute a legal form of payment
- Cryptocurrencies have been declared illegal
- Not protected by any guarantee or deposit insurance

Argentina

- Not legal tender
- They are not regulated
- Treated as goods under the nation's Civil Code

Venezuela is the Ideal Case for Legitimate Use of Cryptocurrencies

- Citizens have distrust of regional banks
- Cryptocurrencies enables trust financial sovereignty to individuals, perhaps outside of regional institutions
 - Venezuela
- Allows an independence which may not have been previously offered through conventional regional currencies due to weak or nonexistent infrastructures

Venezuela

- Currency controls on the Bolivar
- Increasing inflation
- Lack of international bank accounts from most citizens, making cryptocurrency a viable option
- Exchange controls force Venezuelan banks to only use the local currency
 - Increased activity from local bitcoins, a cryptocurrency-to-payment card service

Constituent Decree on the Integral System of Crypto Assets

- “Venezuela’s “Constituent Decree on the Integral System of Crypto Assets” has been published in the country’s official gazette. The decree establishing the legal framework for cryptocurrencies and all related activities contains 63 articles; it entered into force with the publication in the gazette.”

Local Bitcoins

- Analysts have observed a number of actors within Flashpoint's Deep and Dark Web (DDW) datasets discussing services that allow users to convert cryptocurrencies, such as Bitcoin and Ether, into payment card funds.
- Mexico - 47 listings
- Colombia - 97 listings
- Argentina - 81 listings
- Venezuela - 524 listings

Local Bitcoins in Latin America

Buy bitcoins online in Venezuela

Browse Offers: Bank Transfers, Online Wallets, Remittance, Gift Card Codes, Other Payments

Show all trades in Venezuela

Showing results 1 - 50 of 445

← 1 2 3 4 5 6 7 8 9 →

Seller	Payment method	Price / BTC	Limits	Buy
CoinbaseBTCBR (100+; 100%)	Transfers with specific bank: ★ BANCO CARONI - 78.500 Oferta!!!	12,393,000.00 VES	1 - 290,000 VES	Buy
CoinbaseBTCBR (100+; 100%)	Transfers with specific bank: ★ BANCO DEL TESORO 40.000 un pago	12,396,000.00 VES	1 - 280,000 VES	Buy
yodian (1000+; 100%)	Transfers with specific bank: BANCO DE VENEZUELA SOLO 258.400	12,400,850.00 VES	258,400 - 270,000 VES	Buy
Abrahanbitcoins (2; 100%)	Transfers with specific bank: BDV ✓★ ★ BANCO VENEZUELA ✓★ ★ BDV	12,402,140.69 VES	1 - 559,184 VES	Buy
Allen007 (3000+; 100%)	Transfers with specific bank: ── BANESCO PANAMA ── ✓★ LIBERO 5 MIN★✓ j27/02!	3,795.00 USD	1 - 1,180 USD	Buy
demm.25 (500+; 99%)	Transfers with specific bank: ⚡ Banesco Panama ⚡	3,797.08 USD	200 - 765 USD	Buy
armandoc (1000+; 100%)	Transfers with specific bank: ✓★ ★ VENEZUELA ★✓ ── 45.833 ── ⚡	12,550,000.00 VES	10 - 300,000 VES	Buy
doomcaripe (1000+; 99%)	Transfers with specific bank: Banesco!! Rapido libero de una!!	12,550,000.00 VES	0 - 583,309 VES	Buy
doomcaripe (1000+; 99%)	Transfers with specific bank: Banco venezuela!! Frente a la pc. 60.450	12,550,000.00 VES	0 - 583,309 VES	Buy

Buy bitcoins online in Colombia

Browse Offers: Bank Transfers, Online Wallets, Remittance, Gift Card Codes, Other Payments

Show all trades in Colombia

Showing results 1 - 50 of 79

← 1 2 →

Seller	Payment method	Price / BTC	Limits	Buy
Jagonz25 (30+; 100%)	Transfers with specific bank: Bancolombia	10,888,000.00 COP	200,000 - 1,500,000 COP	Buy
luzmy0928 (100+; 100%)	Cash deposit: Bancolombia	10,888,000.00 COP	1,000,000 - 3,000,000 COP	Buy
miguelobo (500+; 100%)	Transfers with specific bank: Bancolombia, av villas, davivienda.baloto.efecty	10,919,000.00 COP	350,000 - 4,600,000 COP	Buy
btcworld3000 (1000+; 100%)	Transfers with specific bank: BANCOL DAVI BBVA BOGOT CAJASOCI FALAB NEQI COLPA	10,950,000.00 COP	1,000,000 - 1,204,500 COP	Buy
Megaplusbtc (14; 100%)	Transfers with specific bank: BANCOLOMBIA	10,980,000.00 COP	500,000 - 2,719,695 COP	Buy
dankolombia (100+; 100%)	National bank transfer: Colombia	10,983,000.00 COP	300,000 - 9,798,817 COP	Buy
Sebasclub (1000+; 99%)	Transfers with specific bank: BANCOLOMBIA ,TRADER PRO 100% SEGURO	10,990,000.00 COP	400,000 - 32,293,088 COP	Buy
Lukas16 (500+; 100%)	Transfers with specific bank: Bancolombia APP, Corresponsal Bancario.	11,000,000.00 COP	50,000 - 900,000 COP	Buy
servibitcoin2018 (70+; 100%)	National bank transfer: Colombia	11,000,000.00 COP	200,000 - 550,000 COP	Buy

RSA®Conference2019

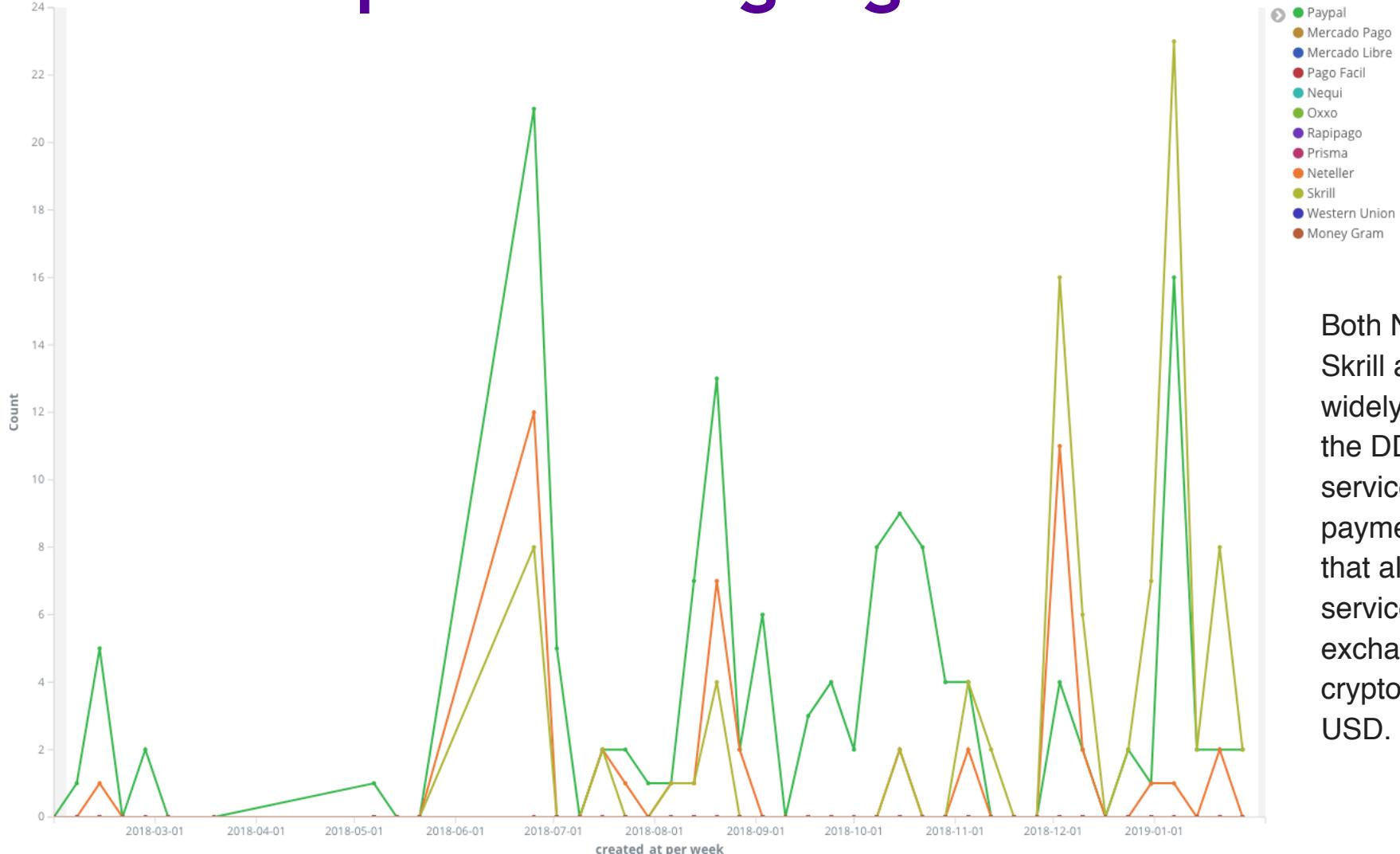
Legitimate Payment Processors

Fraudulent Use of Payment Processors

Cybercrime Payment Processors

- Which is the most popular for fraud?
- What is accepted? What is solicited?
- Cashing out
 - When a threat actor transfers money from a compromised account - for example Venmo, PayPal, or bank accounts - to another account, usually one that is controlled by the threat actor.

Graph of Mentions of Payment Processors in Deep and Dark Web Spanish Language Forums



Both Neteller and Skrill appear to be widely discussed in the DDW. Both services are online payment systems that also offer limited services for users to exchange cryptocurrency for USD.

RSA®Conference2019

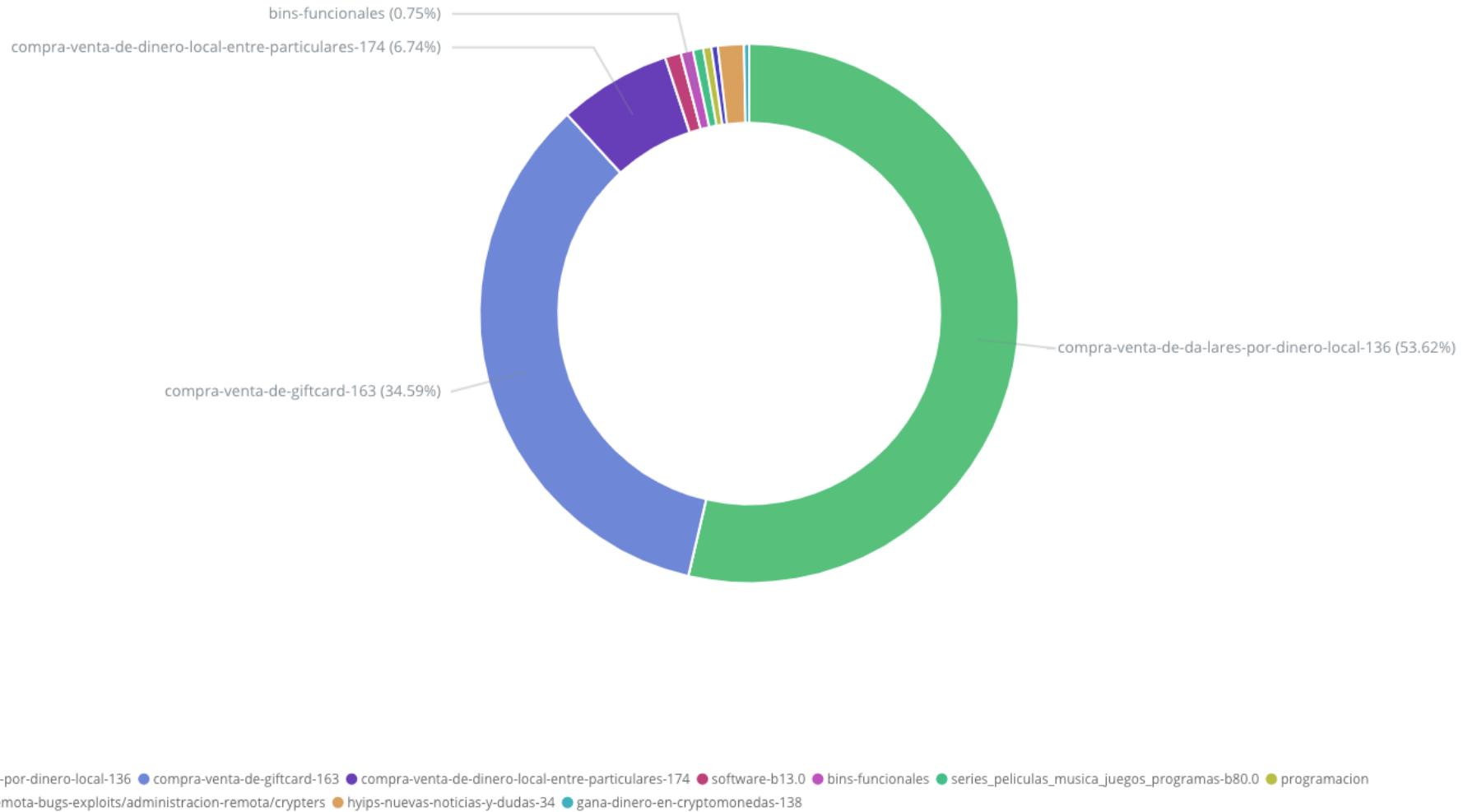
Deep and Dark Web Activity

Popular Cryptocurrencies

Global Illicit Use of Cryptocurrencies

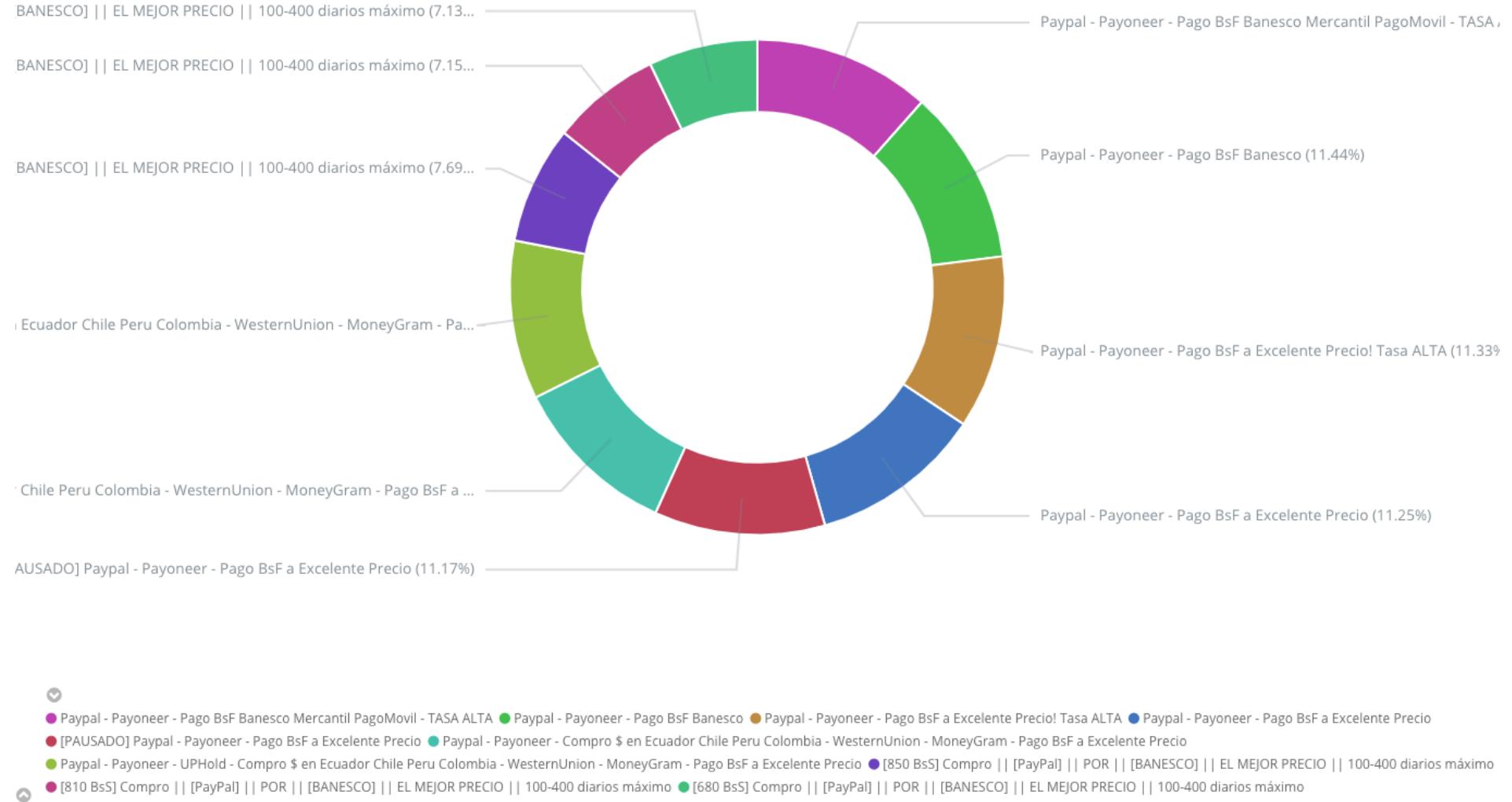
- The perceived anonymity provided by cryptocurrencies, and their increasing valuation has led cybercriminals to adopt them as their primary method of payment.
- Cryptocurrencies are additionally being leveraged to provide additional revenue streams through ransomware and cryptojacking campaigns.
- Although not as sophisticated in their campaigns, there has been an observable uptick in the interest of cryptocurrencies within the Latin American cybercriminal underground. Though the growth has not been consistent to other geographical locations.

Most Popular Rooms on Spanish Language Forums

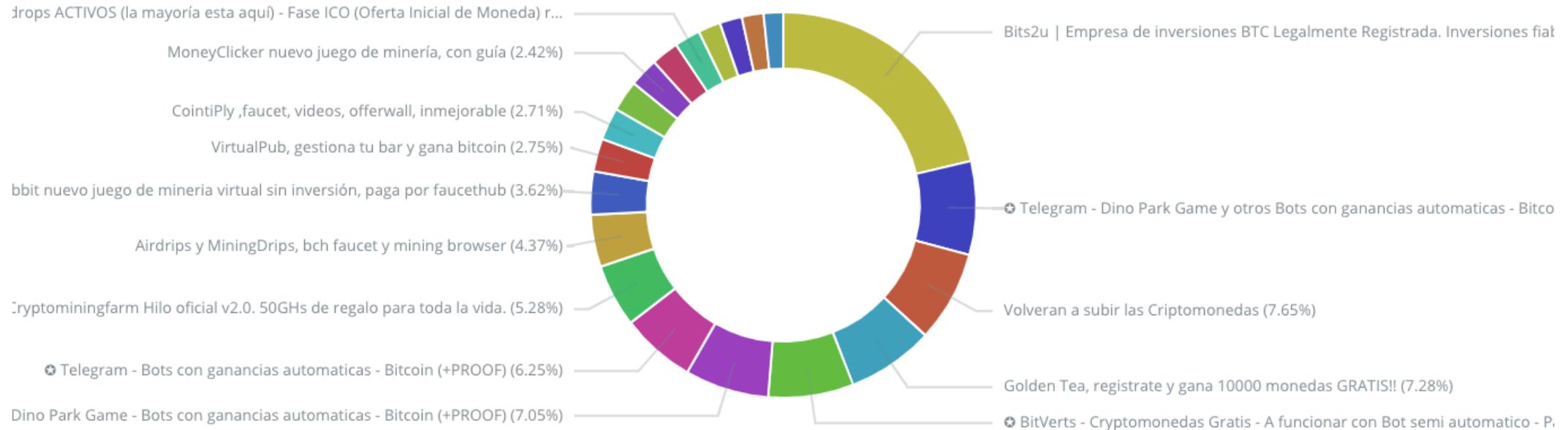


▼
compra-venta-de-dlares-por-dinero-local-136 ● compra-venta-de-giftcard-163 ● compra-venta-de-dinero-local-entre-particulares-174 ● software-b13.0 ● bins-funcionales ● series_peliculas_musica_juegos_programas-b80.0 ● programacion
● hacking-administracion-remota-bugs-exploits/administracion-remota/crypters ● hyips-nuevas-noticias-y-dudas-34 ● gana-dinero-en-cryptomonedas-138

Most Popular Threads within Those Rooms

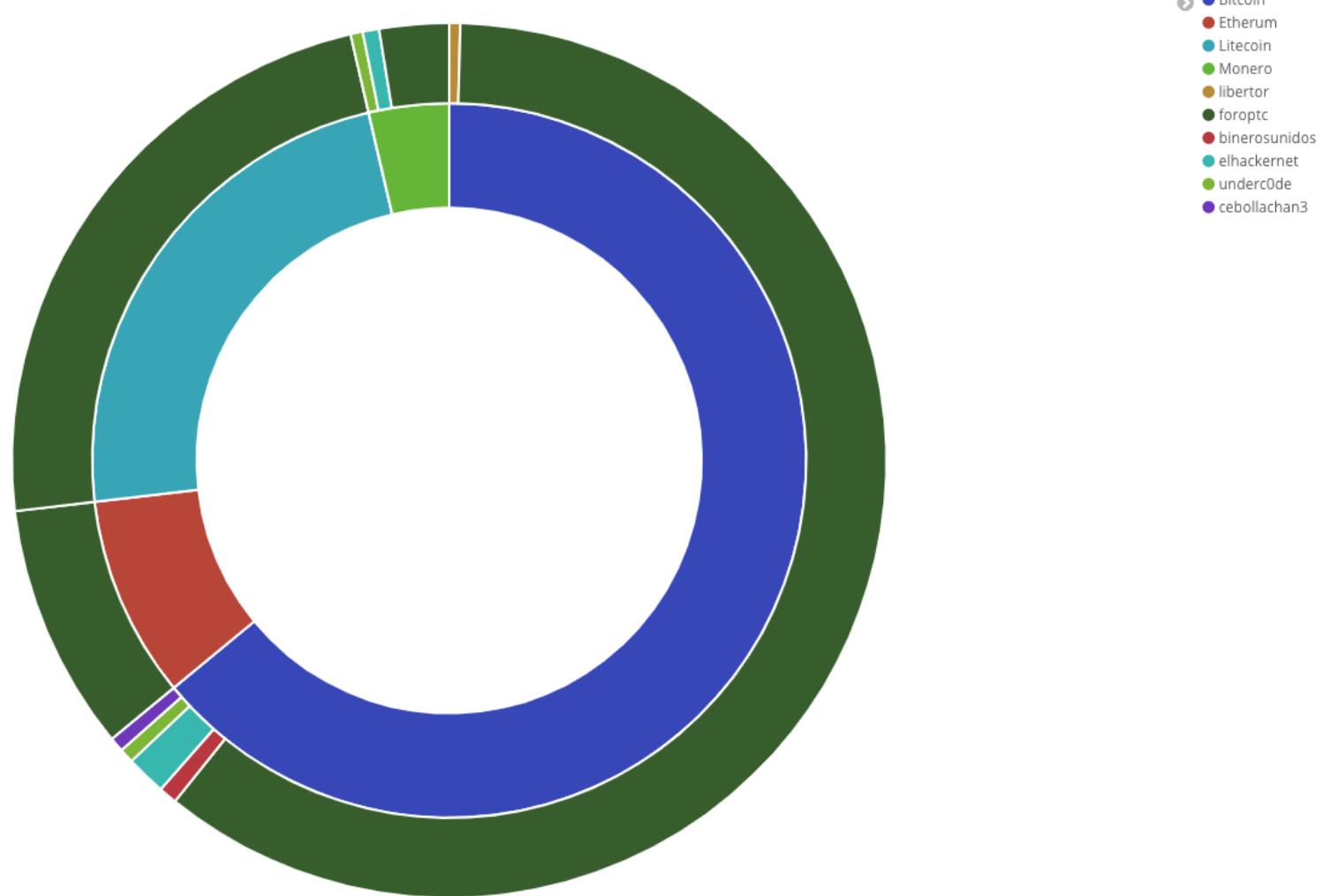


Most Popular Rooms within “Gana Dinero en Cryptomonedas”

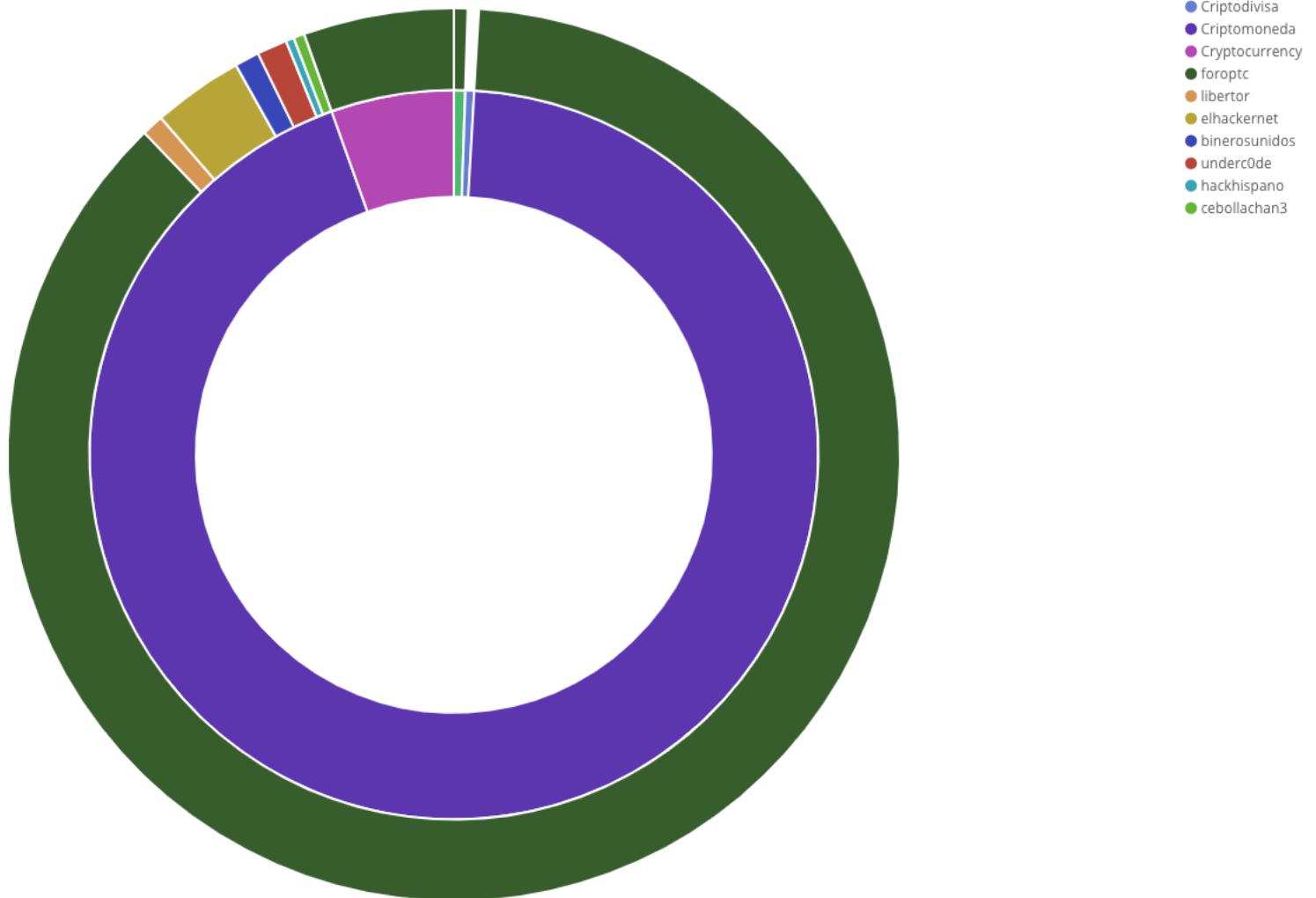


- Bits2u | Empresa de inversiones BTC Legalmente Registrada. Inversiones fiables y muy rentables
- Volveran a subir las Criptomonedas
- Golden Tea, regístrate y gana 10000 monedas GRATIS!!
- BitVerts - Cryptomonedas Gratis - A funcionar con Bot semi automatico - Pagos inmediatos - Bitcoin/BitcoinCash/Litecoin/Ethereum (+PROOF)
- Telegram - Dino Park Game - Bots con ganancias automaticas - Bitcoin (+PROOF)
- Cryptominingfarm Hilo oficial v2.0. 50GHs de regalo para toda la vida.
- Airdrips y MiningDrips, bch faucet y mining browser
- Febbit nuevo juego de mineria virtual sin inversion, paga por faucethub
- VirtualPub, gestiona tu bar y gana bitcoin
- CointiPly ,faucet, videos, offerwall, inmejorable
- CointiPly ,faucet, videos, offerwall y MiningGame, inmejorable
- MoneyClicker nuevo juego de minería, con guía
- CryptoMKT exchange REGALA 50 usd en crypto por registro! APROVECHEN!!
- Lista Actualizada de Airdrops ACTIVOS (la mayoría esta aquí) - Fase ICO (Oferta Inicial de Moneda) regalando tokens/monedas 30/05/18
- Bsa1, simulador de trading + Airdrops gratis, más de 1000\$ en premios cada 10 días
- CointiPly ,faucet, videos, offerwal y MiningGame, inmejorable
- Solarmining - Cloud Mining con energía solar - 10 MH/s de bonificación por registro - Mina BTC, LTC, USD y DOGE (27 Pruebas de pago, \$2 diario)
- BtcMines, BitMines y BitRig, satoshi sin límites, esfuerzo cero

Cryptocurrency Mentions Distributed Through Various Forums



Criptomonedas Mentions Distributed Through Various Forums



Payment Preference for DDW Vendor

- Another well recognized Latin American vendor with over 1000 transactions (according to the fraud forum) appears to accept Bitcoin, Western Union, and OXXO payments to carry out refund fraud.

Medios por los que pagas

Bitcoin
Western Unión
OXXO

BANCOS LOCALES [EN PROCESO PREGUNTA PARA QUE TENGAS TODO CLARO]

WARNING: SI DESCONOCES LOS MÉTODOS DE PAGO Y COMO USARLOS, NO DUDES EN CONSULTARME.

After carrying out an in-depth conversation with the threat actor they explained that most of the payments for their services tend to be Western Union and National Banks. The researchers were able to corroborate after conducting blockchain analysis in the actor's wallet.

Payment Preference for DDW Vendor

- Vendors across the Latin American Deep and Dark Web often use a large array of payment methods including cryptocurrencies, national and international bank transfers, as well as a large array of payment processors.

METODO DE PAGO | FORMAS DE PAGAR:

(SI NO TIENES NINGÚN METODO DE PAGO Y LO TIENES EFECTIVO, NO DUDES EN CONTACTAR, TE AYUDARÉ PERSONALMENTE)

Bitcoin o Otras Criptomonedas

Oxxo

Bancos Locales

Transferencia Bancaria Nacional o Internacional

SPEI

SEPA

WesternUnion

MoneyGram

Nequi

PayPal

Skrill

(SI NO TIENES NINGÚN MÉTODO DE PAGO Y LO TIENES EFECTIVO, NO DUDES EN CONTACTAR, TE AYUDARÉ PERSONALMENTE)

Moderator of a well known Latin American carding forum accepts a large array of payment methods for illicitly obtained flights.



Spanish Speaking Dark Net Vendors

- Spanish speaking threat actors operating on Dark Web marketplaces such as Dream Market and AlphaBay Market have to carry out transactions with cryptocurrencies due to the markets' enforcement.
- Most DDW vendors, even if Latin American, will list their products in English; potentially obfuscating their country of origin and getting a larger market share.



Product description

Hola traigo este hash directo de Morocco. Soy el único intermediario por lo que puedo asegurar su calidad. Este producto que traigo es de una calidad excepcional, a un precio comercial insuperable. Este hash procede de la segunda vareada de la marihuana, "<https://www.youtube.com/watch?v=LLeVRTQA9jw>", en este video se puede apreciar el proceso de fabricación para que se entienda como se hace el hash en morocco. Hay varios procesos de vareo para la extracción del hash y este hash se puede considerar de segunda categoría real. En relación calidad/precio es el hash que yo recomiendo, es un hash perfecto para revender por su precio y calidad, no hay nada mejor en toda la darknes. Al fumar este hash se puede apreciar que es suave, pero tiene muy buen sabor y un olor agradable. La fumada de este hash te da sensación de tranquilidad y relajación. Para cualquier duda consultarme sin problemas os ayudare lo antes posible.

AlphaBay Market Archive

Facebook Adsense Real / Facebook Publicidad Real

Last Observed: Dec 20, 2017 10:27 UTC ⓘ

Dream Market ⓘ

2gr Hash Of Morocco SAMPLE! Launch Offer (MAX 2GR)

Last Observed: Jun 22, 2018 21:57 UTC ⓘ

ITEM DESCRIPTION:

TRANSLATE

Hola

Estoy ofreciendo el servicio de por publicidad real en facebook. Así es, con esto usted podrá seleccionar el:

País
Ciudad
Sexo
Edades
Intereses
Segmentación
Idiomas

De todo para que su publicidad llegue a las personas que estén interesadas en su producto.

Con este servicio usted podrá:

Atraer Personas a su sitio web
Aumentar las conversiones en su sitio web
Promocionar sus publicaciones
Promocionar su página
Aumentar las instalaciones de su aplicación
Incrementar la interacción en tu aplicación
Aumentar los asistentes a tu evento
Conseguir que las personas soliciten su oferta
Aumentar las reproducciones de video.

Just Another Payment Method

- It appears that Latin American threat actor vendors utilize cryptocurrencies just as an additional method to sell their products.
- If a potential customer is only interested in purchasing goods and services with cryptocurrencies, vendors will give them that option.
- However, it is clear that due to the fact that they also offer regular payment methods in addition to cryptocurrencies, that the latter option is meant as an additional option and not a necessity.

Bitcoins in Brazil

- Brazil, while Portuguese language, has a fairly sophisticated cybercrime ecosystem
- This recent conversation from a dark web version of Reddit demonstrates current cryptocurrency mentality



1 points 3 months ago*

well, people here think that opsec and buying bitcoin is too complicated compared to buying from the streets. you can find anything you want in the street if you really look for it the other factor is that LE cannot get everywhere at anytime. I send the stuff I buy to a guy in a favela. they know his name and address but they can't go there and catch him!

EDIT: typo

Reply Permalink Report Save

1 points 3 months ago*

those people have to be pretty stupid if they think it's too complicated imo. anyway you can find everything on the streets, no matter where you are. the only difference might be the quality if you don't have the right connect. DNM tend to provide better quality in general though.

So basically you say you buy bulk to distribute to your dealer in the favela and you trust a guy who sells on facebook and receives bank transfers from you? I wouldn't worry about the dealer in the favela but I certainly would worry about you in this constellation. You (if you use bank transfers) and even more your source are the weak spots in this chain.

Reply Permalink Report Save

1 points 3 months ago*

everybody does bank transfers and sends the stuff to his address my case is very different: I buy stuff to a friend of mine who lives in a favela. he's a dealer. he just gives me some stuff for free as I don't need to make money out of drugs I buy bitcoins, make the purchase, he gives me the money and some freebies unfortunately street drugs have been very very bad recently everything is mixed with a lot of shit, there is a very large difference in cost and quality buying from DNM my biggest mistake was buying from a local market, as nothing really works in brazil the problem is I had some money lost/stole/something I dunno on dream market recently, so I was a little hesitant dream is actively discussing the matter with me trying to find a solution, but this loss of fund encouraged me to make the purchase from a local market where I've done a successful small purchase before

Reply Permalink Report Save

RSA® Conference 2019

Summary

What have we learned?

The Case for Non-use of Cryptocurrencies

Deterrence or Acceptance?

- Cryptocurrencies, however, retain connotations and associations with cybercrime
- There are technical barriers to entry that may deter neophytes, or individuals without access to technology
- Lack of regional law enforcement may not deter cybercriminal use of legitimate payment processors, or cryptocurrencies
- Convenience



Future Cryptocurrency Use

- Legitimate use of cryptocurrencies within the region will continually be slow, as the volatility of the currency, and lack of regulation, will deter most individuals
- Cybercriminal use of cryptocurrencies will be slow, as convenience trumps security, for most threat actors
- The lack of law enforcement actions regarding cryptocurrencies within the region will permit potential future use, though will likely be accepted as a secondary payment method to more legitimate payment methods