FTEC 5520 (Week 1 - 2)

Agenda - CyberSecurity Basics and Cryptography Week 1 - 2

1. Brief Introduction of Blockchain and Bitcoins
2. Basics of Cyber-Security
3. Application of Cryptographic Tools to Online Banking

Blockchain and Bitcoins

What is blockchain, bitcoins and what are their relevant technology

What Comes After FTX For Blockchain Technology?

If you haven't been following the saga of the collapse of the centralized cryptocurrency exchange known as FTX you can catch up here. Sam Bankman-Fried, the once-CEO of the exchange was loved and heralded as the "good" billionaire, making impactful donations and being a champion for "effective altruism."

As FTX has declared bankruptcy and its financial follies have come to light, the crypto world has once again taken up the war cry of "not your keys, not your coins." A slogan for decentralization, cautioning that if holders of crypto want to securely own their assets, they need to have them in a self custody wallet.

So with trust broken for centralized exchanges like FTX what happens next with blockchain tech?

Coinbase, FTX, Binace and more all offer something that decentralized solutions don't and will never have, which is ease of use. Users come to these experiences for the same reason they trust banks with their money instead of keeping it in a coffee can under their proverbial mattresses. They allow an individual to outsource financial custody and gives ease of management.

Blockchain.com's founder and CEO, Peter Smith, believes that on-chain analytics will play a significant role in locating the billions in missing FTX customer funds, though it will have its limitations.

On Dec. 20, Fox Business host Liz Claman said that blockchain's selling point was that it makes crypto transactions transparent and traceable, and asked Smith what could be traced in the case of FTX's missing customer funds.

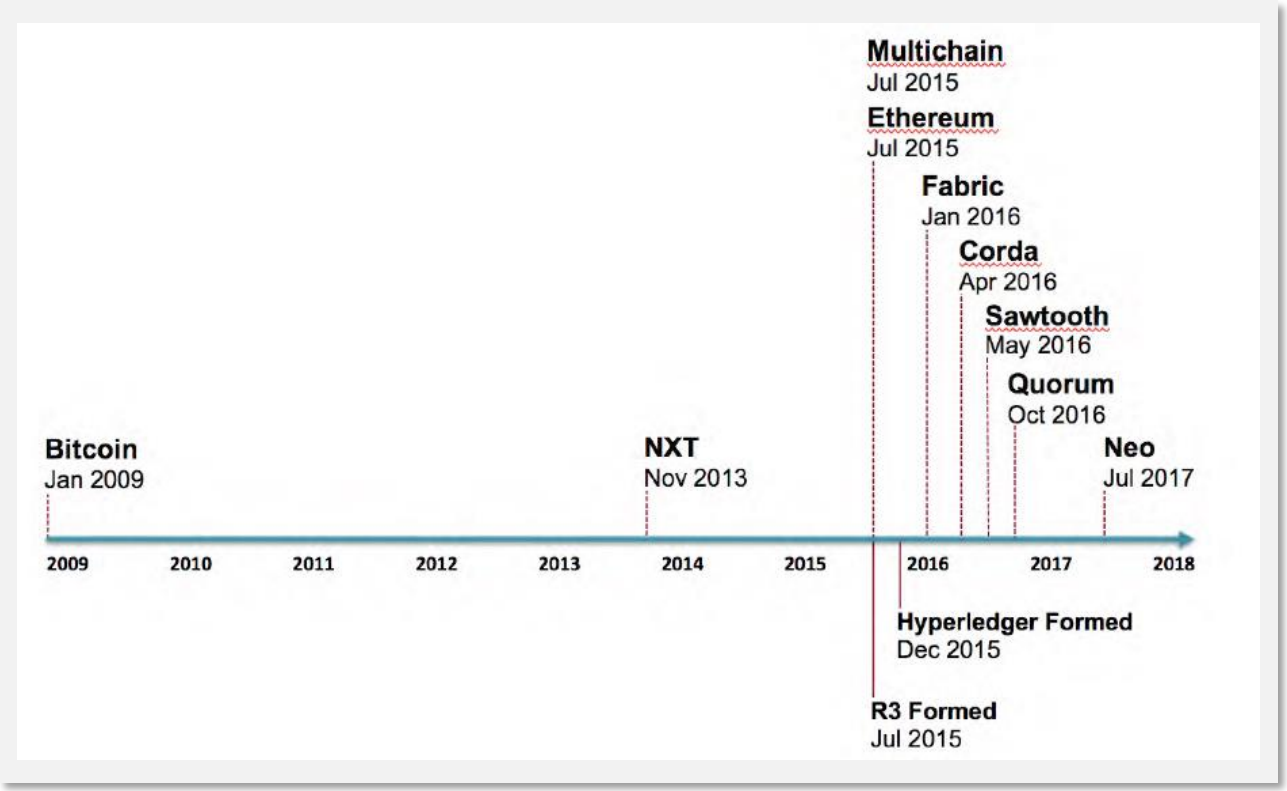
Smith said that blockchain sleuths have already done a fair bit of work in chasing the money trail, adding that it could in fact be the banking system where the trail could turn cold:

> **"The most challenging thing for [blockchain analytics] firms working on this today is when money moves off chain and into the banking system because they're no longer able to track it."**

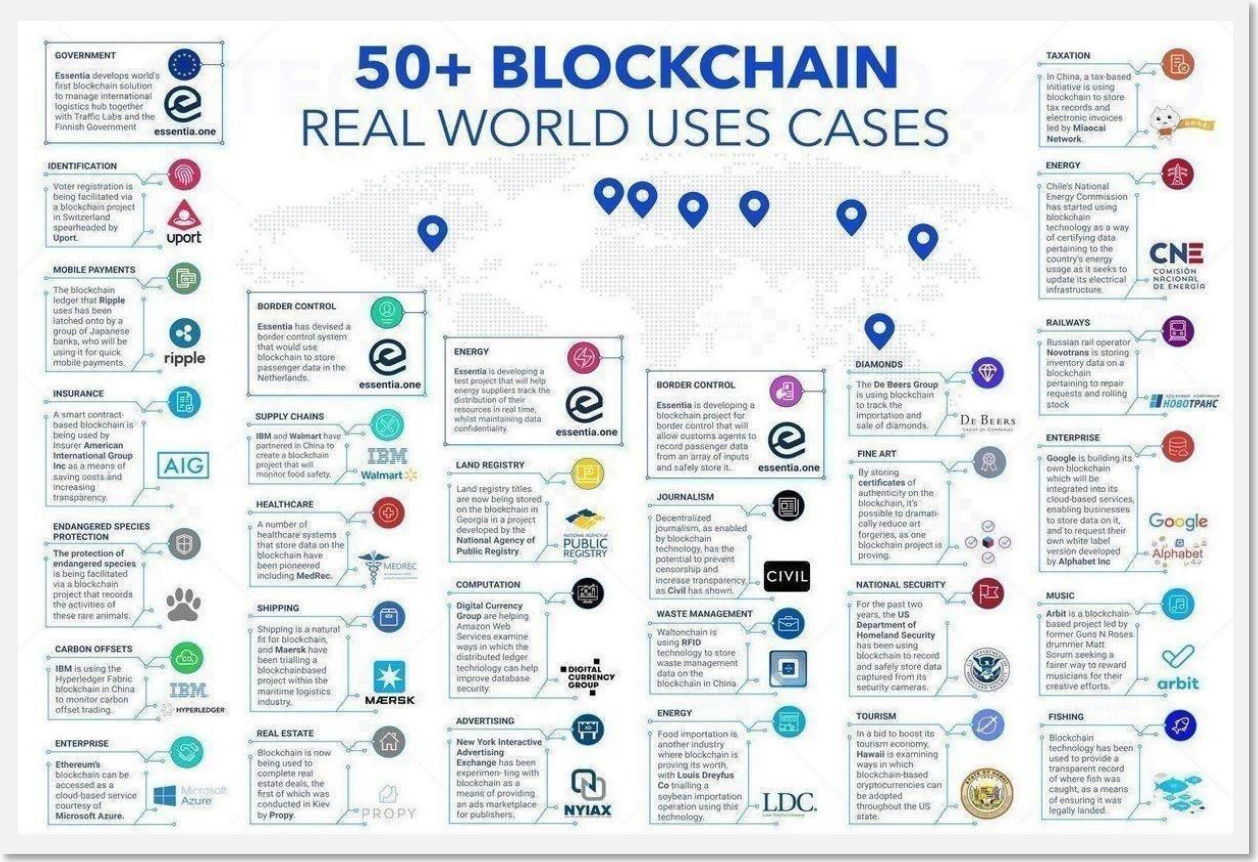
He cited an example of when Sam Bankman-Fried or associates purchased real estate, as that would have originated from a bank. Those assets would be hard to trace back to FTX or a blockchain once they leave the crypto ecosystem, he said.

The interviewer also questioned whether shadow banking was used. This is a system of lenders, brokers, and other credit intermediaries operating outside the realm of traditional regulated banking, which can be used to mask transactions.

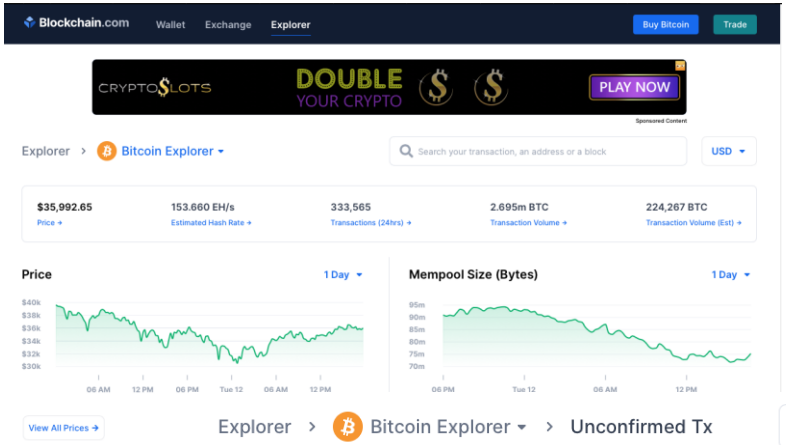
Blockchain – the birth of new era

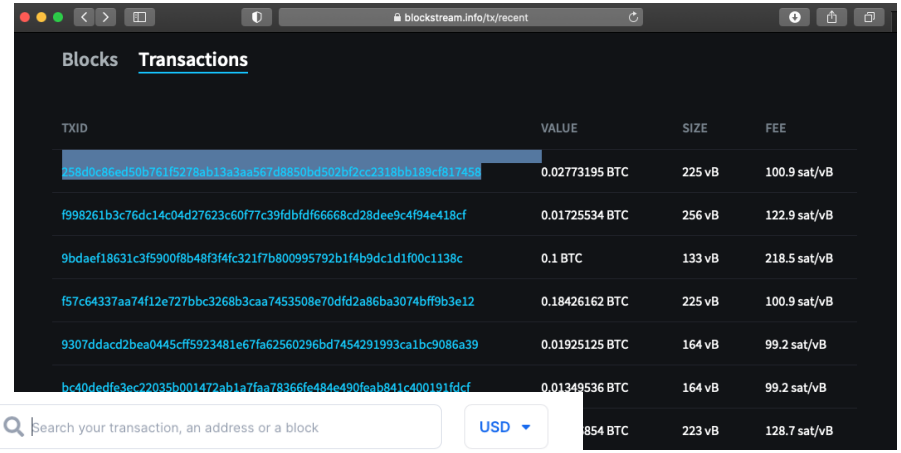


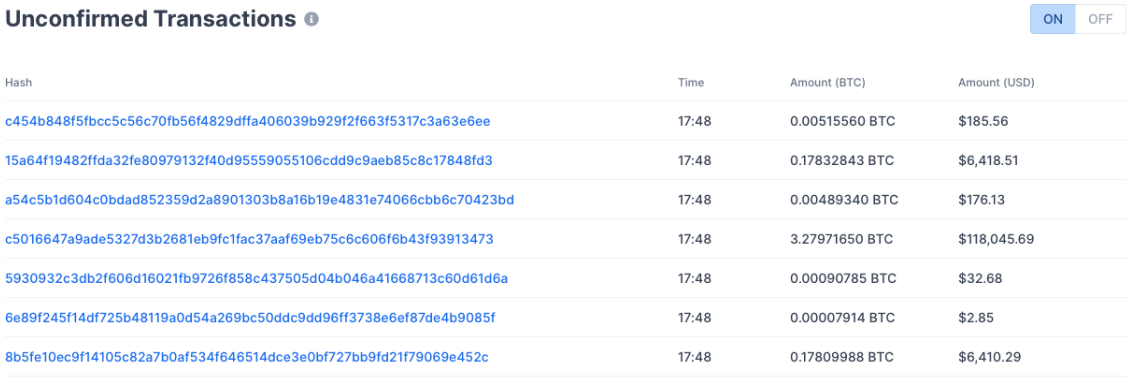
50+ Blockchain Real World Use Cases



Bitcoin Transaction

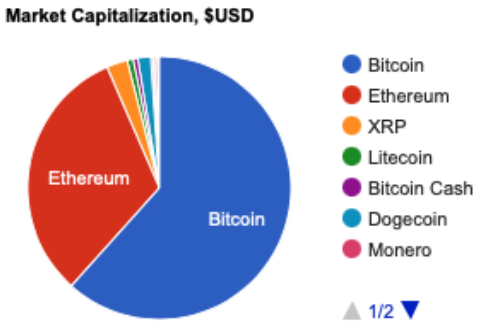


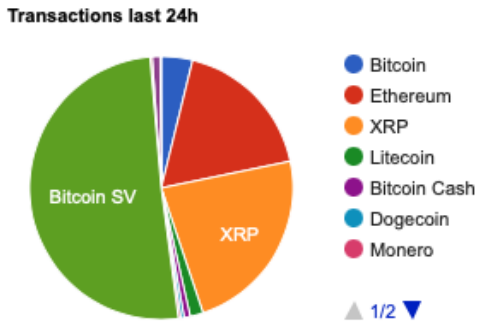


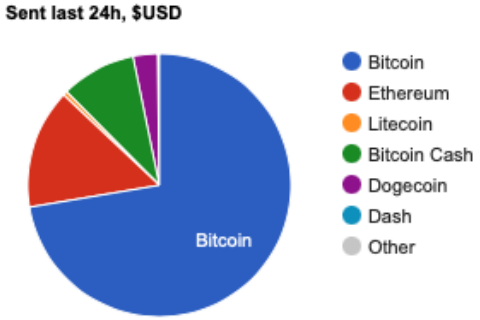


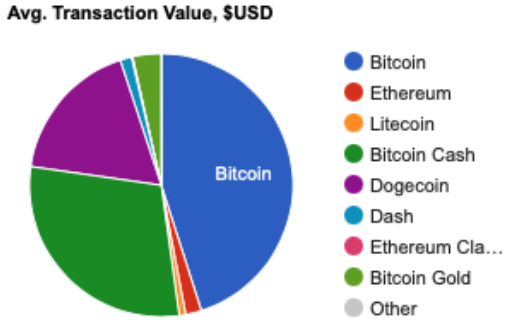
https://www.blockchain.com/explorer?utm_campaign=dcomnav_explorer

CryptoCurrency Capitalization (Jan 2022)



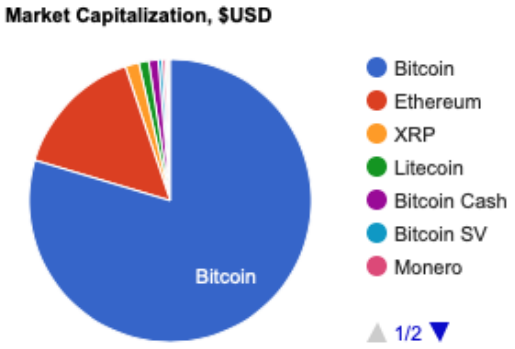


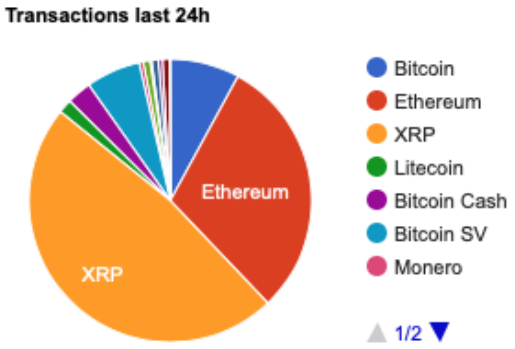


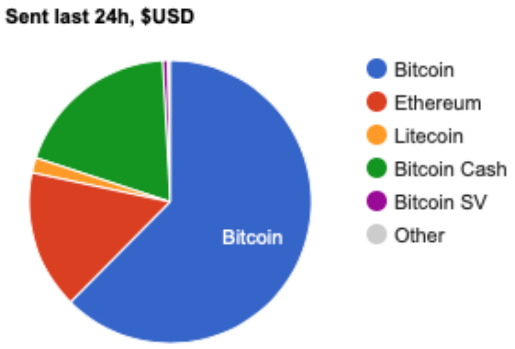


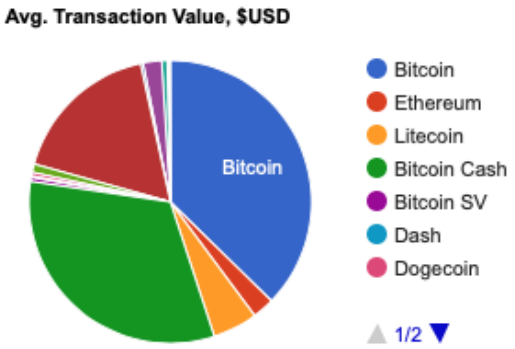
https://bitinfocharts.com/cryptocurrency-charts.html

CryptoCurrency Capitalization (Jan 2021)







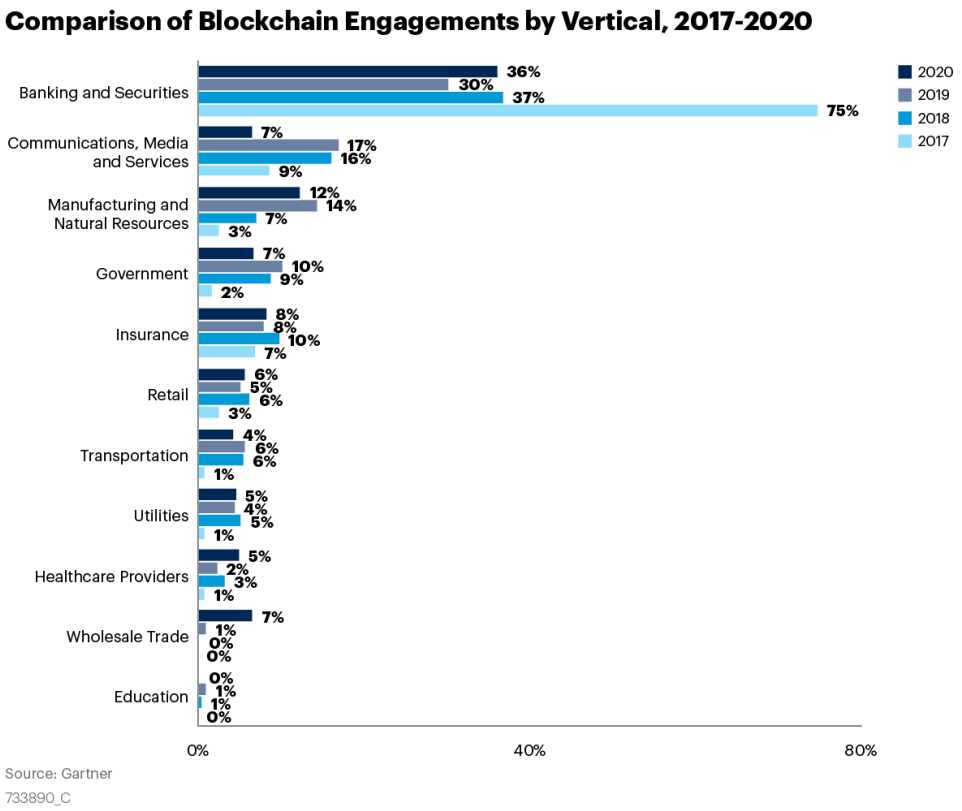


https://bitinfocharts.com/cryptocurrency-charts.html

Blockchain Statistics – Use Cases

Source: Gartner (May 2017)

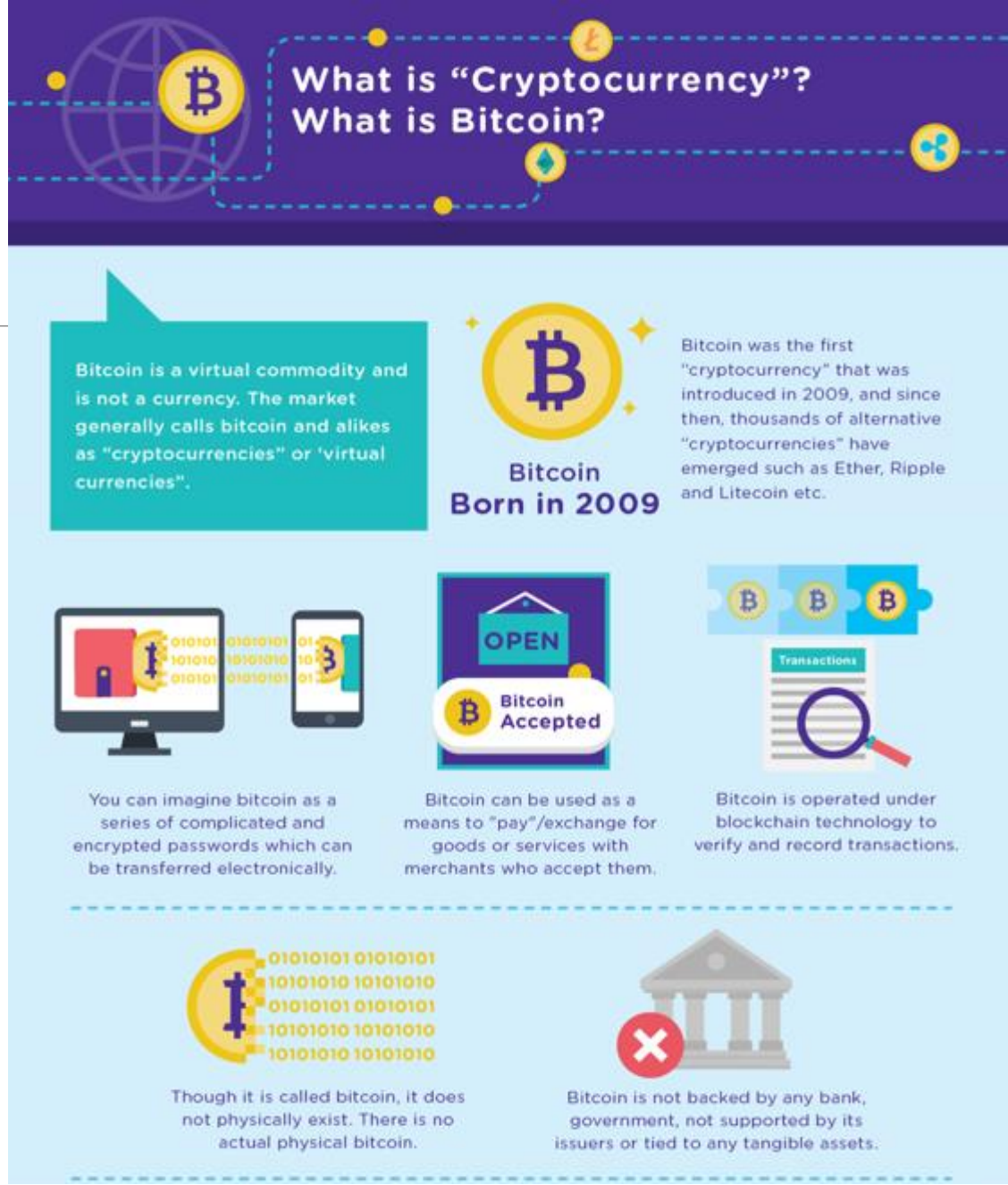
Blockchain Statistics – Engagement by Vertical



Digital currencies

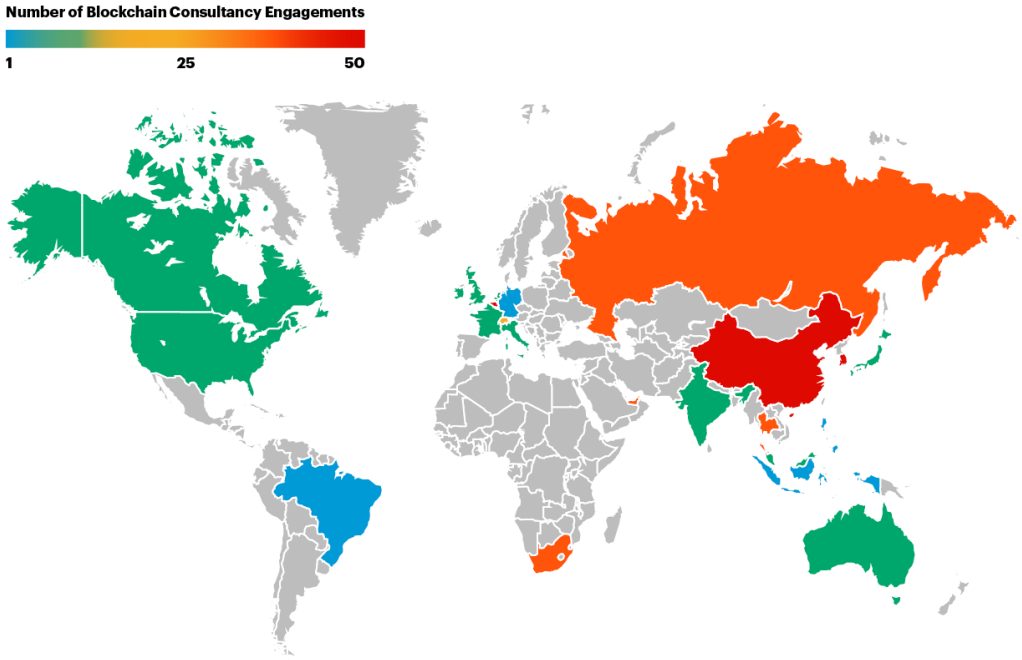
https://www.thechinfamily.hk/web/en/financial-products/fintech/ico-bitcoin/basic-concept-bitcoin.html

…Bitcoin and other “cryptocurrencies” are considered to be “virtual commodities” and are not legal tenders….

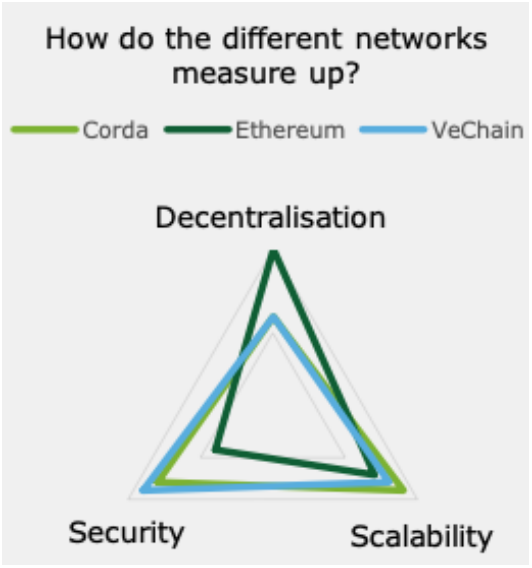


Blockchain Engagement in Production

Heat Map of Proportion of Blockchain Consultancy Engagements Moving to Production, 2020

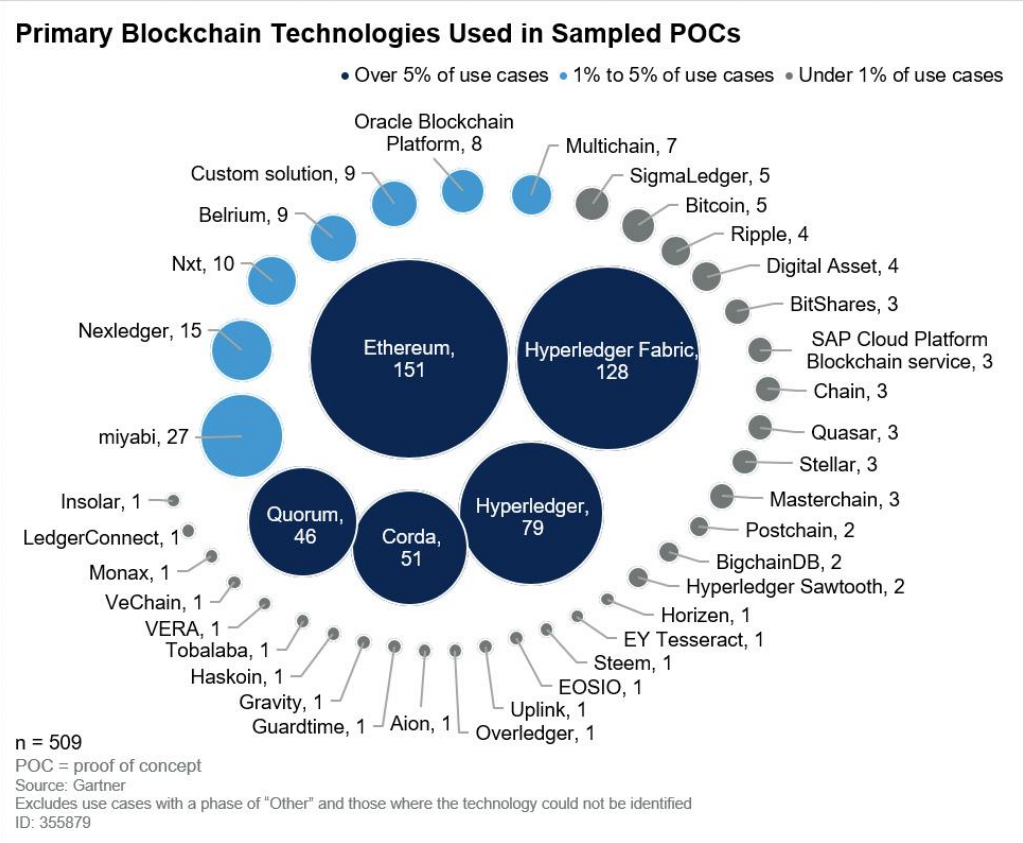


Source: Gartner
733890_C

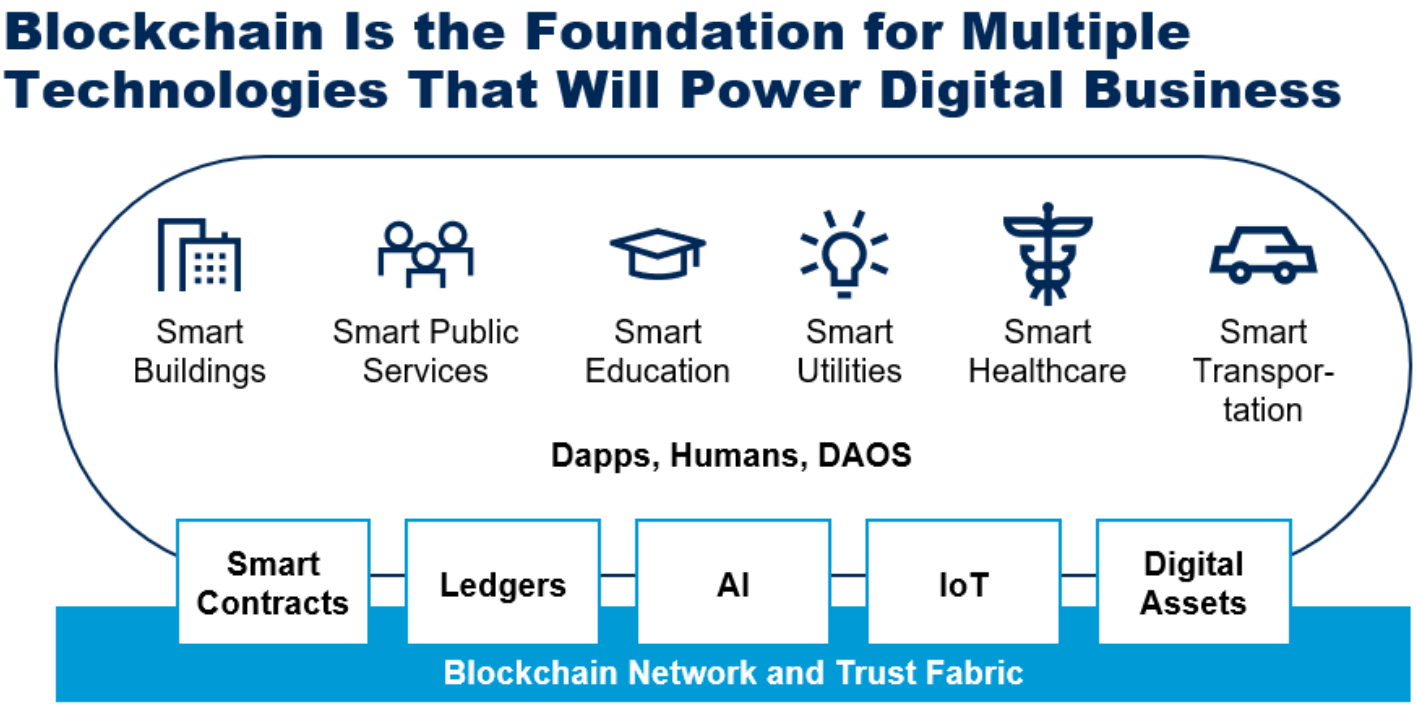


Deloitte

Blockchain Technology used in POCs (2019)

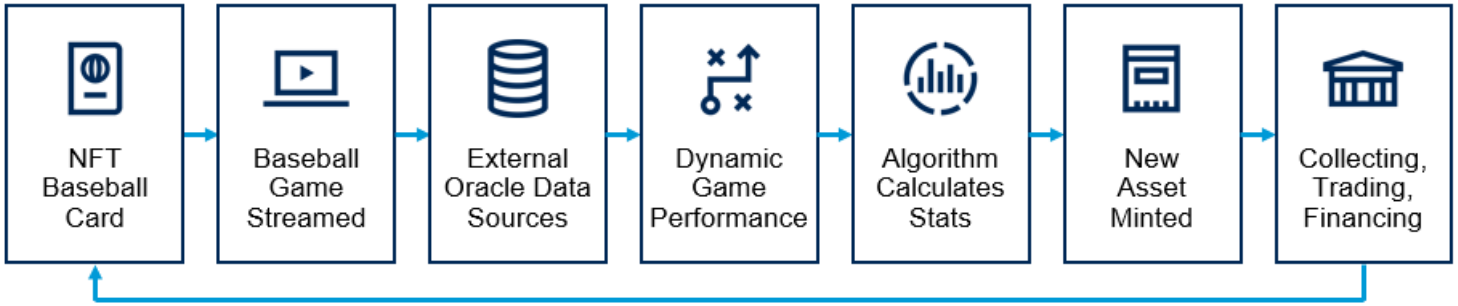


Gartner's view and wish



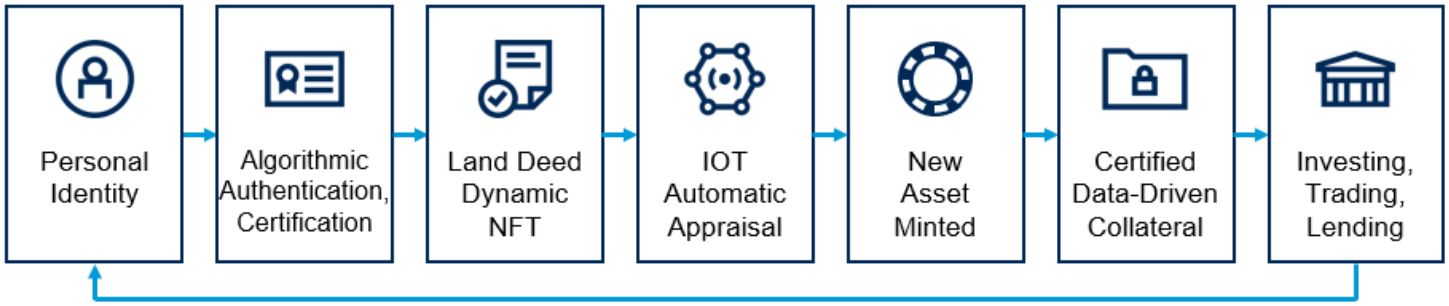
Gartner's view and wish

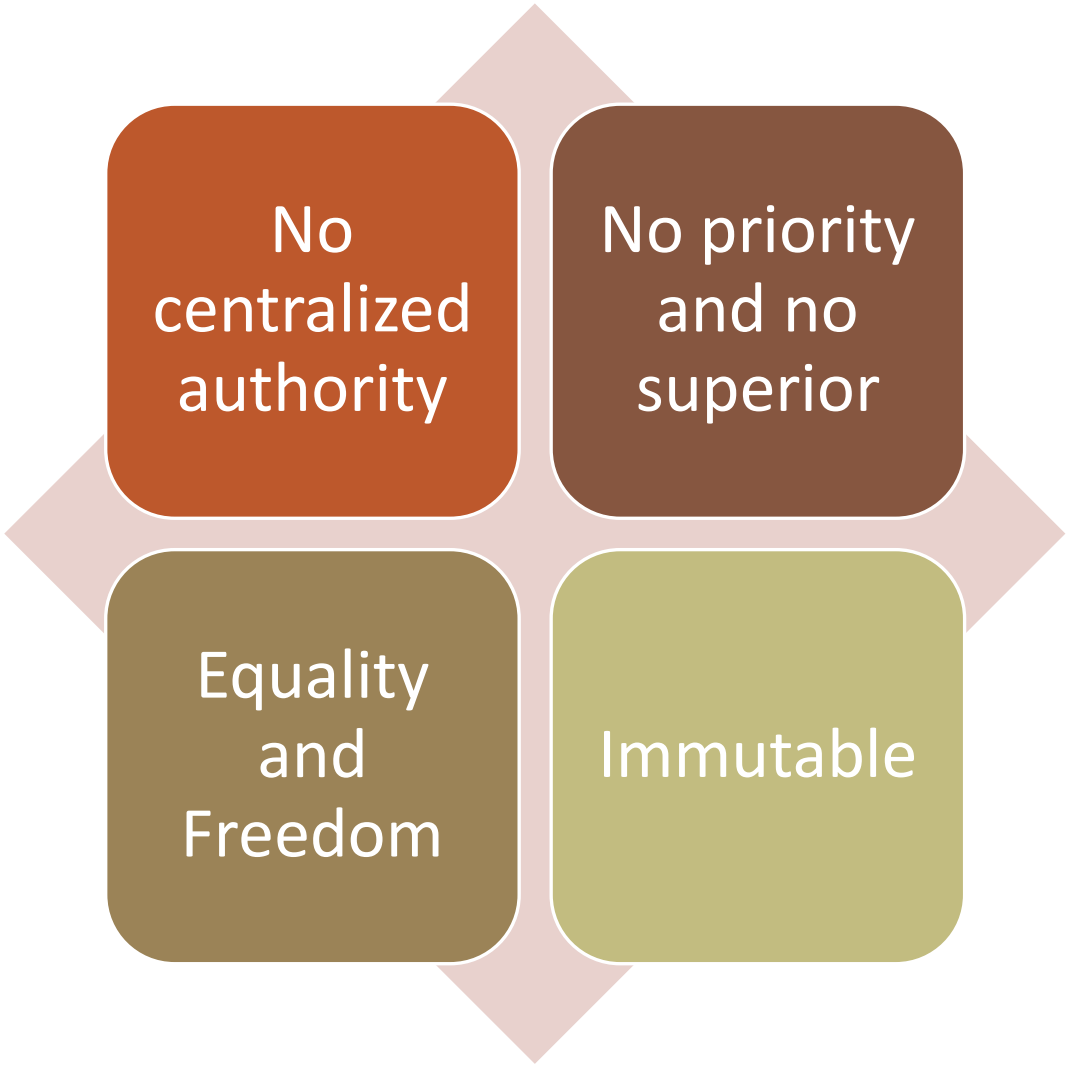
DeFi Is Transforming Industry Value Propositions: Example 1 — Sports



Gartner's view and wish

DeFi Is Transforming Industry Value Propositions: Example 2 — Property





Belief and Rationale behind Distributed Ledger Technology

Vitalik Buterin States “Centralized Anything is Evil by Default” …

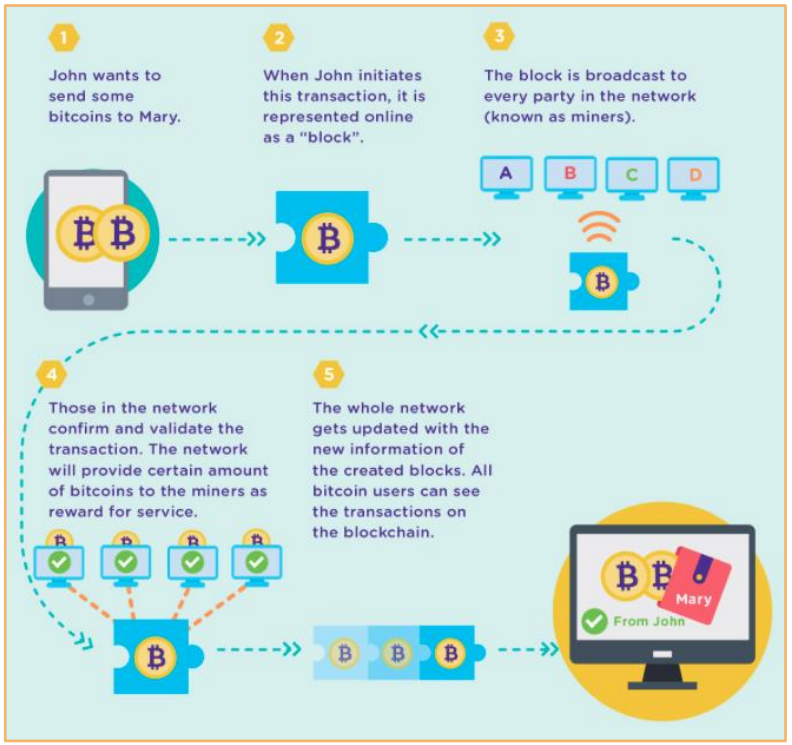
Let’s start with Bitcoin…

What is Blockchain (Starts from Bitcoin)

Blockchain technology is the underlying foundation of “cryptocurrencies”.

Every single transaction that takes place in bitcoin network is recorded in a shared public ledger.

Whenever a new block of transactions is created, it is added to the blockchain.



Bitcoin exchange status (2022)

Bitcoin Network Satoshi Nakamoto

A pseudonymous software developer proposed bitcoin in 2008..

To exchange without the need of any central authority and transfer in more secure, verifiable and immutable way

Bitcoin is designed for decentralized, avoid double-spending, limited supply, anonymous, immutable

Keywords and terms

Cryptography

Hash, Hash Chain

Digital Signature

Immutable

Ledger, Centralized Ledger, Distributed Ledger

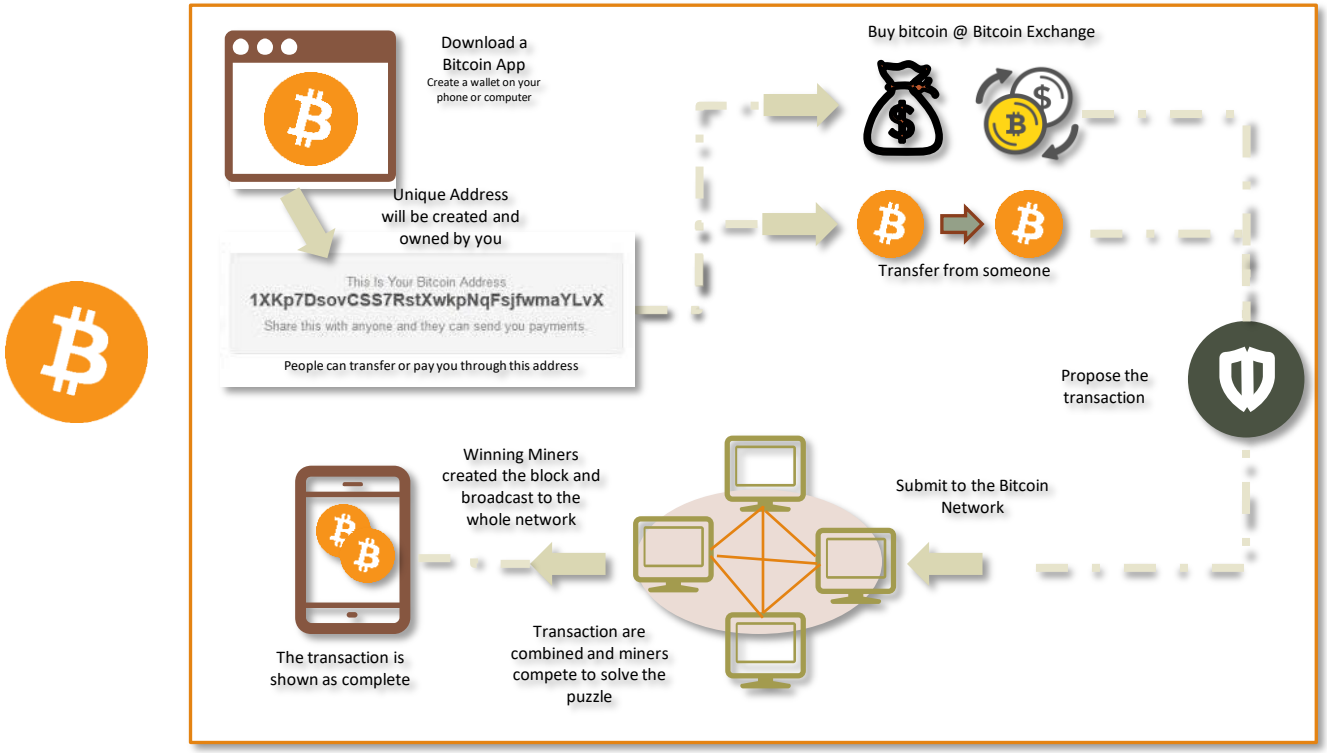
Distributed Programming

Private vs Public, Permission Blockchain vs Permissionless Blockchain

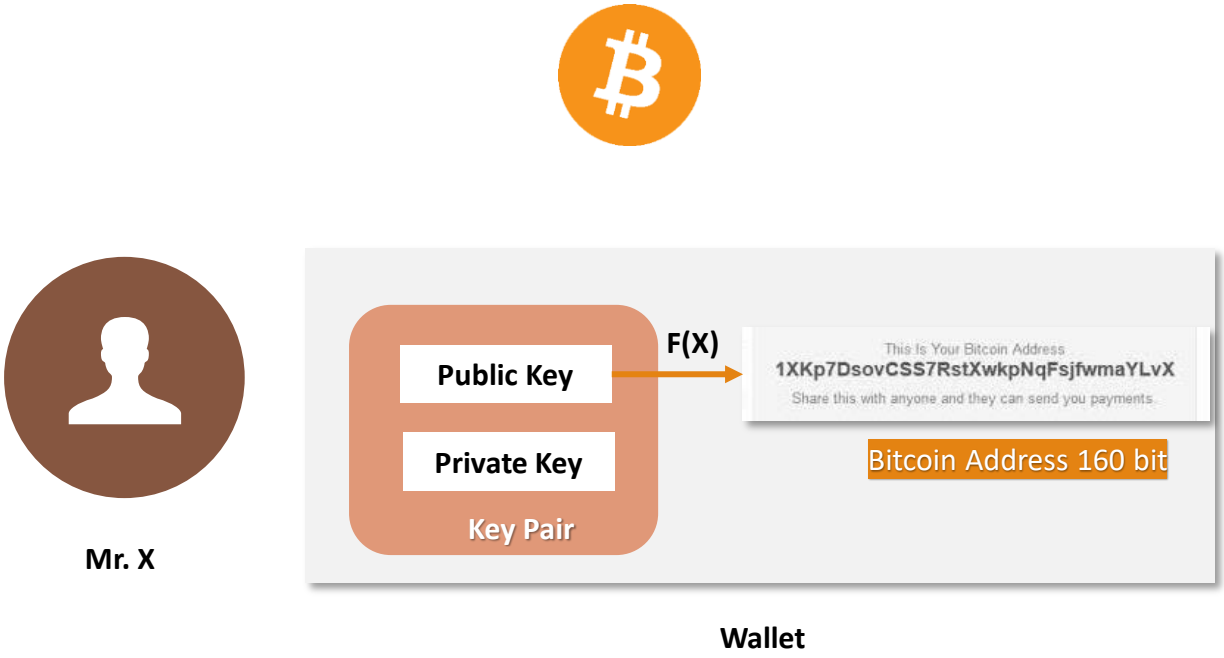
Consensus, Consensus Algorithm

Smart Contract

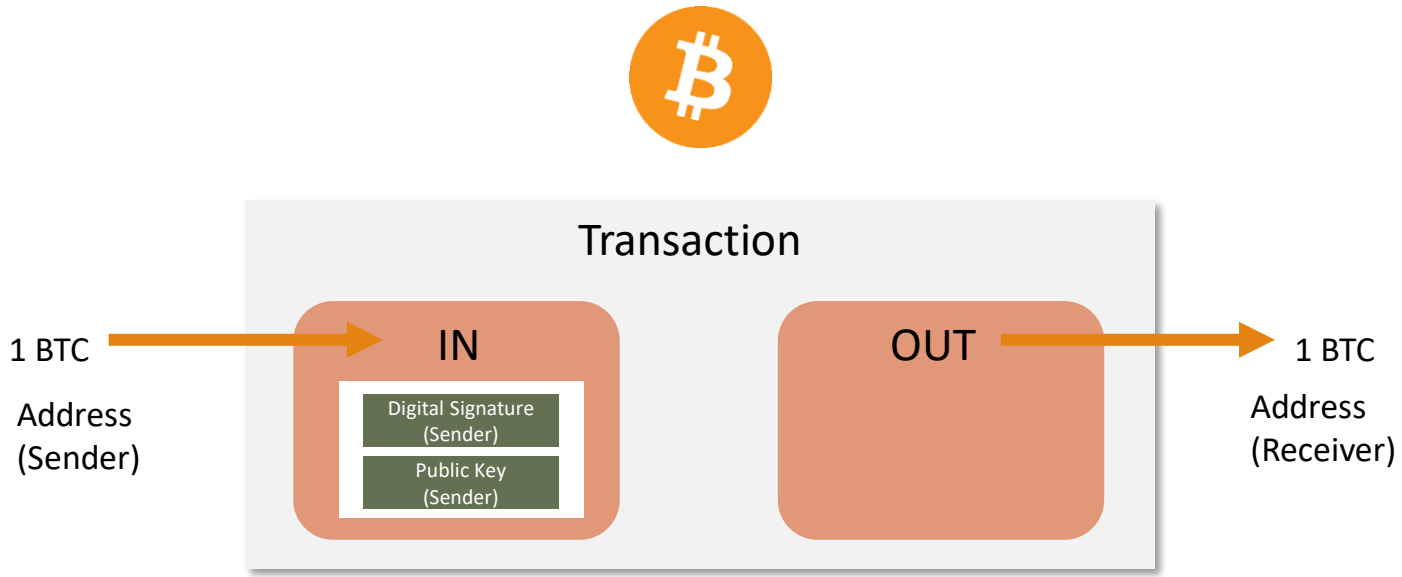
Currency, Cryptocurrency, Digital Currency



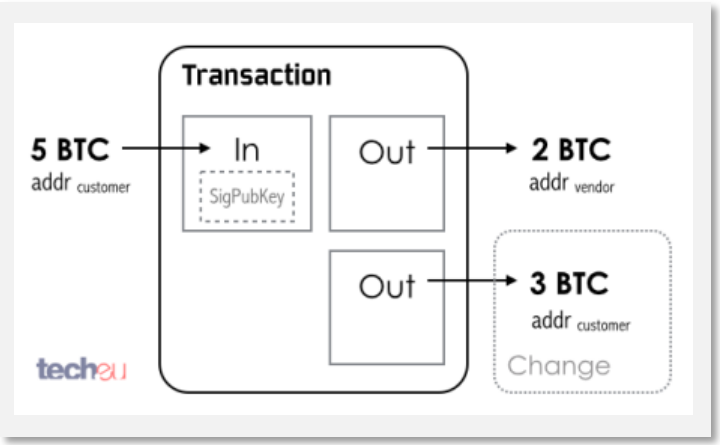
PKI and Address

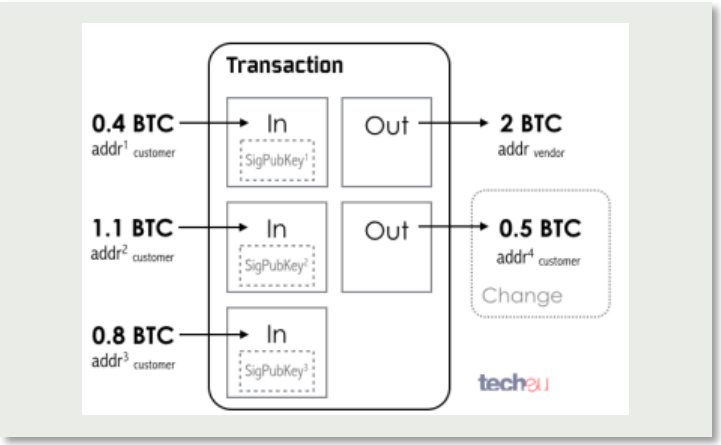


Transaction Block

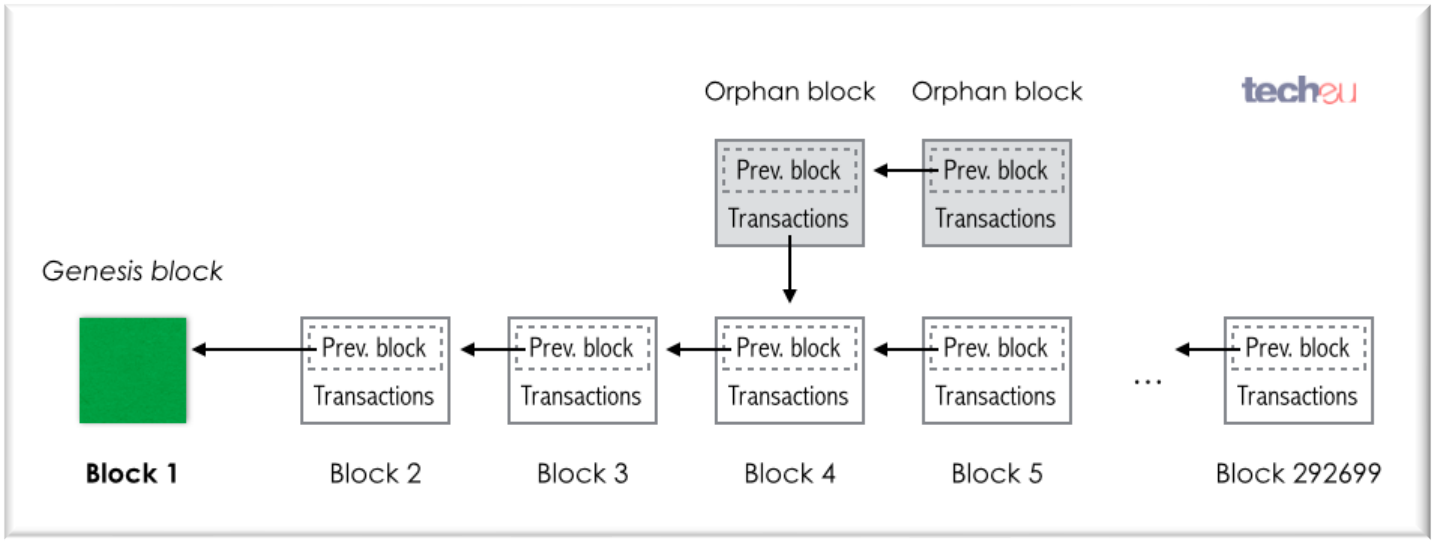


Multiple transaction

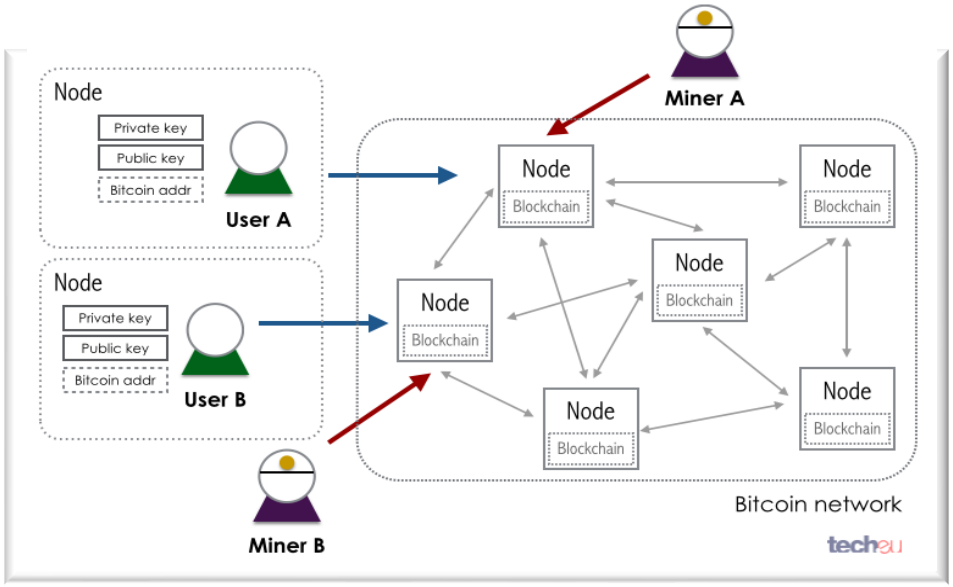




Blockchain



Bitcoin Network

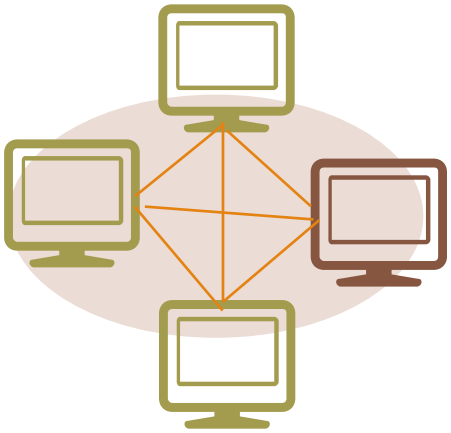


Miners – Mining Node

In Bitcoin network, data is shared among nodes.

When a new node added and connected to the Bitcoin network, it would download the transactions.

Now, the whole block of transaction is about 128G in size.

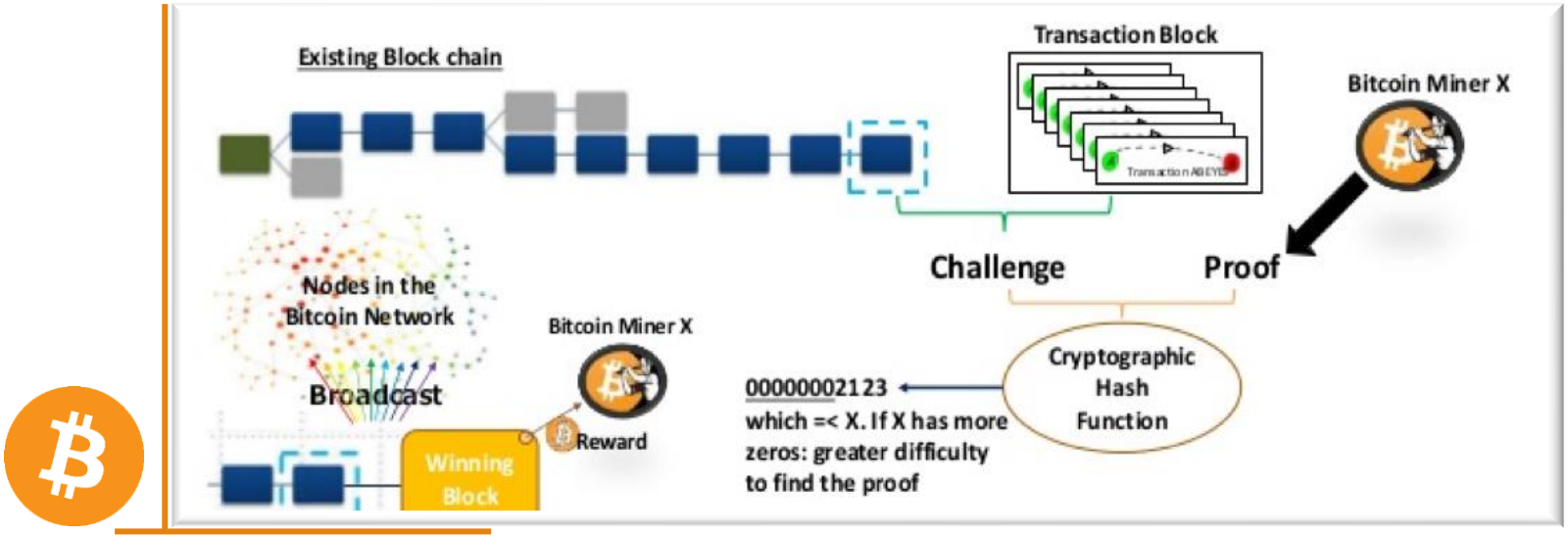


Some nodes are mining nodes and they perform the following:

1. Group the outstanding txn into block
2. Solving a complex math puzzle as part of the bitcoin program.
3. The miner who solve the problem first, include the answer into the block and announce to the network.
4. The winner will be rewarded with new bitcoin.

https://charts.bitcoin.com/bch/chart/blockchain-size

What is the math puzzle?

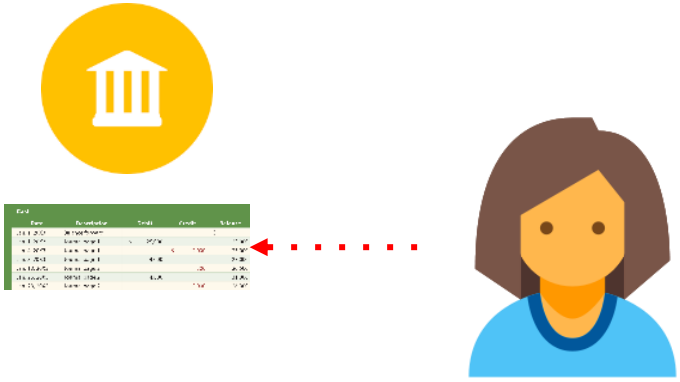


What is the impact to the world?

Immutable Distributed Ledger?

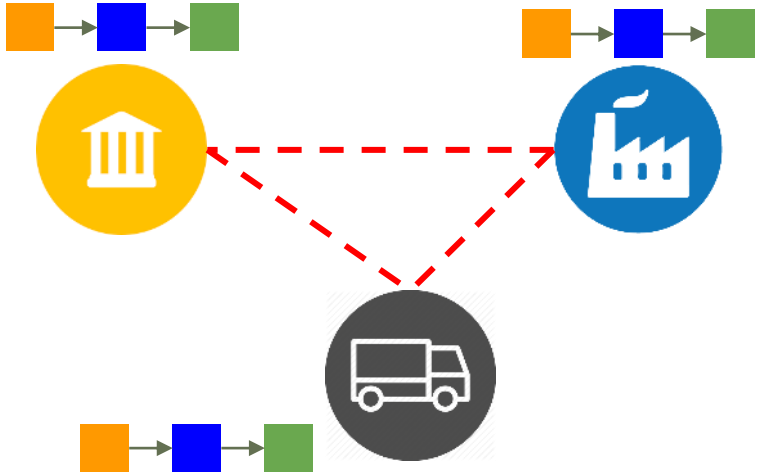
TRADITIONAL LEDGERS

CENTRALIZED...

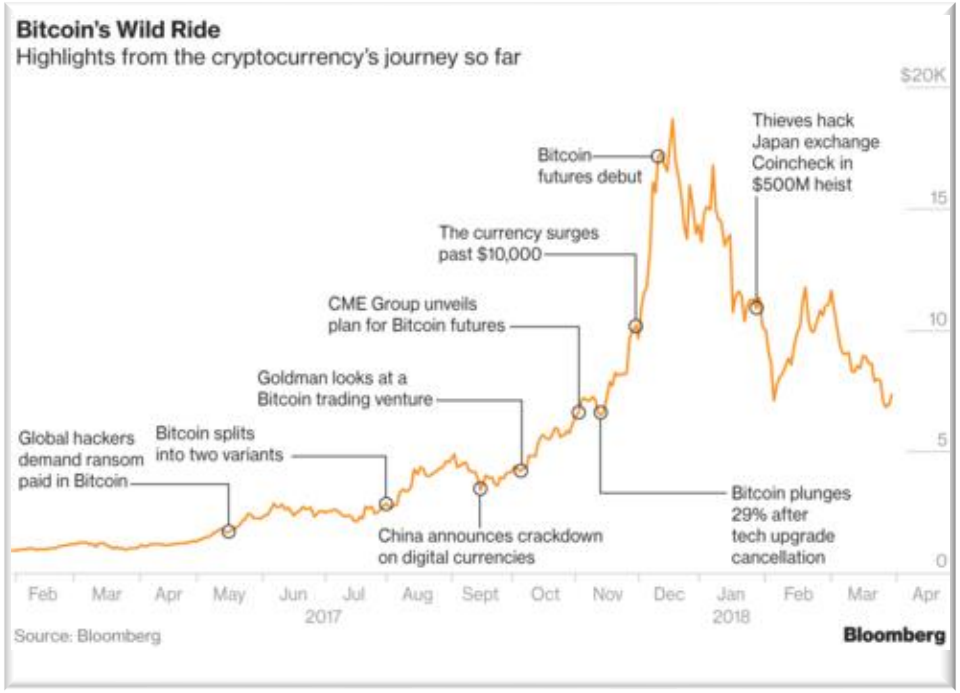


SHARED LEDGERS

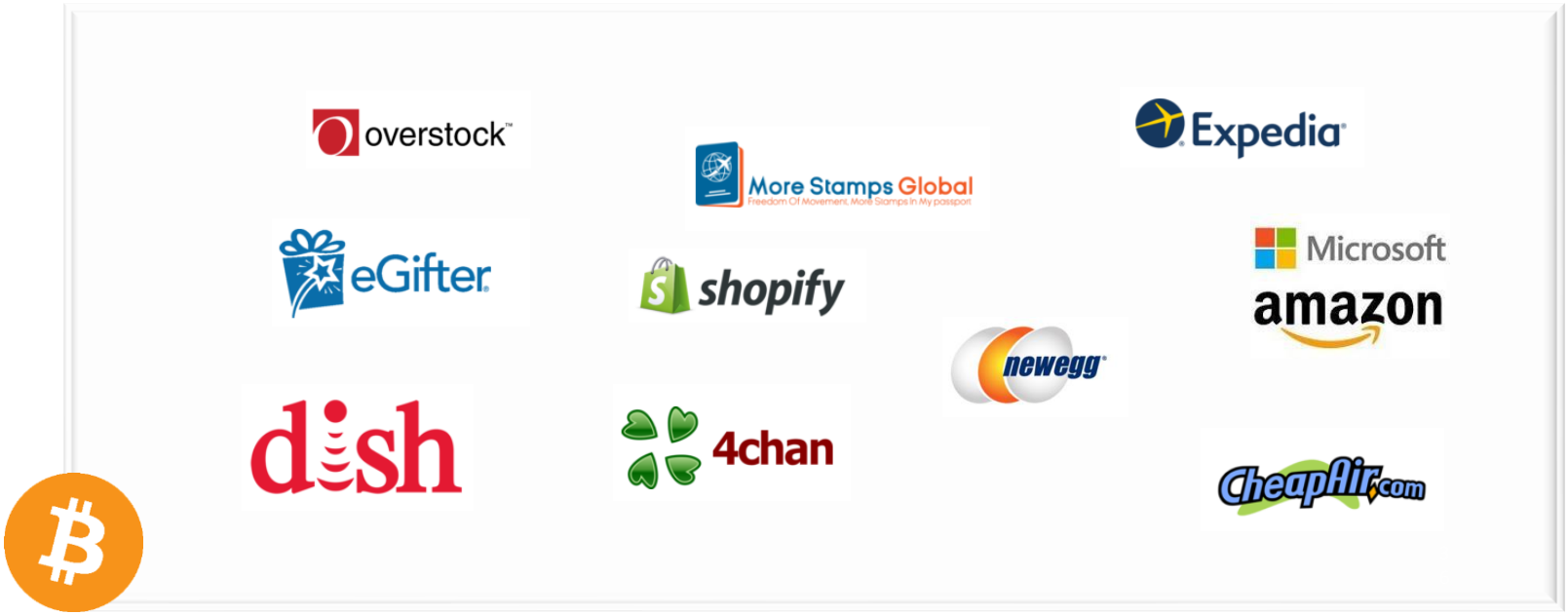
IMMUTABLE?



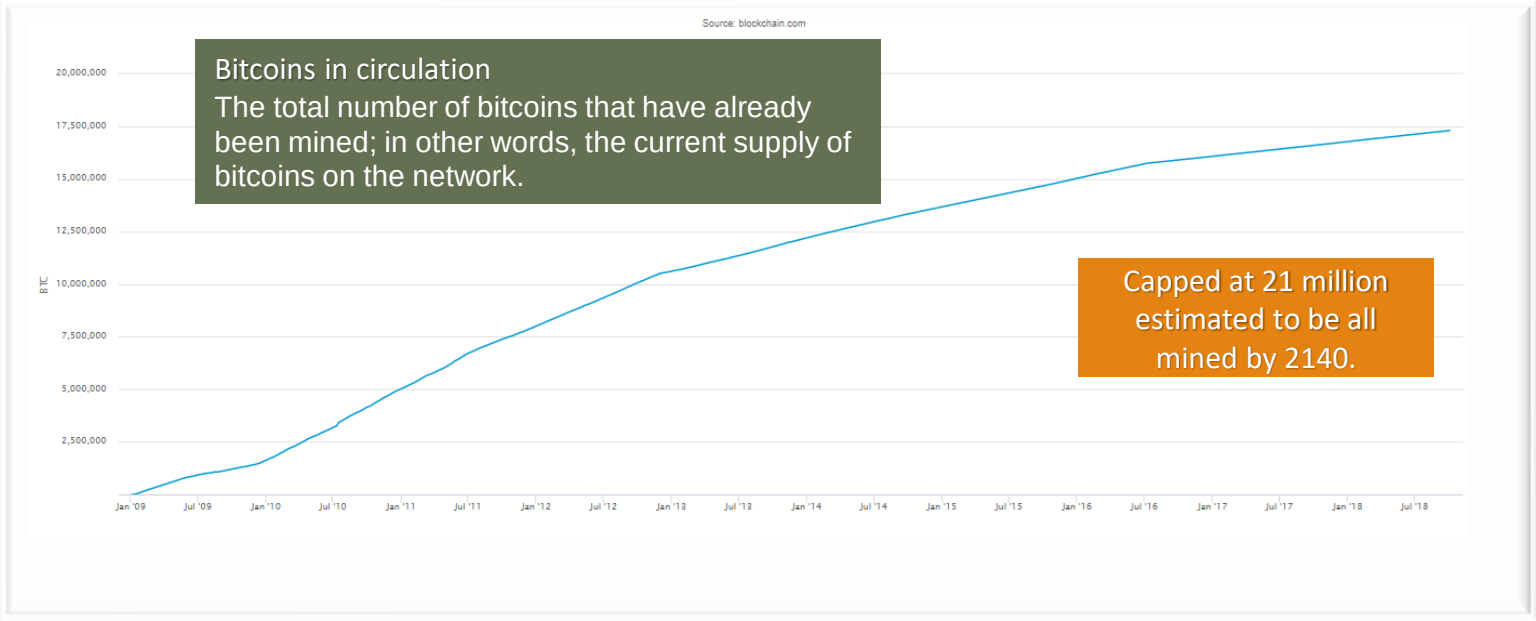
A digital money market – cryptocurrency independent to any central bank or



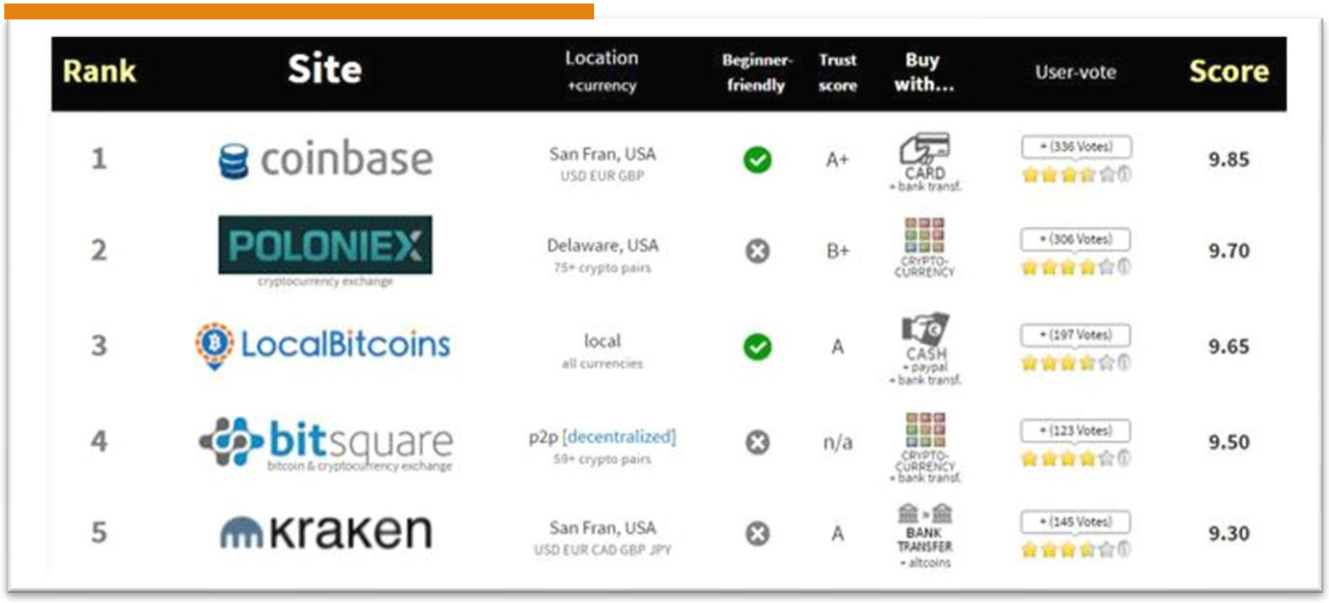
E-Commerce starts to accept Bitcoin



Bitcoin is scarce resource with limited supply…



Bitcoin can be traded in different Bitcoin Exchanges with charges



Rank	Site	Location +currency	Beginner-friendly	Trust score	Buy with...	User-vote	Score
1	coinbase	San Fran, USA USD EUR GBP	✓	A+	CARD + bank transf.	+ (336 Votes)	9.85
2	POLONIEX cryptocurrency exchange	Delaware, USA 75+ crypto pairs	✗	B+	CRYPTO-CURRENCY	+ (306 Votes)	9.70
3	LocalBitcoins	local all currencies	✓	A	CASH + paypal + bank transf.	+ (197 Votes)	9.65
4	bitsquare bitcoin & cryptocurrency exchange	p2p [decentralized] 50+ crypto pairs	✗	n/a	CRYPTO-CURRENCY + bank transf.	+ (123 Votes)	9.50
5	kraken	San Fran, USA USD EUR CAD GBP JPY	✗	A	BANK TRANSFER + altcoins	+ (145 Votes)	9.30

What are the risks?

Key risks of Bitcoin

High volatility – unstable to be accepted as currency

Government **regulations** – can be classified as illegal by government

Competition from other cryptocurrency which offer faster transaction

Security - expose to hackers without any asset/company to back

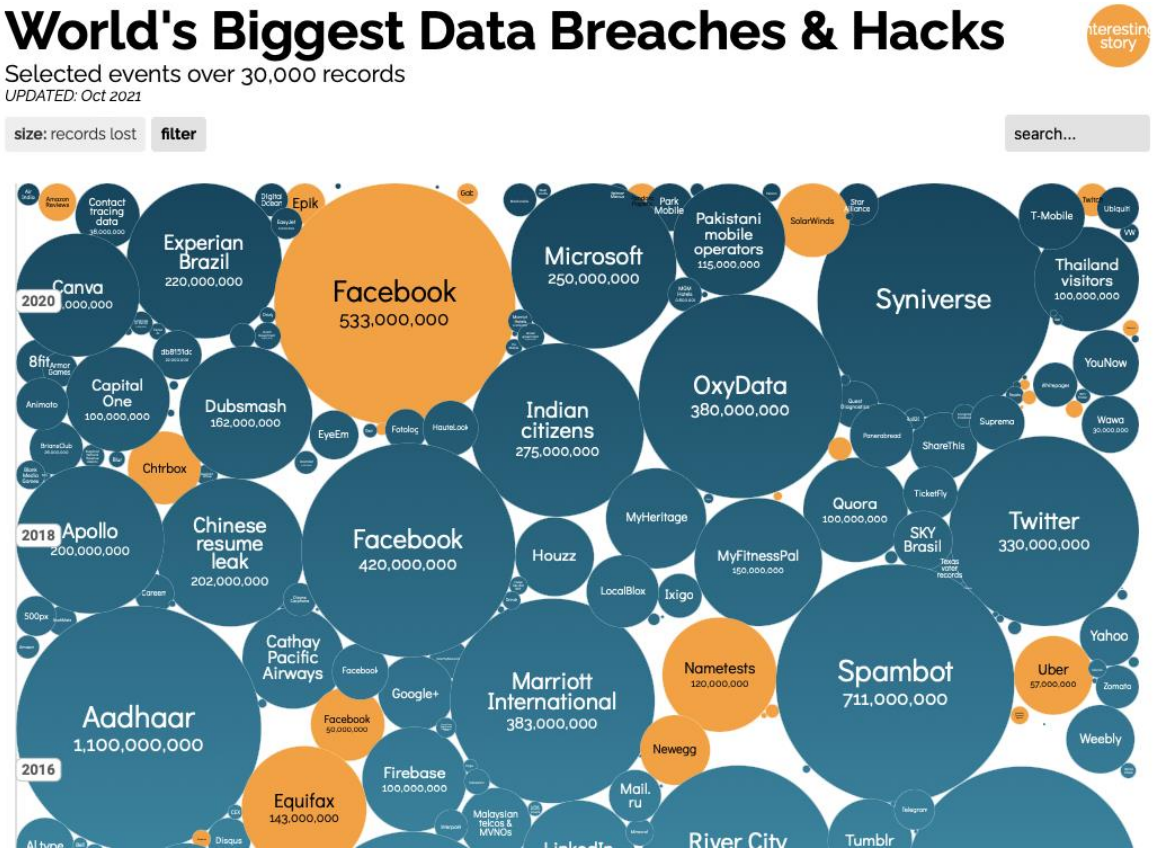
No **Safety mechanism** – private key is the only way to protect your wallet

Basics of Cyber-Security

Crisis ahead of IT world

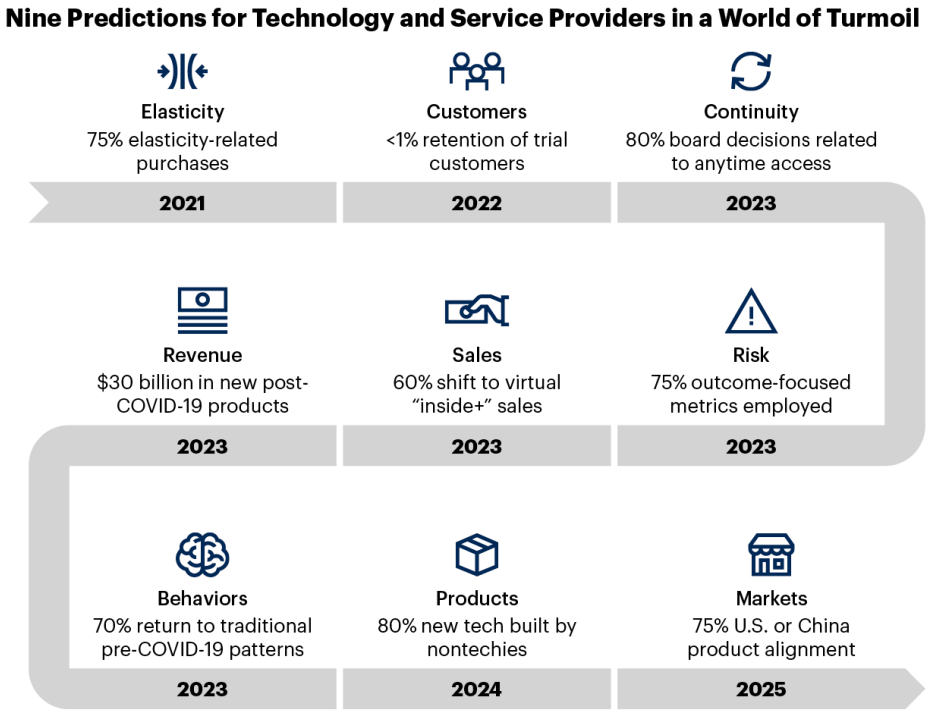
cpr.mtninet.com

World's Biggest Data



https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

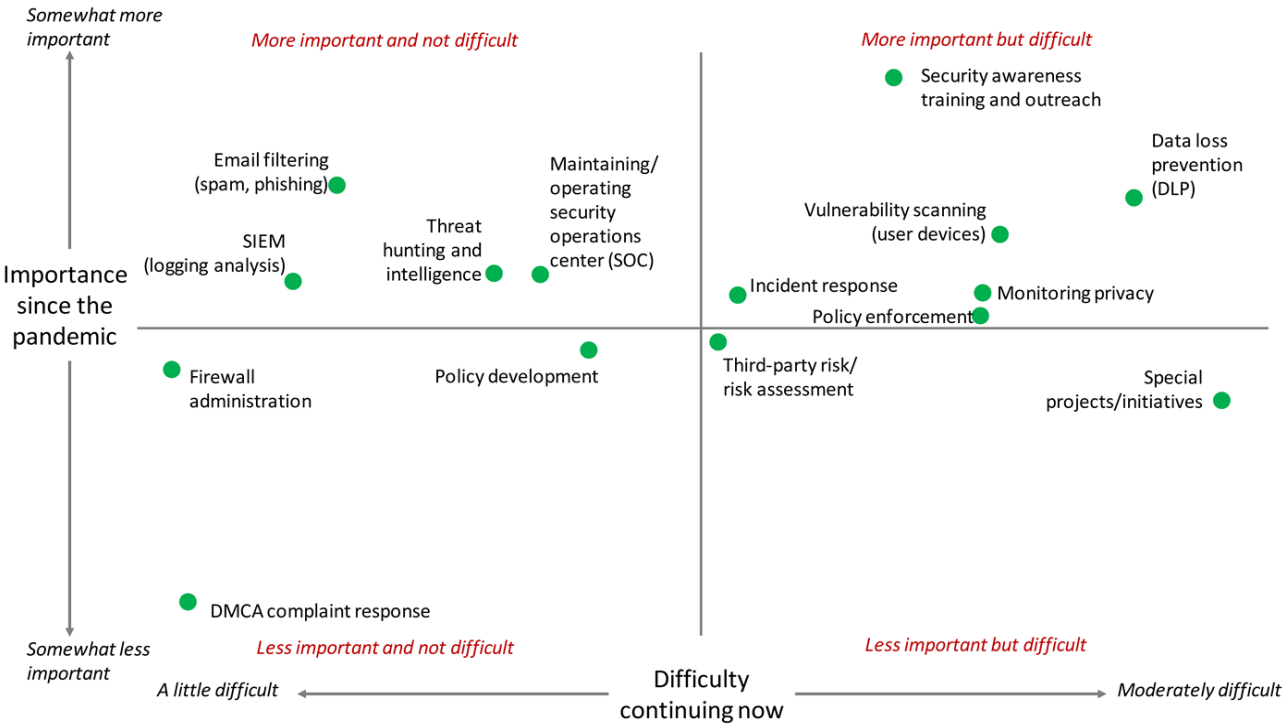
What happened this Year?



Source: Gartner
725599_C

Nine Predictions for Technology and Service Providers in a World of Turmoil
Published 7 August 2020 - ID G00725599

COVID-19 and Information Security



Threats and Opportunity in Cybersecurity (Post-COVID-19)

Key words: Massive Remote Voluntary actions only

Threats

- More phishing and human-facing social engineering tactics
- More destructive ransomware tactics
- More business email compromise
- More account identity theft
- More attack at remote services

The Distributed Workplace of the Future Is Now
Published 17 September 2020 - ID G00726412

Opportunity

- Increase use of MFA and modern authentication solution
- Increase eKYC, eIDv usage
- Increase Cloud Computing and Cloud Security requirement
- Increase automation security
- Enhance endpoint protection requirement
- Use of Zero Trust network access

How to Respond to the 2020 Threat Landscape
Published 17 June 2020 - ID G00719273

Robbers steal more than HK$3 million in bitcoin from trader (Jan 2021)

Robbers steal more than HK$3 million in bitcoin from trader, escape after kicking him out of ca... SUBSCRIBE

The victim claimed he spoke to two of the suspects online and agreed to meet them to make the bitcoin transaction in person. Photo: Reuters

A gang of robbers stole bitcoin valued at more than HK$3 million from a trader on Monday, luring him to meet for the transaction and then kicking him out of the car on a Hong Kong hillside.

The robbers fled with HK$3 million (US$387,000) in cash that they had pretended to pay their victim, but took back later when 15 bitcoin worth about HK$235,000 each were transferred.

The incident, which has sparked a citywide manhunt, took place after two non-Chinese men arrived in a white car and picked up the victim – a 37-year-old man – outside a hotel in North Point just before 8pm.

Hong Kong cracks down on crypto trading in bid to tackle fraud

3 Nov 2020

Another police source said the robbery did not involve any weapons and no one was injured. The six perpetrators fled in the two cars.

The case came to light at around 8.48pm when the victim walked for abou five minutes and stopped a police officer to seek help at a nearby housing estate.

New anti-money-laundering regulations should exclude bitcoin ATMs: industry body

24 Dec 2020

Officers scouted the area, but no arrests had been made as of 11am on Tuesday. Police said the six robbers, of non-Chinese ethnicity, were aged around 30.

Officers from the Eastern district crime squad are handling the case.

In the first 10 months of 2020, police handled 242 reports of robbery across the city, up 103 per cent from 119 cases over the same period in 2019. There were 210 robbery cases in the whole of 2019, and 147 such reports in 2018.

Bitcoin trader robbed of $523k in cash (Jul 2021)

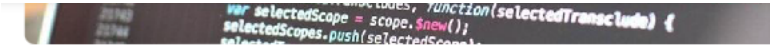
Bitcoin trader robbed of $523k in cash when 'sellers' in Hong Kong show up with knife

JULY 29, 2021 PUBLISHED AT 10:08 AM
By DANNY MOK | SOUTH CHINA MORNING POST

The 39-year-old trader from South Korea arrived at Astoria Building on Ashley Road in Tsim Sha Tsui for the exchange at about 6.20pm. He was approached by four men, one of whom attacked him with the knife.

The criminals snatched a bag he was carrying with about HK$3.29 million inside and fled. The trader asked a friend to call police and officers searched the area but failed to locate the suspects.

Hong Kong crypto crime rate surges as China sees a fall (Aug 2021)



According to blockchain forensics platform Chainalysis, criminal cryptocurrency activities on the Chinese darknet have fallen.

However, due to geopolitical turmoil, Hong Kong's crypto crime rate has risen alarmingly.

The Chainalysis report shows that, in the period from April 2019 and June 2021, Chinese crypto addresses sent more than $2.2 billion worth of cryptocurrencies to addresses connected with scams and darknet markets, with more than two billion moving in the opposite direction.

That volume, say Chainalysis, has since dropped significantly.

Illicit transaction volume

"While China remains one of the top-ranked countries for illicit transaction volume, it used to beat all others by a wide margin, suggesting that cryptocurrency-related crime in the country has fallen," said a Chainalysis spokesperson.

Chinese police recently arrested more than 1,100 people suspected of using cryptocurrencies to launder illegal proceeds from telephone and Internet scams.

Crypto crimes surge to record levels in Hong Kong

In Hong Kong, however, criminal activity involving cryptocurrency looks to be reaching record levels this year. According to police, there are three main categories of crypto-related crime: money laundering, investment scams and face-to-face transaction theft.

A report by the crypto news outlet Forkast says that around 500 crypto-crime cases have been registered in the first half of 2021, while the year's losses amounted to 214 million Hong Kong dollars ($27.5 million) – almost double the total from last year.

The Hong Kong government attributed the rise to the growing popularity of crypto investing in this special administrative region. Also, it clams, the COVID-19 pandemic forced people to spend more time online, allowing more opportunities to lure individuals into illicit actions.

crypto-related crime: money laundering, investment scams and face-to-face transaction theft.

Bitcoin Core Dev Loses At Least $3.6 Million in BTC to Hack (Jan 2023)

Luke Dashjr, who claims to be "the longest contributing Bitcoin Core developer," revealed that an unknown hacker had raided "basically all" of his Bitcoin holdings on New Year's Day.

The total sum of Bitcoin stolen is unknown, but in a Twitter thread, Dashjr tracked "some of it" to a wallet address that received a little under 217 Bitcoin, or about $3.6 million at today's price.

Dashjr blamed the hack of his Bitcoin wallet on a compromised PGP (Pretty Good Privacy) key and later, in a Reddit discussion, he stated that the attacker's IP came from a ColoCrossing server. He was at a loss to explain how his cold wallets were compromised, but he said the last time he'd accessed them was in September.

Cold Wallet being compromised

According to the information shared by Luke Dashjr, the hacker used the CoinJoin privacy method to move the stolen funds to another address. With this tool, it is possible to mix the inputs and outputs of thousands of transactions so that it becomes impossible to identify and track the participants in each transaction.

Earlier in November 2022, he had tweeted about his server being compromised by some "new malware/backdoors on the system."

He said, "PSA: My server was accessed this morning by an unknown person. Full analysis in progress, but take extra care that you PGP-verified any downloads."

Full details still not known

10大跨鏈橋被駭紀錄！遭竊總額逾19億美元，15.5億賠付或追回 (Oct 2022)

區塊鏈世界已有上百條公鏈，然而因為缺乏主流資產，需要使用跨鏈橋從以太坊等公鏈上獲取資產。近期，DeFi 安全事故頻發，跨鏈橋資金量大且頻繁遭到攻擊。下文中，PANews 盤點了過去跨鏈橋中比較大的 10 次攻擊過程，所有開發團隊都需安全警鐘長鳴。相對而言，開發團隊背景越好越有資本的跨鏈橋在出現安全事故後，確實更容易找回資產或者由項目方進行賠付，因此用戶選擇有實力的跨鏈橋會更加穩妥。

PANews www.PANewsLab.com

跨链桥攻击及赔付情况

时间	跨链桥	被盗金额	赔付情况
2021/7/11	ChainSwap	800万美元	重新发币
2021/8/10	Poly Network	6.1亿美元	已找回
2022/1/18	Multichain	600万美元	已赔付
2022/1/28	Qbridge	8000万美元	仅赔付2%
2022/2/3	Wormhole	3.2亿美元	已赔付
2022/2/6	Meter Passport	420万美元	用未来收益赔付
2022/3/29	Ronin Network	6.2亿美元	已赔付
2022/6/7	EvoDeFi	预计上千万美元	未赔付
2022/6/24	Horizon	1亿美元	处理中
2022/8/2	Nomad	1.9亿美元	处理中

来源：PANews总结 统计日期：2022/8/03

PANews 扫码下载应用 阅读原文

BNB Chain遭攻擊超5億美元：時間軸梳理與原因解析

by wublockchain — 2022-10-07 in 犯罪 AA

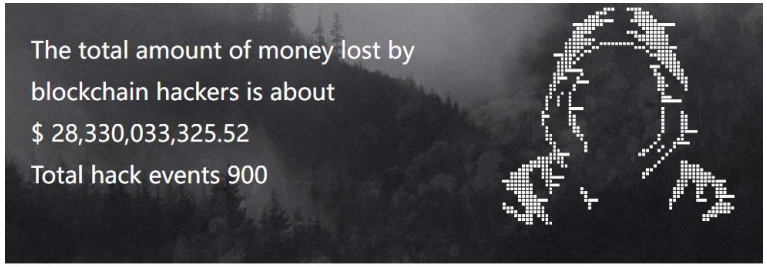
Network	Token Amount	Amount($)	Borrowed($)
Ethereum	23,975.01 ETH, 9,797.21 WETH, 4,778,091.93 USDT(blacklisted), 2,711,280.17 USDC	53,283,623 (4,778,091.93 Frozen)	
Polygon	399,895.34 USDC	399,895.34	
Fantom	79.55 FTM, 21,285,045.41 USDC, 19,000,003.81 gfUSDT(Gesit Lending Supplied), 10,683,368.93 gUSDC(Gesit Lending Supplied), 7,999,999 fUSDT	58,968,432 (29,683,374.51 Supplied)	Gesit: 10,194,204
Avalanche C-Chain	6.99 AVAX, 1,729,320.75 USDT(blacklisted), 7,898,761.6 USDT(Trader Joe Lending Supplied)	9,628,202 (1,729,320.75 Frozen, 7,898,761.68 Supplied)	Trader Joe: 6,297,430
Arbitrum	1,457.24 ETH, 2,000,000 USDT	3,973,998	
Optimism	1,102,163.81 USDC	1,102,163.81	
Total		127,356,314.15 (6,507,412.68 Frozen, 37,582,136.19 Supplied)	16,491,634

(BNB Bridge Hack Token Stolen Table)

分析師 @samczsun 發文解釋了駭客利用 Binance Bridge 盜取 BNB 的方式。攻擊者經過兩次分別盜取 100 萬 BNB，但使用的高度均為110217401，遠低於正常高度。

此外，攻擊者提交的證明短於合法證明，可見攻擊者偽造了該特定塊的證明。具體方法是在當 COMPUTEHASH 函數生成根 hash 時，增添一個新的葉節點，然後創造一個空白內部節點以滿足證明者，在找出與內部節點匹配的跟 hash 後提前退出。目前為止，通過這種方式生成的偽驗證只有兩條。

Lost by Blockchain Hackers (2022)



All Blockchain Exchange Wallet ETH Ecosystem BSC Ecosystem Tron Ecosystem EOS Ecosystem Polygon Ecosystem
HECO Ecosystem Fantom Ecosystem Solana Ecosystem Avalanche Ecosystem Polkadot Ecosystem NFT Bridge Other

48 hack event(s)

Hacked target: Loopring 2022-11-05

Description of the event: Ethereum L2 protocol Loopring tweeted that it was hit by a large-scale DDoS attack. While the funds were not at risk, the service was down for 11 hours. Currently, domain access on the mobile app side has been reconfigured and the Loopring wallet service has been restored.

Amount of loss: - **Attack method:** DDos attack

View Reference Sources

Hacked target: Dogechain 2022-09-11

Description of the event: In a tweet, @0xCrumbs disclosed that Dogechain was hacked yesterday, and the attackers exploited the vulnerability to mint 9.7 million $Doge (about $600,000) and transfer $316,000 through a cross-chain bridge. Currently 3 million remain in the starting wallet, in addition to $100,000 worth of USDC/ETH. Therefore, @0xCrumbs believes that yesterday's Dogechain maintenance was caused by the attack. SlowMist also tweeted that the attackers used Anyswap to bridge funds to the BSC and ETH chains, which were then transferred to Binance. But Dogechain officials tweeted that no funds were lost during the maintenance period.

Amount of loss: $ 600,000 **Attack method:** Contract vulnerabilities

View Reference Sources

Hacked target: Sui 2022-08-27

Description of the event: Public chain project Sui tweeted that its Discord server had been hacked, and asked users not to click on any links posted on the Discord server in the past 8 hours. According to some replies to the tweet, some users have already lost money by clicking on links posted by the hackers on Sui Discod.

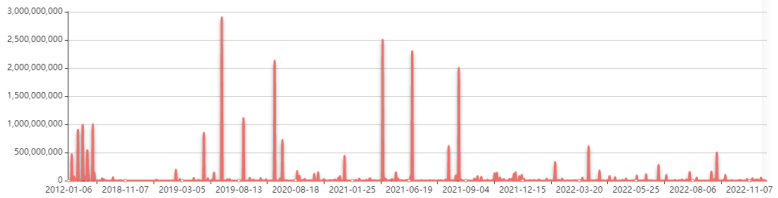
Amount of loss: - **Attack method:** Discord was hacked

View Reference Sources

[SlowMist Hacked Statistical]:

Total hack event(s) 899 ;

The total amount of money lost by blockchain hackers is about $ 28,330,033,325.52 ;



Category	Hack event(s)	Amount of loss ($)
Blockchain	48	206,505,567.00
Exchange	109	10,289,201,175.39
Wallet	31	299,741,253.59
ETH Ecosystem	169	2,845,979,975.56
BSC Ecosystem	124	1,422,271,935.55
Tron Ecosystem	23	11,224,334.36
EOS Ecosystem	119	25,927,302.55
Polygon Ecosystem	11	55,185,949.00
HECO Ecosystem	3	8,064,533.00
Fantom Ecosystem	11	86,592,814.00
Solana Ecosystem	13	202,741,994.22
Avalanche Ecosystem	7	118,673,000.00
Polkadot Ecosystem	9	61,545,641.00
NFT	69	190,055,307.00
Bridge	29	1,867,656,543.30
Other	124	10,638,666,000.00

Crypto Exchange Fraud (2022)

Police arrested two men in crypto exchange AAX-related case

Local | 24 Dec 2022 3:56 pm

Police in Hong Kong arrested two men on Friday in a case related to cryptocurrency exchange AAX and has frozen the company's bank account.

One of the people arrested "manages the platform," Lee Wai-chung, an acting chief inspector at the commercial crime bureau, said at a press conference Friday.

Local media reported that one of the people was Thor Chan Chun-hung, the founder and ex-chief executive officer of AAX, and the other man was Leung Ho-ming, the director and chief executive officer of Vico Capital Ltd.

Police's public relations department declined to confirm the identity of the arrested persons. Thor Chan didn't immediately reply to a written request for comment sent on Saturday.

Cryptocurrency exchange AAX suspended withdrawals in November, citing a glitch in a system upgrade. Police's investigation found that there were liquidity issues at the company, but the mastermind and the people arrested "used data maintenance as an excuse to prevent users from withdrawing fund," Lee said.

The case involves HK$98 million of total reported loss, according to a press release from the police.

Cryptocurrency exchange AAX suspended withdrawals in November, citing a glitch in a system upgrade. Police's investigation found that there were liquidity issues at the company, but the mastermind and the people arrested "used data maintenance as an excuse to prevent users from withdrawing fund," Lee said.

The case involves HK$98 million of total reported loss, according to a press release from the police. Bank accounts of AAX and the people who've been arrested have been frozen.

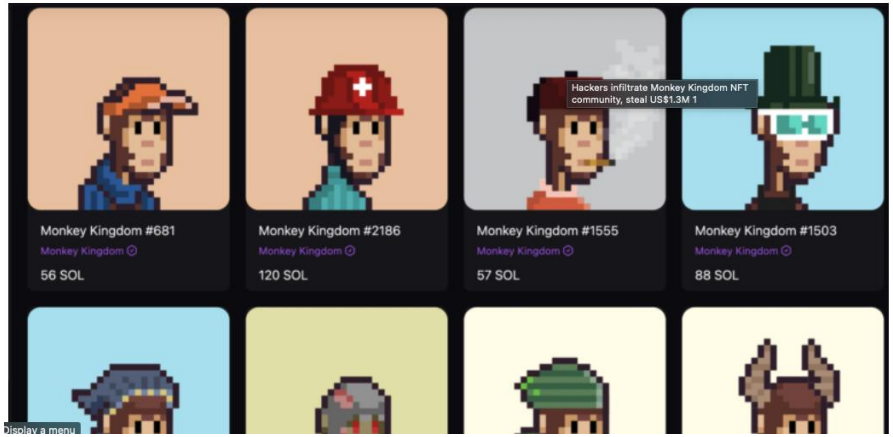
Hot Hong Kong NFT project Monkey Kingdom loses US$1.3 million in hack (Jan 22)

Hot Hong Kong NFT project Monkey Kingdom loses US$1.3 million in hack, exposing security concerns

- A hacker stole an administrator account of the project's group chat on Discord, a popular online instant messaging service
- Monkey Kingdom fraud is the latest in a series of scams seen in the space in recent months as the popularity around NFT reaches fever pitch

Hackers infiltrate Monkey Kingdom NFT community, steal US$1.3M

Hackers scam 7,000 Solana, or US$1.3 million, from would-be buyers of a new NFT collection of the Monkey Kingdom project.



Popular non-fungible token (NFT) project Monkey Kingdom, founded by entrepreneurs in Hong Kong and promoted by celebrities such as JJ Lin and Steve Aoki, had its group chat hacked on Tuesday, allowing a cyber thief to steal nearly US$1.3 million worth of cryptocurrencies with a phishing link.

A hacker stole an administrator account of the project's group chat on Discord, a popular online instant messaging service, and posted a phishing link in the group chat on Tuesday, just as the project kicked off a new sale in earnest. Buyers lost more than 7,000 Solana, a popular cryptocurrency, to the scam, which amounts to nearly US$1.3 million.

Phishing is a common form of online fraud often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. It is now being used to breach access to users' cryptocurrency wallets.

Scammers steal $150K worth of crypto from NFT project with Discord hack (Dec 21)

The attacker posted a fraudulent message from the project's official channel

By Corin Faife | @corintxt | Dec 21, 2021, 4:23pm EST

SHARE

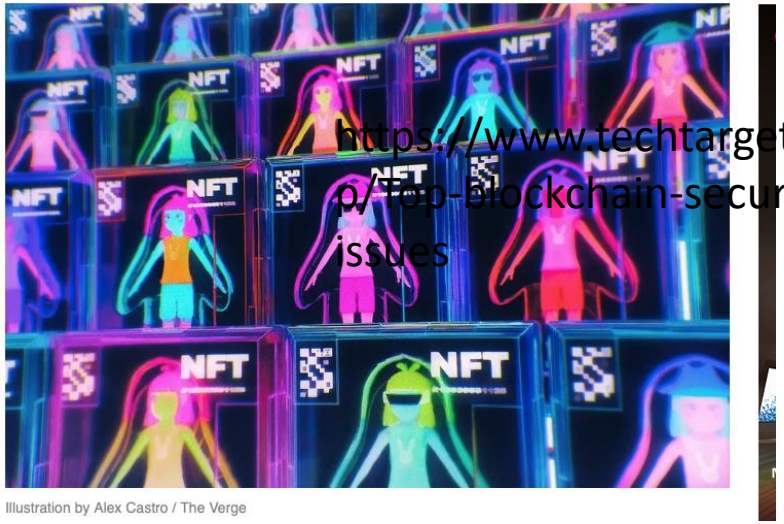


Illustration by Alex Castro / The Verge

https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues

Buyers hoping to get a limited-edition NFT from Fractal, a new marketplace for game item NFTs, were given an unpleasant and costly surprise on Tuesday morning when it was revealed that a link sent through the project's official Discord channel was a scam set up to steal crypto.

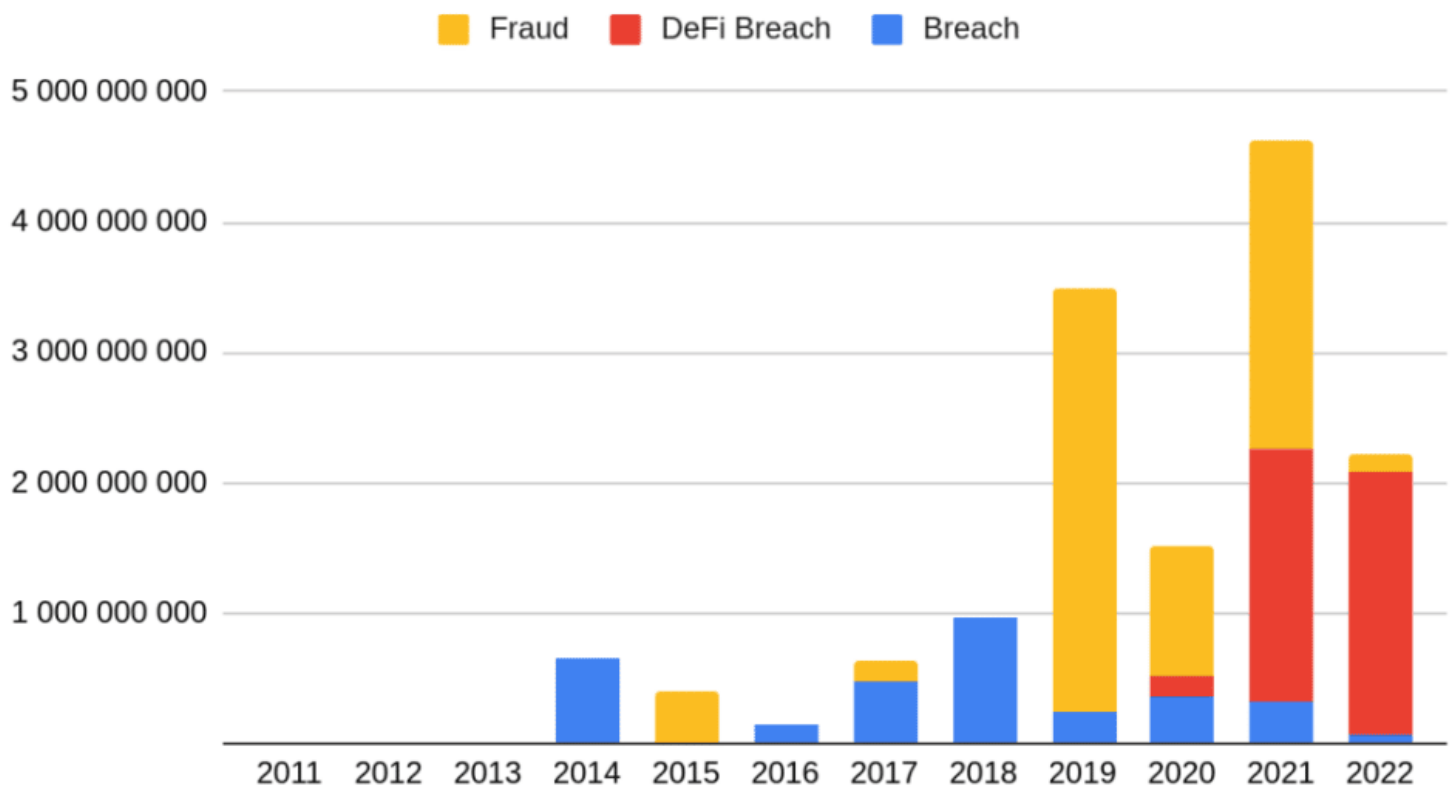
Users who followed the link and connected their crypto wallets, expecting to receive an NFT, instead found that their holdings of Solana (SOL) cryptocurrency were emptied and transferred to the scammer's account. An analysis posted on Medium by Tim Cotten, founder of another NFT gaming project, estimated the value of SOL stolen to be around $150,000.

Fractal is a startup project from Twitch co-founder Justin Kan specializing in the buying and selling of NFTs representing in-game assets. It was announced earlier in December and quickly amassed a following of more than 100,000 users through Discord — making it a target for the kind of scammers that have plagued NFT projects since the beginning.

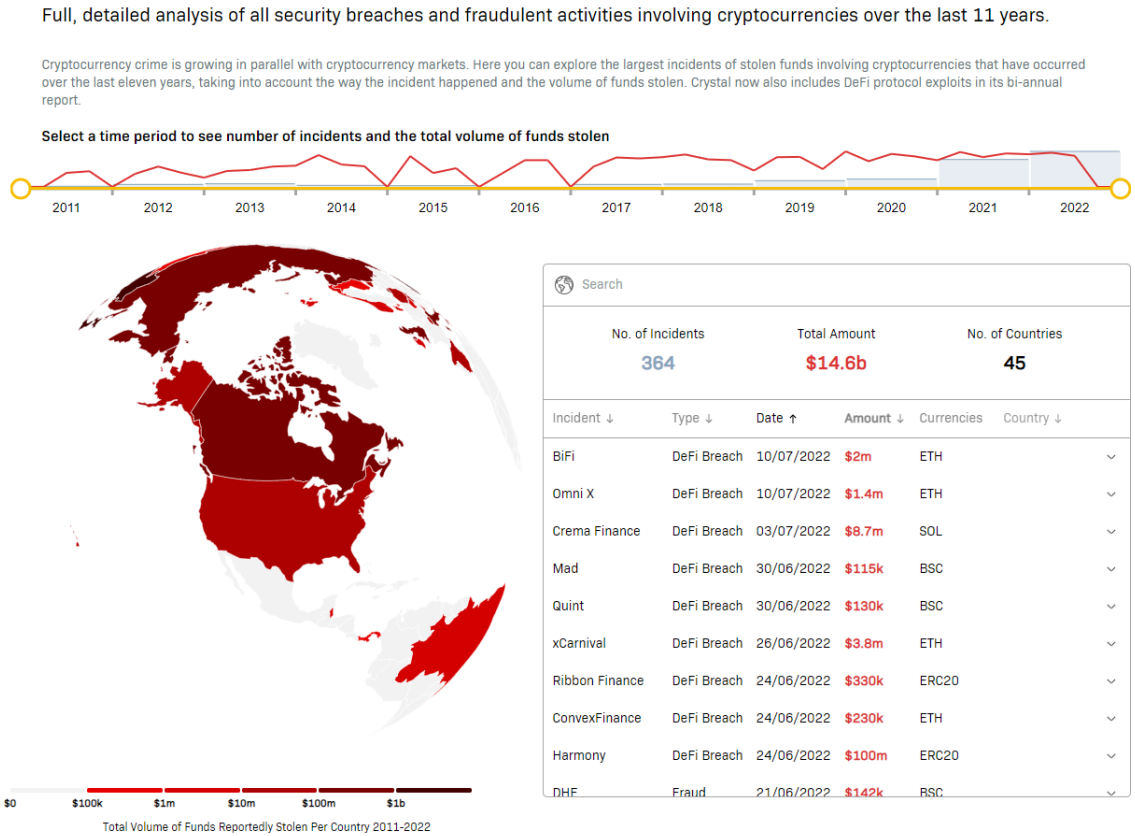
News reached Twitter when a tweet from Kan informed followers that the announcements bot on Fractal's Discord server had been hacked. Another tweet from the main Fractal Twitter account confirmed that a fraudulent link had been posted through the channel.

https://www.theverge.com/2021/12/21/22848840/scammers-steal-crypto-nft-project-fractal-discord-hack-solana

Top blockchain security attacks



Top blockchain security attacks



https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/

Top NFT incidents

Since the non-exchangeable token standard was first introduced, there have been 186 incidents, totalling USD 722.3 million in losses up till October 2022.

This data has been collected by means of Comparitech's service.

https://www.h-x.technology/blog/top-nft-incidents-of-all-time

The largest NFT thefts

1. Lympo — USD 18.7 million stolen. The NFT sports mining platform, a subsidiary of Animoca Brands, lost 165.2 million LMT tokens in hot wallet hacks in January 2022.

2. Farmers World — USD 15.7 million stolen. The WAX cryptocurrency network game, Farmers World, suffered a hack in November 2021, resulting in a loss of more than ¥100 million (USD 15.7 million). However, some experts speculate that the figure could be as high as ¥300 million.

3. Bored Ape Yacht Club — USD 13.7 million stolen. In April 2022, fraudsters stole tokens from the developers of the Bored Ape Yacht Club collection. The theft was committed by hacking into an Instagram account. Mutant Apes, Azuki, Otherside and CloneX tokens from the same developers also suffered from scammers, but in different incidents.\

4. DragonSB Finance — USD 10 million stolen. In April 2022, the smart contract of the company that developed this game project was hacked by hackers.

5. OpenSea — USD 3.4 million stolen. In February 2022, hackers managed to steal over 1,200 ETH from the NFT in a phishing attack. The attackers tricked users of the OpenSea marketplace.

6. TopGoal — USD 2.2 million stolen. In February 2022, TopGoal was attacked and over 4.8 million TMT were transferred from the platform's hot wallet to the hacker's address.

7. The Shifters — USD 2 million stolen. At the launch of The Shifters collection, thieves stole money from users through fake websites and Discord messages. The incident happened in March 2022.

8. Alethea AI — USD 1.8 million stolen. In March 2022, 840 ETH was stolen as a result of a Discord compromise.

9. Moonbirds — USD 1.5 million stolen. Hackers created a malicious link that, by tricking users, brought them 29 NFT Moonbirds with an estimated value of 750 ETH. The incident took place in May 2022.

10. Omni — USD 1.4 million stolen. NFT financial platform Omni, suffered a hacking attack in July 2022. The damage to the platform was estimated at 1,300 ETH. Omni provided the ability to borrow funds against NFT collateral. The theft took place through a re-entry attack.

Financial Losses due to Technology Crime Cases in Hong Kong (2021)

Year	Total No. of Cases	Financial Loss (HK$ million)
2021	16159	3204
2020	12916	2964
2019	8322	2906.5
2018	7838	2771
2017	5567	1393.0
2016	5939	2300.8
2015	6862	1828.9
2014	6778	1200.68
2013	5133	916.9
2012	3015	340.41
2011	2206	148.52
2010	1643	60.38
2009	1506	45.1

Source: Hong Kong Police Force

Target confirms Credit/Debit cards hacked (Dec 2013)

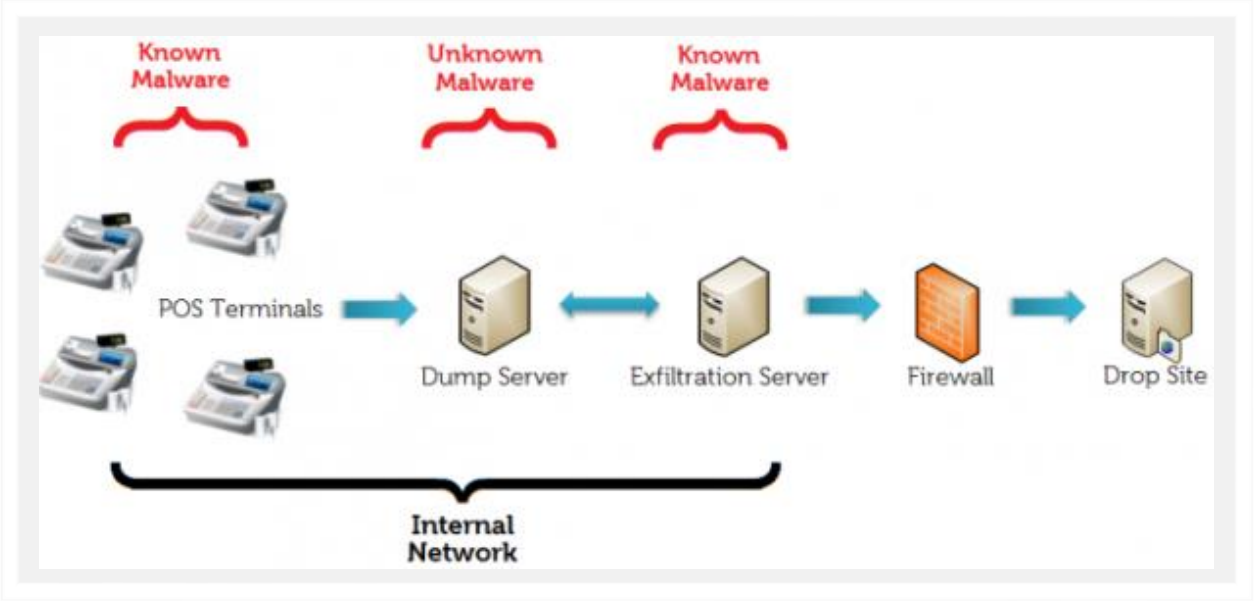
Target Confirms Up to 40 Million Credit and Debit Cards Hacked

Ashley Feinberg
Filed to: TARGET 12/19/13 10:33am

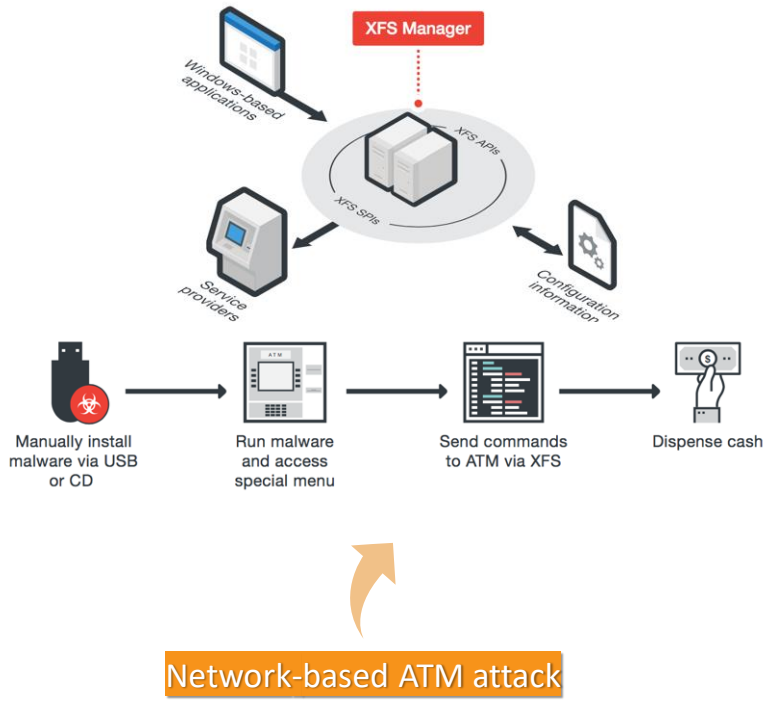
87,640 6

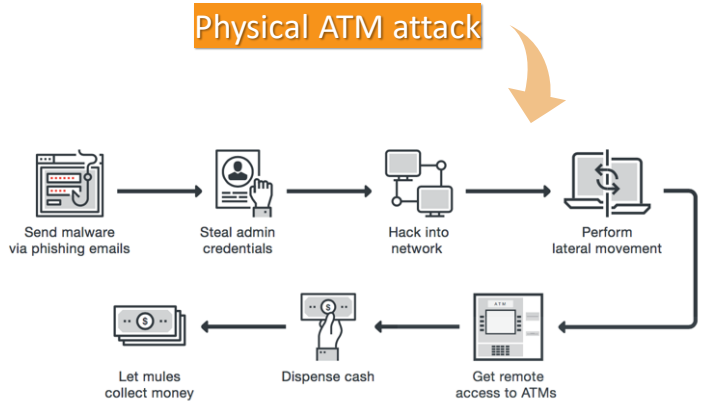
New Clues in the Target Breach

Relationships between compromised and attacker-controlled assets (by Dell Secureworks)

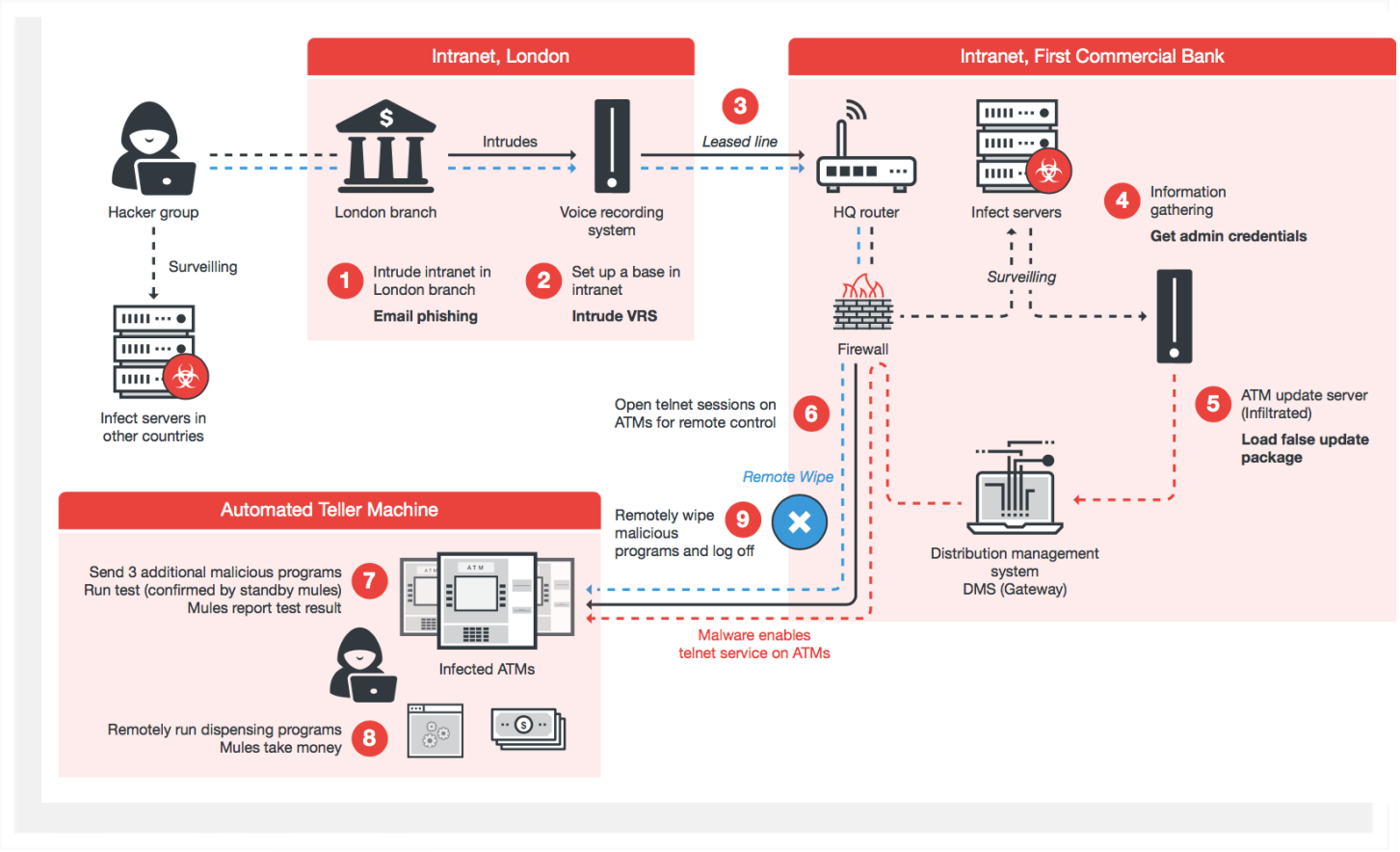


ATM machine attack



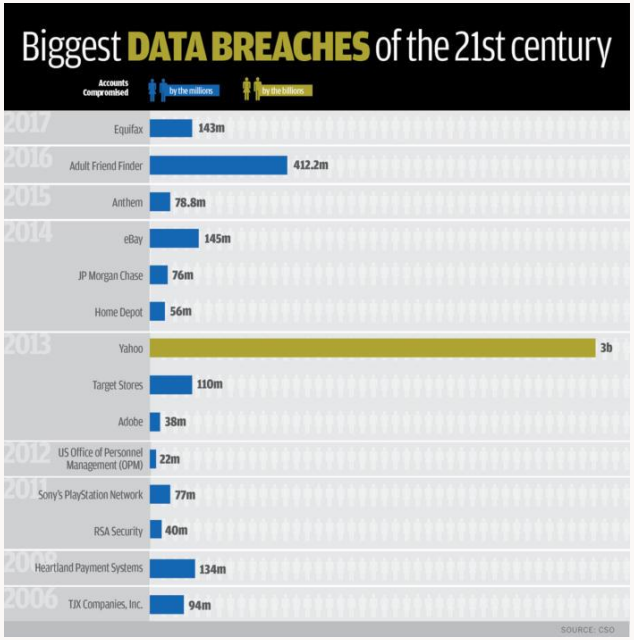


ATM machine attack (Taiwan)



Biggest Data Breaches of the 21st century

- Yahoo
  - 2013-14
  - Impact: 3 billion user accounts
- Adult Friend Finder
  - Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com
  - Oct 2016
  - More than 412.2 million accounts
- eBay
  - May 2014
  - Impact: 145 million users compromised



What is CyberSecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. – *ITU-T X.1205, Overview of cybersecurity*

Cyber security – defined as the protection of systems, networks and data in cyberspace – is a critical issue for all businesses. Cyber security will only become more important as more devices, 'the internet of things', become connected to the internet. – *ITGovernance.co.uk*

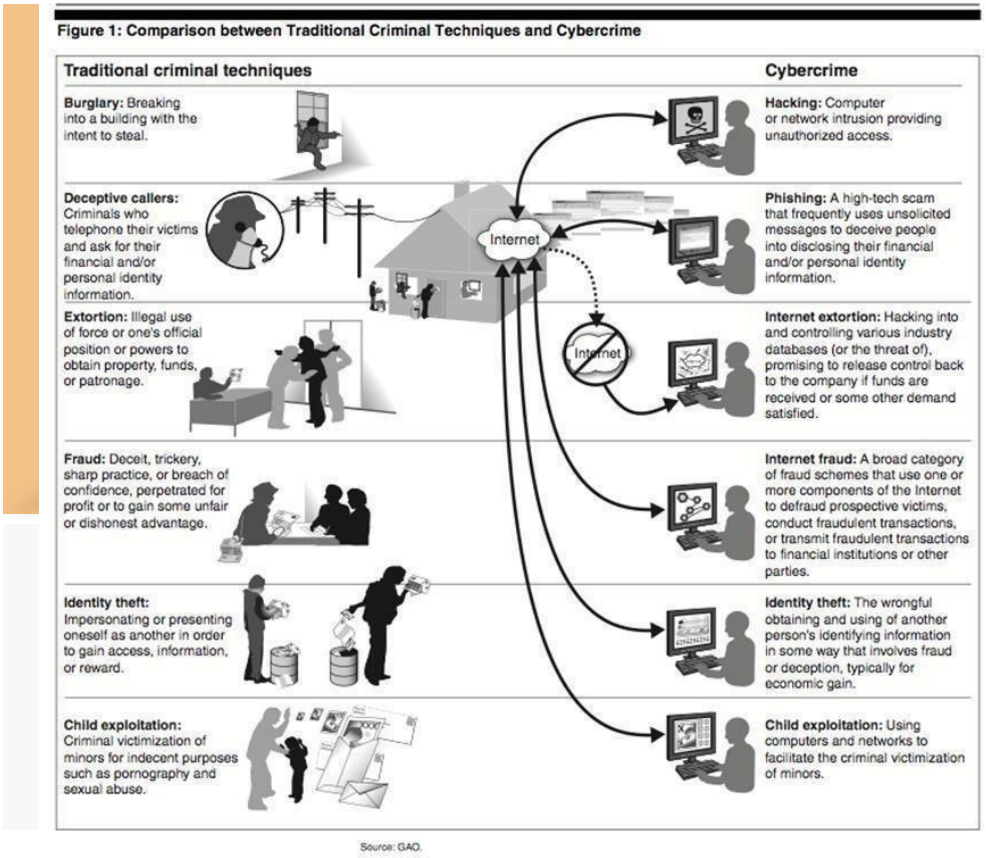
Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management. – *Definition in Techopedia.com*

What's the difference between Cyberspace and Internet

The Internet is the global communication network, both hardware and software infrastructure that links smaller computer networks throughout the world. Most people use the term as a loose synonym for WWW (World Wide Web), a system of interlinked hypertext documents ("website pages") accessed through the Internet.

Cyberspace, on the other hand, is a vaguely defined term - invented by William Gibson - that refers the non-geographical, virtual, even metaphoric space in which all computer objects "exist". The term can include the entire content on the Internet, as well as the objects created by virtual reality simulations and computer games.

Comparison between Traditional and Cybercrime techniques



Difference between Information Security and CyberSecurity

The terms “cybersecurity” and “information security” are often used interchangeably.

Information security deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people’s minds, and verbal or visual communications.

Cybersecurity, on the other hand, is concerned with protecting digital assets—everything from networks to hardware and information that is processed, stored or transported by internetworked information systems.

What is Computer System?

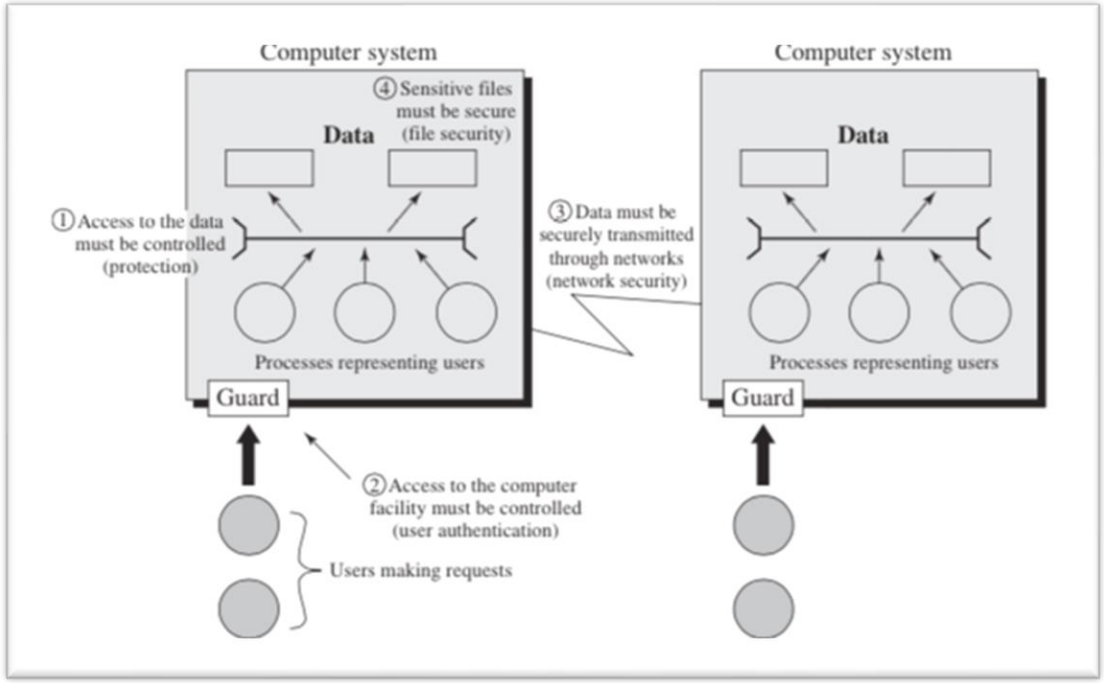


Figure 1.3 of Computer Security Principles and Practice 2nd Edition, William Stallings

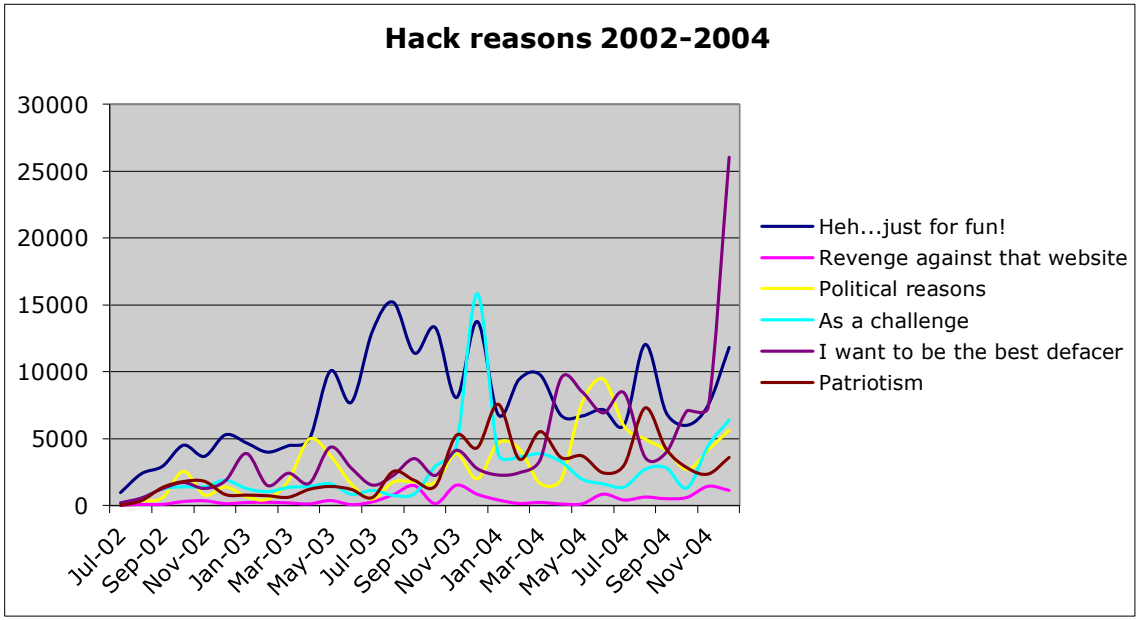
Hacking

"Hacking" is a common term to describe an attack against a network infrastructure, usually but not necessary over the internet.

Types of hacking:

Web defacement: change the context of a web page.
Application data attack: obtain secret information, such as customer credit card numbers
Denial of Service attack: prevent users accessing the server(s).

Hack Reasons



Types of Security Attacks

Exploitation
- Buffer Overflow

Cross-site scripting

SQL Injection

Canonicalization

Authentication and authorization attack
- Brute force attacks
- Dictionary attacks
- Cookie replay attacks
- Credentials theft
- Authorization

Sensitive information disclosure
- Disclosure of confidential data
- Sensitive Data

Input manipulation
- Parameter Manipulation
- Query String manipulation
- Form field manipulation
- HTTP Header manipulation
- Data tampering

Configuration issue
- Over-privileged process and accounts
- Configuration management
- Unauthorized access to administration interfaces
- Unauthorized access to configuration stores
- Retrieval of plain text configuration secrets

Lack of individual Accountability

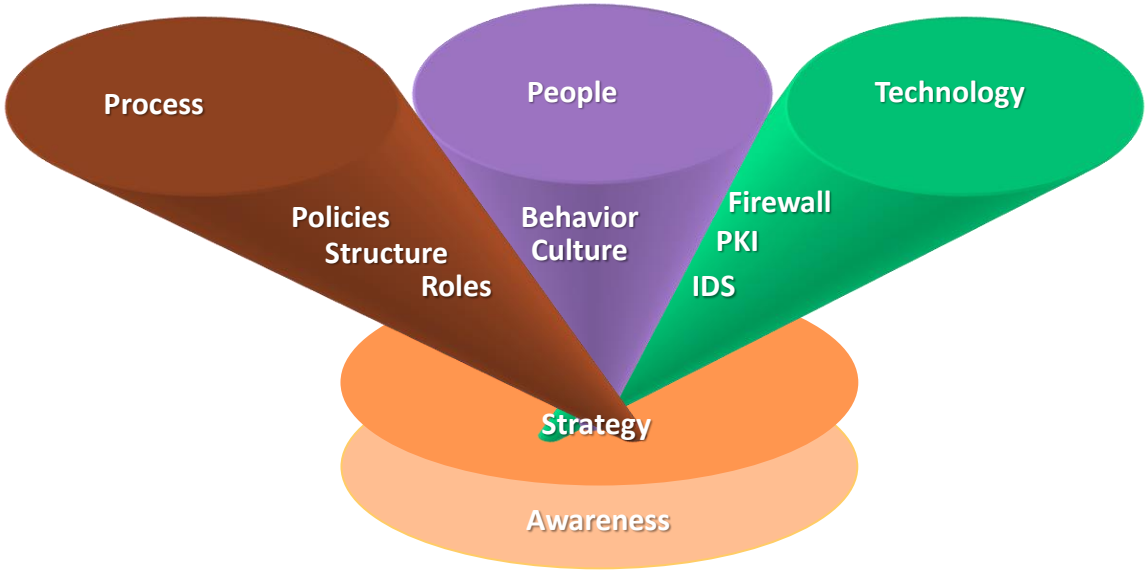
Session Hijacking

Luring Attacks

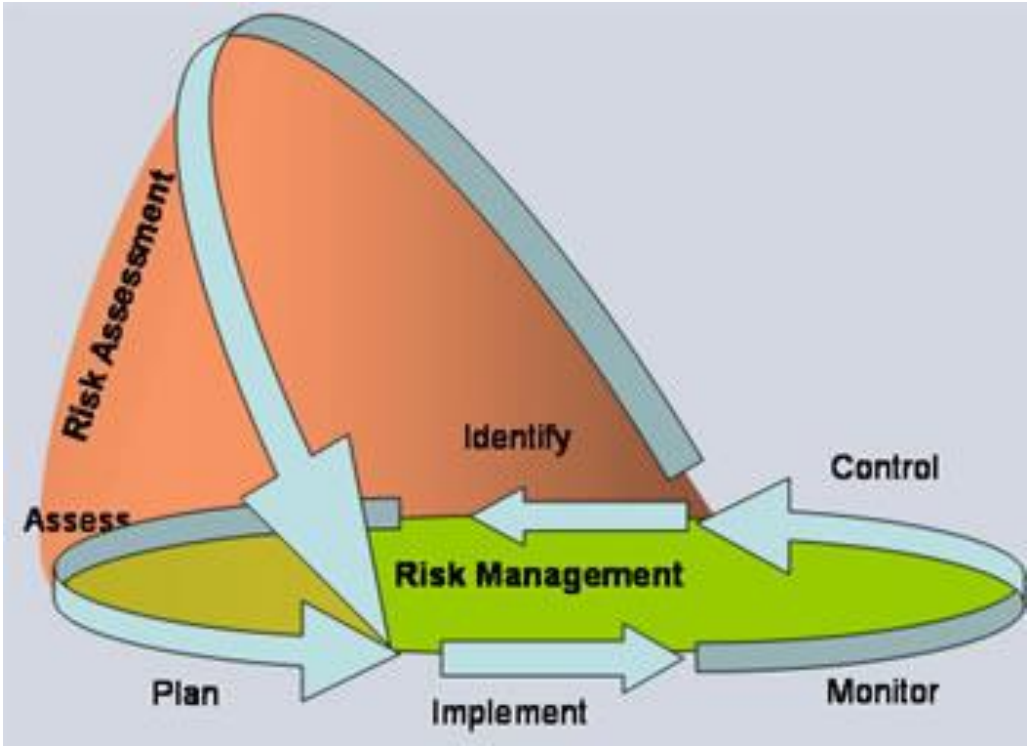
Network Attack
- Session Replay
- Session Hijacking
- Man in the middle attacks
- Network Eavesdropping

Encryption Attack
- Weak key management
- Weak Encryption

Pillars of Security



ENISA Risk Analysis



Risk Assessment Theory

Overall Risk = A x V x T

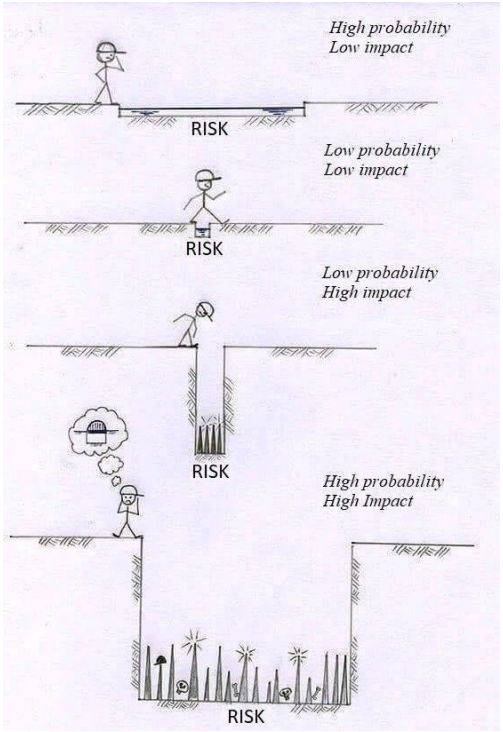
- Asset Value (A) = Confidentiality + Availability + Integrity
- Vulnerability Evaluation (V) – does not have any limit in rating
- Threats Evaluation (T) – depends on the human and environmental factor

Another risk analysis scheme is (NIST SP800-30)
R = Likelihood x Damage:

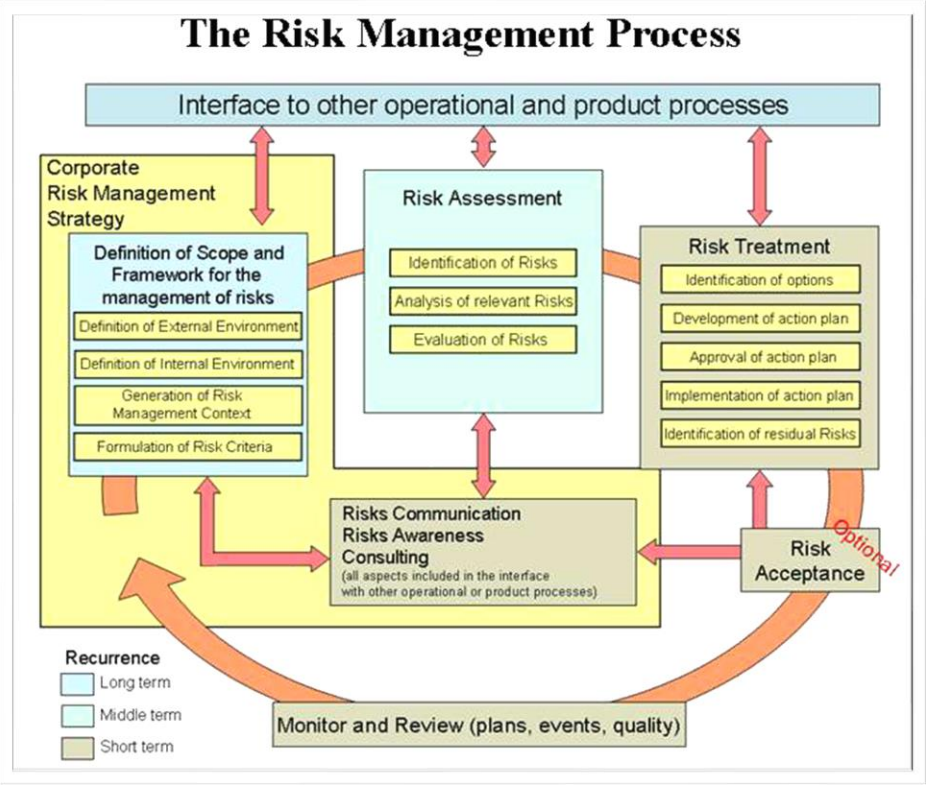
- Likelihood of the threat occurrence
- Impact/Damage of the threat

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

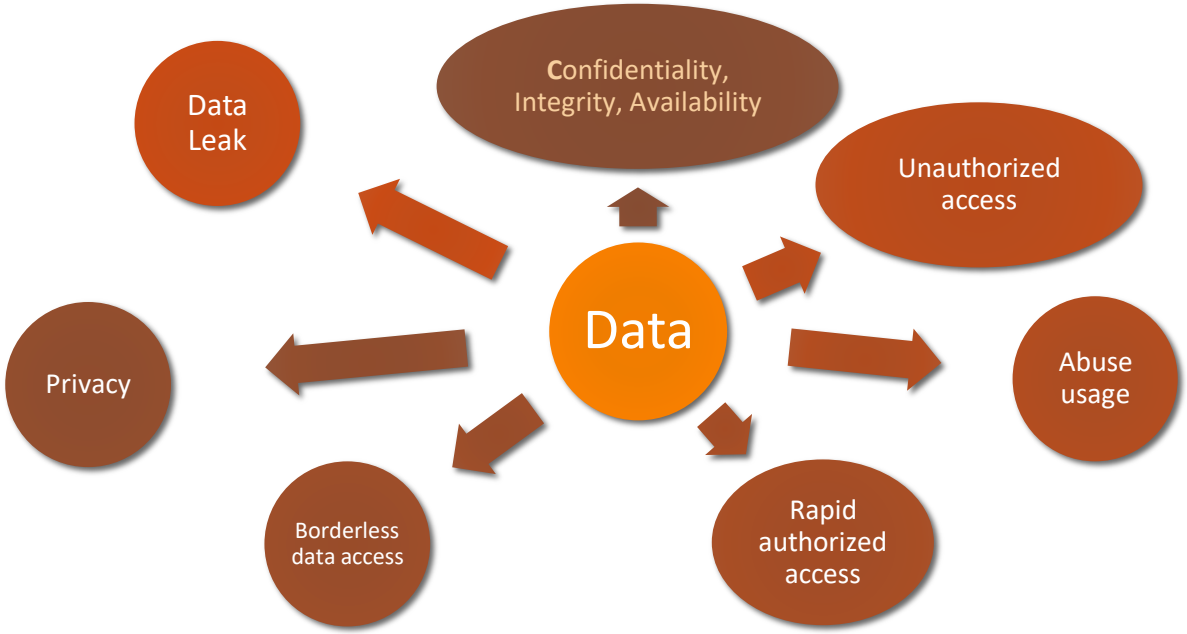
https://en.wikipedia.org/wiki/IT_risk



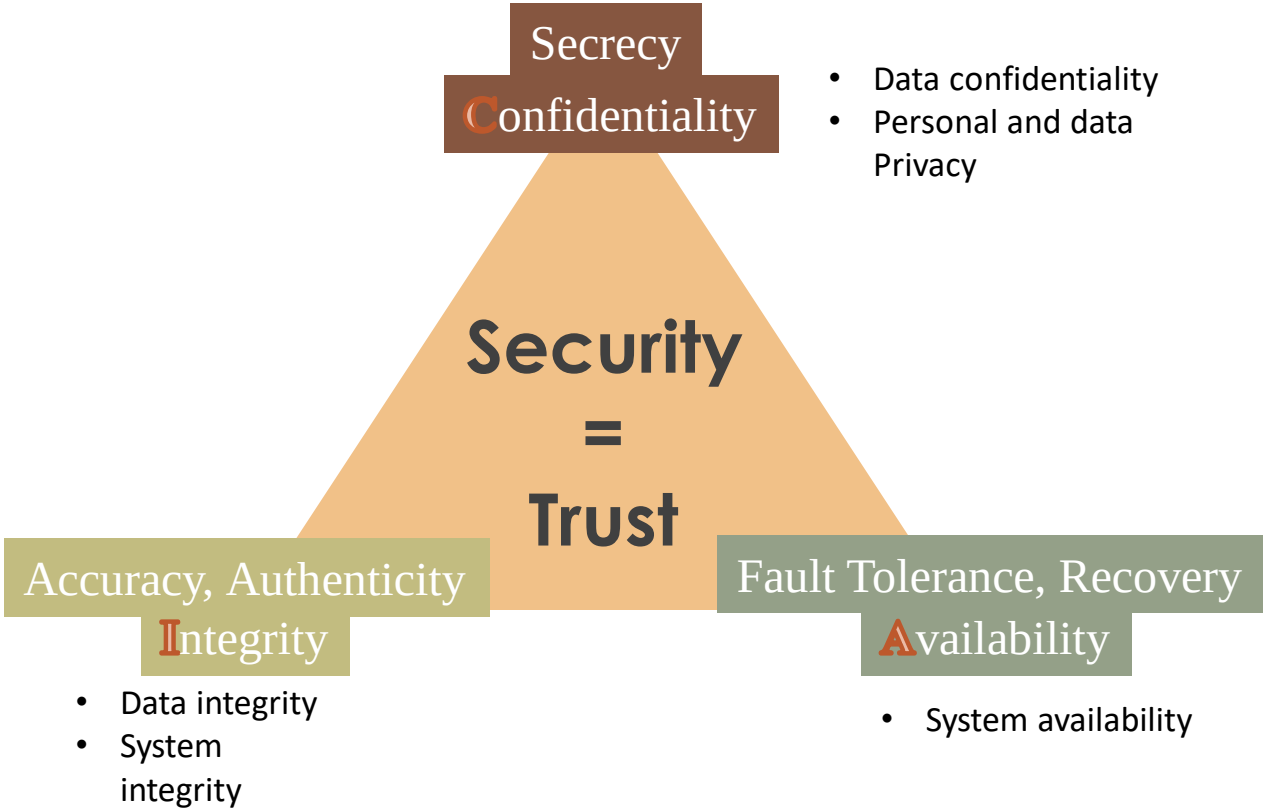
Typical Risk management process



What is the Most Valuable Asset and Why Cybersecurity is Critical?



CIA Triad



- Data confidentiality
- Personal and data Privacy

- Data integrity
- System integrity

- System availability

Security Concepts

- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability**: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.
- **Authenticity**: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability**: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems aren't yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

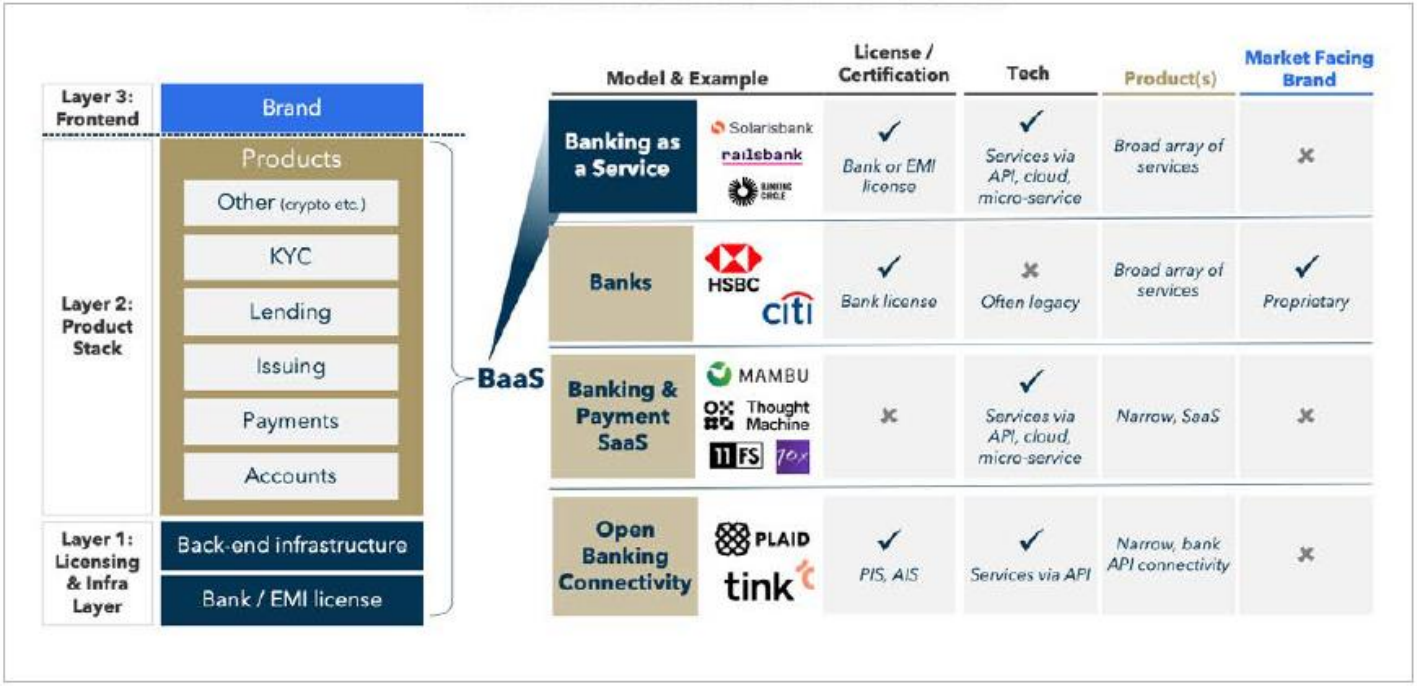
From Computer Security, Principles and Practice (2012)

Application of Cryptographic Tools to Online Banking

Online Banking site

Bank as a Services

Figure 2: BaaS platform stack and comparison by business model



Source: Flagship market observations

Overview

Specify a basis for interoperation between components from different vendors

Establish Trusts

Components in PKI may include:

Certification Authorities

Components

Certificate Authority

- Issue and manage subordinate/cross certificates
- Accept revocation requests from certificate holders and ORAs for certificate is issued
- Post Certificates and CRL to Repository
- Accredit ORAs
- Cross certifies other CAs

Organizational Registration Authority (ORA)

- Handle the process of applying a certificate
- Scalable PKI – delegate management functions

Certificates

Electronic document binds entities to their public keys

- Name
- Serial Number
- Expiry date
- Digital signatures of Trusted CAs
- Approved functions (Object IDentifiers)

Types and Classes

- e.g. 3 Classes in VeriSign
  - different applications, different levels
- Server Certificates, Personal Certificates, Code-Signing Certificates, Server Gated Certificates …

Certificates (cont'd)

Certificates Handling

1.Issued

- Received the request from ORAs
- Sign the key with corresponding functionality requirement
  - policy driven

2.Verified

- ORA has the responsibility to verify the identity of applicant
  - Address, Salary Form, …
  - Social Security Number, HKID

3.Distributed

- Directory Services
- People to lookup the certificate of the partner

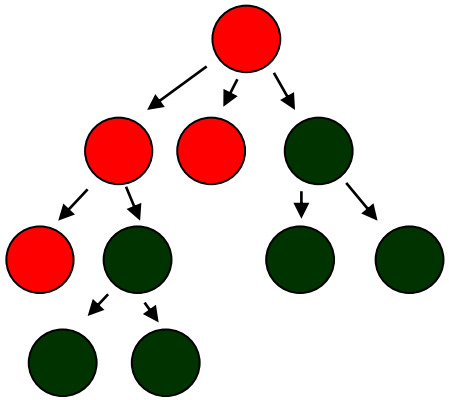
4. Revoked

- People could know that the certificate shall be discarded and void the trust

Certificate Management

Hierarchical Structures

- Trust intermediate signing certificate inherit trust to decedent
- Root CAs
- Subordinate CAs
  - Issue different kinds of Certificates
- Excellent security over insecure channels
- Distribution of certificates are valid at time of receipt
- Offline model
- Bottleneck at CA
- Concentration of trust in one entity
- Burden to protect private key



Applications

EFT

- SSL
- SET

Digital signatures of official documents

Single Sign On

Standards

RFC

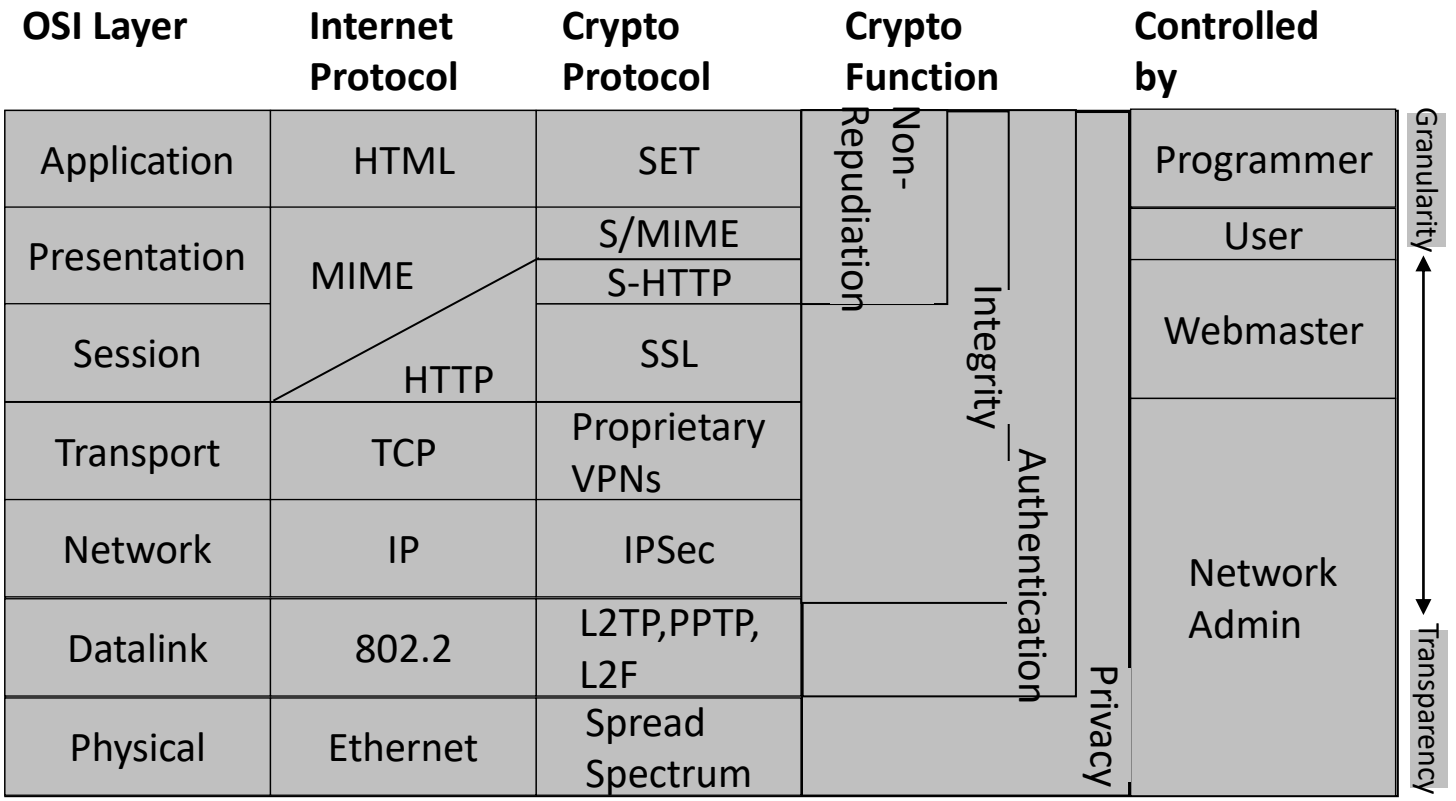
- 2459, 2510-11, 2527-28, 2585, 2692-93, 2559-60

IEEE 1363

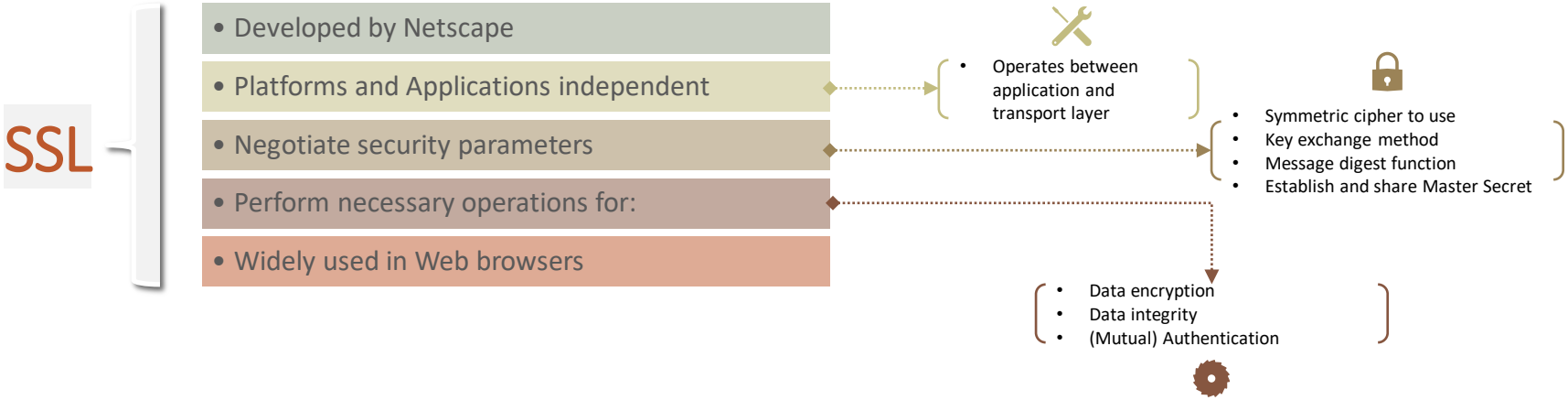
X.509 v3

X.500 – directory

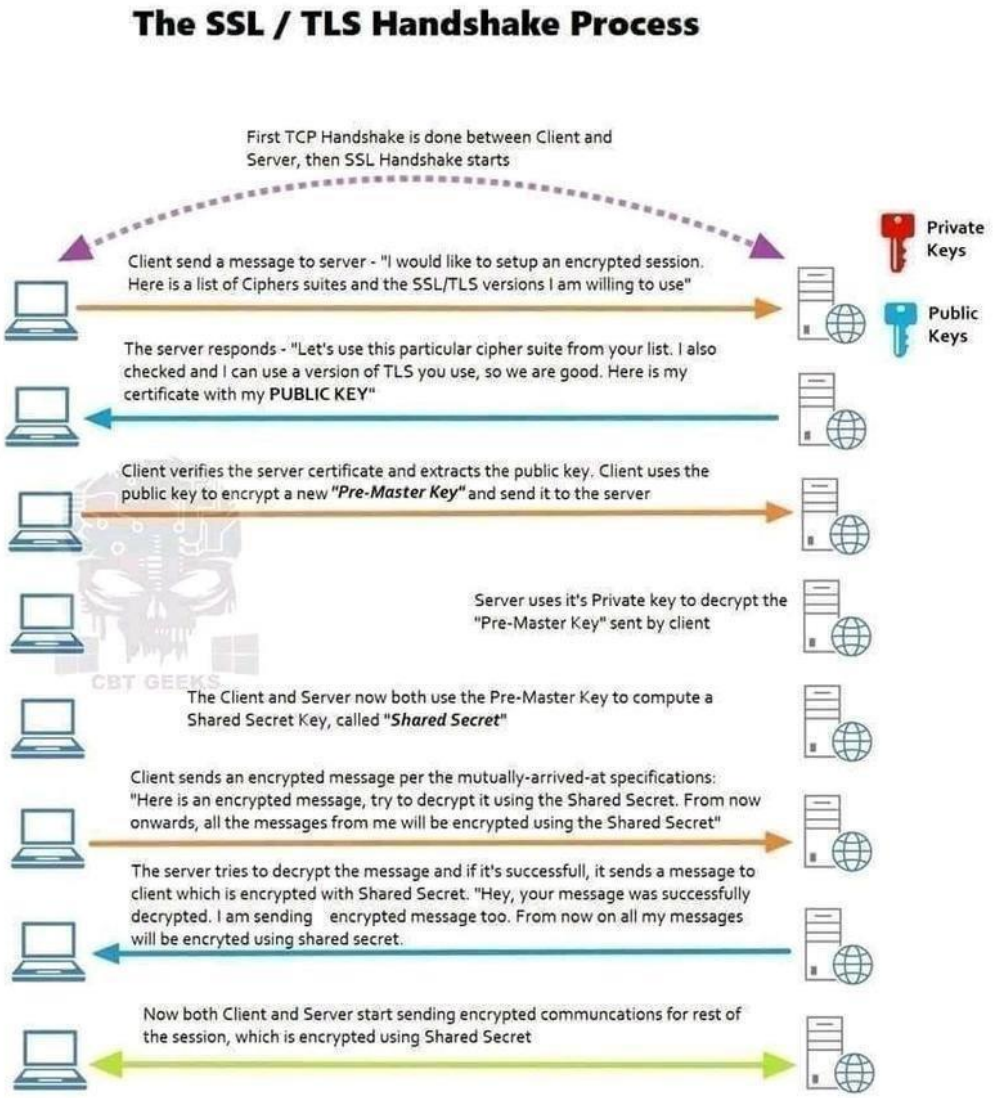
OSI Model Diagram
Excerpt from Information Security Management Handbook, 4th Edition



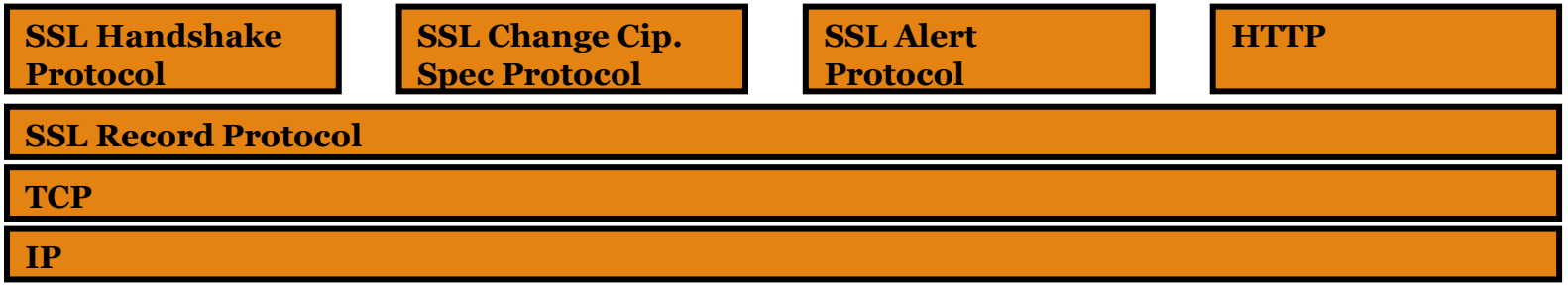
Secure Socket Layer (SSL)



SSL/TLS Handshake Process



SSL - Secure Socket Layer Protocol



SSL connection

- Transport (RM OSI) that provides suitable type of services. Every connection is associated with one session.

SSL session

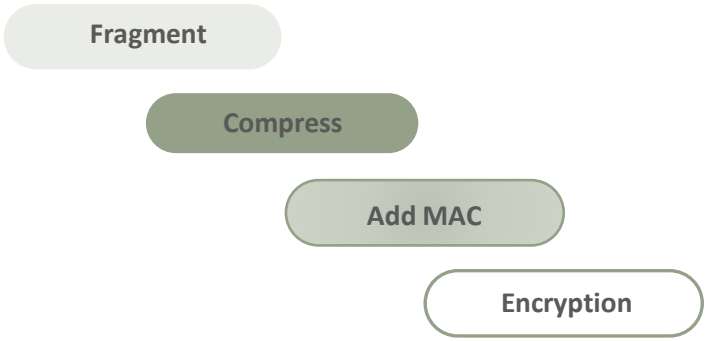
- An association between a client and a server. Sessions are created by the Handshake protocol (defines set of cryptographic security parameters, that can be shared among multiple connections)

SSL - Secure Socket Layer Protocol (Cont.)

SSL Record Protocol - provides two services for SSL connections

- Confidentiality - handshake protocol defines shared secret key for encryption of SSL payloads
- Integrity - handshake protocol defines shared secret key to form message authentication code MAC

Operations of SSL Record Protocol



SSL - Secure Socket Layer Protocol (Cont.)

Supported key exchange methods

- RSA - secret key is encrypted with the receiver's RSA public key (receiver's certificate available)
- Fixed Diffie-Hellman - server's certificate contains the D-H public parameters
- Ephemeral Diffie-Hellman - the D-H public keys are exchanged, signed using the sender's private RSA or DSS key
- Anonymous Diffie-Hellman - base D-H algorithm is used with no authentication
- Fortezza

SSL - Secure Socket Layer Protocol (Cont.)

Supported cipher algorithms:

- RC4, RC2, DES, 3DES, DES40, IDEA, Fortezza
- Supported MAC algorithms:
- MD5, SHA-1

Transport Layer Security (TLS)

- IETF standardisation initiative for producing an Internet standard version of SSL. (Current version of TLS is very similar to SSLv3.)

TLS

The Transport Layer Security (TLS) protocol was released in January 1999 to create a standard for private communications.

implementation of the TLS protocol on two levels: the TLS record protocol and TLS handshake protocol

There are seven main differences between **SSL and TLS**.

- Protocol version number
- Alert protocol message types
- message authentication
- Key material generation
- Certificate verify
- Finished
- Baseline cipher suites

SSL and TLS protocols

Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecated in 2020[7][8][9]
TLS 1.1	2006	Deprecated in 2020[7][8][9]
TLS 1.2	2008	
TLS 1.3	2018	

TLS

TLS 1.1

- Added protection against cipher-block chaining (CBC) attacks.
  - The implicit initialization vector (IV) was replaced with an explicit IV.
  - Change in handling of padding errors.

TLS 1.2

- TLS Extensions definition and AES cipher suites were added

TLS 1.3

- Remove support for a number of options and functions
  - Remove support for weak and less-used ciphers
  - Remove support for MD5 and SHA-224 cryptographic hash functions
  - Remove Compression, 32-bit timestamp as part of the Random parameter in the client_hello message
  - Remove Change Cipher Spec Protocol
  - Remove Static RSA and DH key exchange
- TLSv1.3 uses Diffie–Hellman or Elliptic Curve Diffie–Hellman for key exchange and does not permit RSA. Because with DH or ECDH, a new key is negotiated for each handshake.
- TLSv1.3 allows for a “1 round trip time” handshake by changing the order of message sent with establishing a secure connection.
- Encrypts all handshake messages after the ServerHello

Card payment solutions

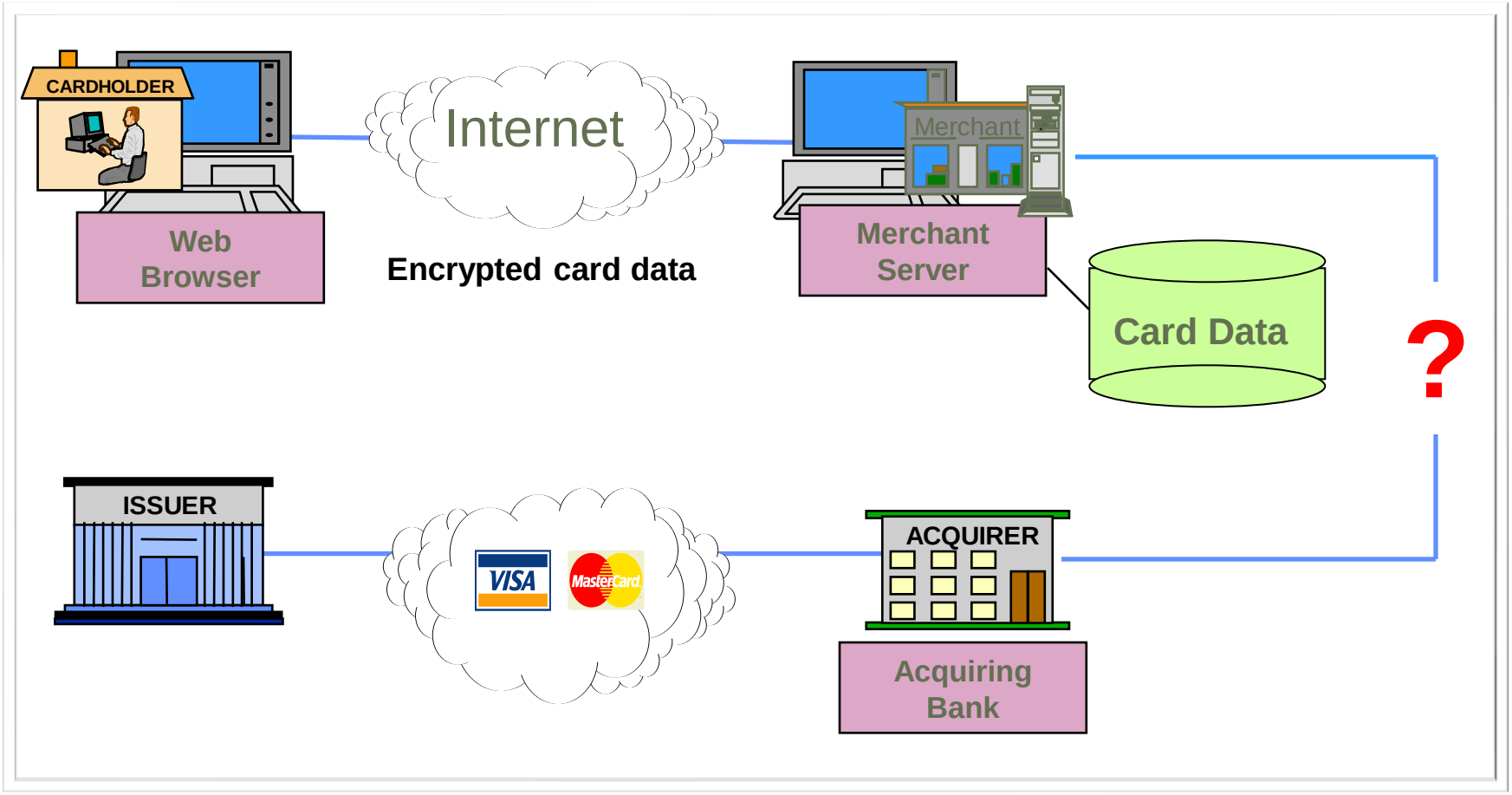
Allows web-enabled browser and servers to authenticate each other. In other words, it verifies that all parties involved are indeed who they say they are.

Limits access to servers, directories, files and services so that no undesirable parties would have access to them.

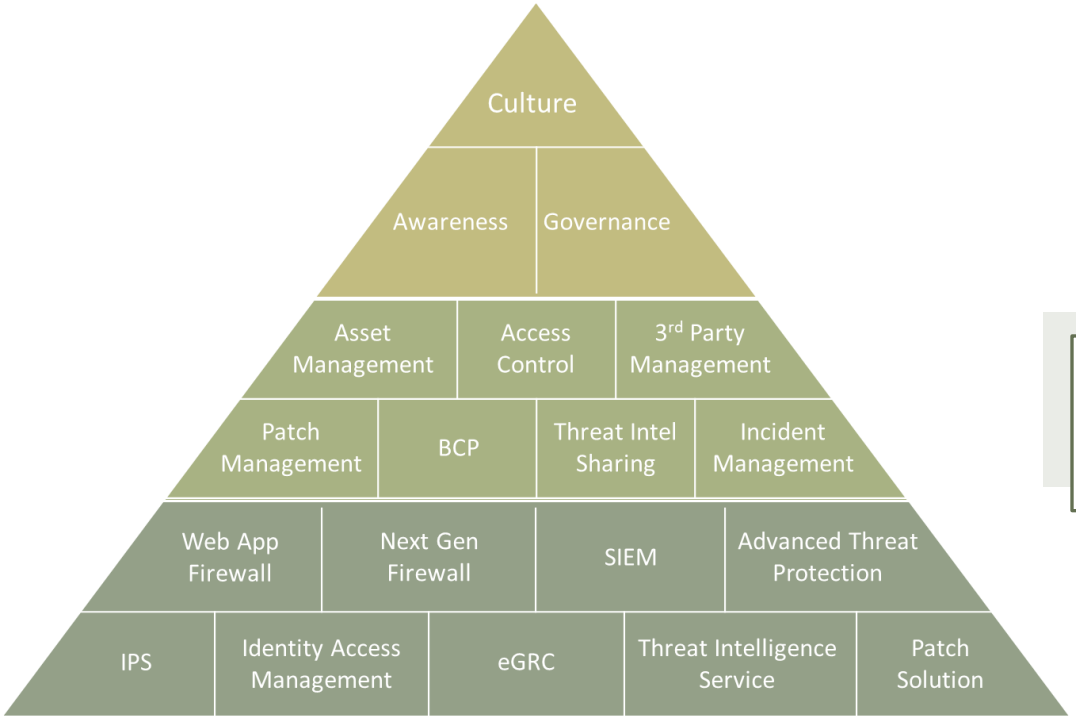
It allows information to be shared between the shopper, bank and merchant only.

SSL protects all data to ensure that exchanged data cannot be corrupted without detection.

Card payment solutions



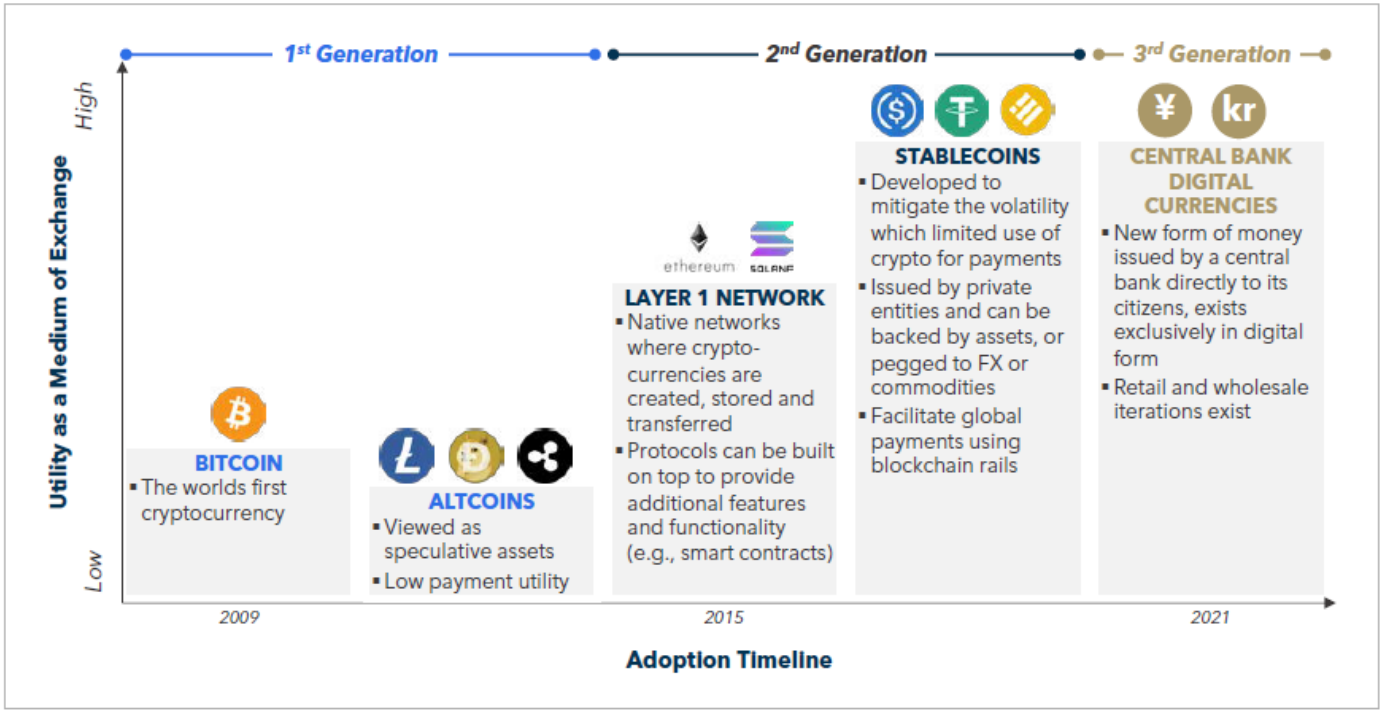
Holistic Approach to Security



- Where to spend the money
- Which processes to improve?
- What solutions to buy?
- How to prioritize?

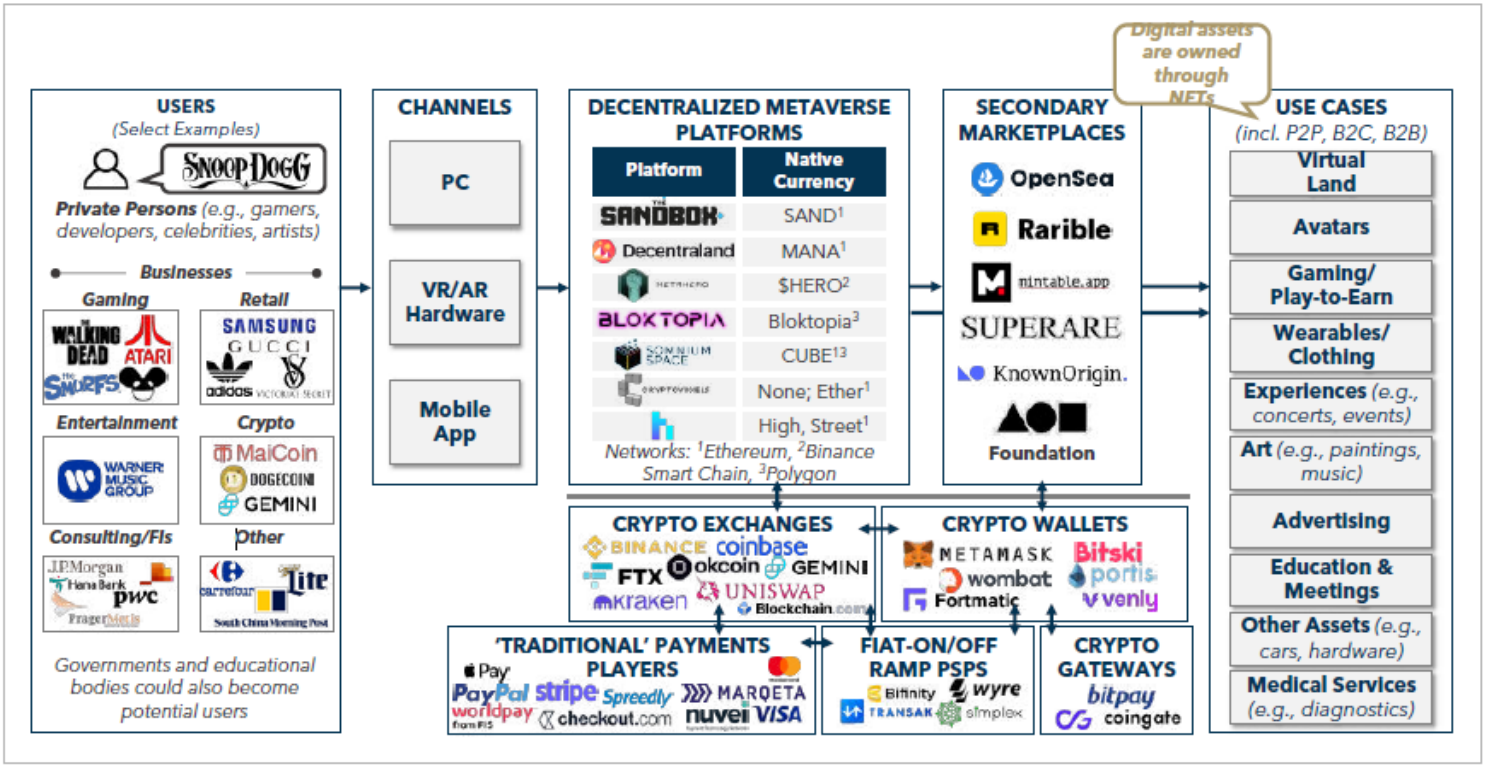
Evolution of Crypto & Relevance as a Medium of Exchange

Figure 1: Evolution of Crypto & Relevance as a Medium of Exchange



Source: Flagship market observations

Decentralized metaverse ecosystems



Source: Flagship Advisory Partners