This report is made possible by the support of the American People through the United States Agency for International Development (USAID.) The contents of this report are the sole responsibility of USAID Financial Sector Transformation Project, being implemented by DAI Global LLC, and do not necessarily reflect the views of USAID or the United States Government.
Annexes

8.4. Other important issues

8.3. Regulatory approach to asset tokens

7.9. ICO Tokens, Crypto Derivatives

7.8. Currency

7.7. Anti-tax / simplified tax system, personal income tax

7.6. Corporate tax / simplified tax system, personal income tax

7.5. Taxation by VAT

7.4. Taxation by VAT

7.3. Cryptocurrency Mining

7.2. Cryptocurrency Mining

7.1. Cryptocurrency Definition

6. Cryptocurrency and ICO Regulation Internationally

5. Mining in Ukraine

4. Ukrainian Cryptocurrency Market

3. Cryptocurrency Mining

3.1. Proof-of-work in Bitcoin

3.2. Proof-of-stake in Ethereum

3.3. Improvements in processing power of personal devices

3.4. Pooled mining

3.4.1. The risks of mining centralization

3.4.2. Can decentralization be strengthened?

2. Private blockchains

1. Introduction

Key Aspects

- Some Thoughts on Regulation

2.5. Private blockchains

2.4. The challenge of scalability

2.4.1. The Lightning Network

2.4.2. Ethereum scalability

2.3. Cryptocurrency trade globally

2.2. Cryptocurrency Mining

2.1. Bitcoin

1. Introduction

Introduction

Glossary
Foreword

As the cartoon below suggests, cryptocurrency is a new and poorly understood phenomenon. In 2017, irrational exuberance seized the market for bitcoin and its price skyrocketed by 1800% in a single year, only to fall by 70% in 2018. Nevertheless, serious amounts of money are being invested in distributed ledger and blockchain technology by leading banks, financial companies, and governments.

This paper examines cryptocurrency generally (the technology underlying it, its limitations and promise, its characteristics and uses financially, international regulation), and in Ukraine specifically. For the general reader, it is important to understand the key issues that will decide whether cryptocurrency becomes widely accepted as a means of exchange, or whether it will fade away, as private money issuance did at the beginning of the 1900s. For financial authorities, it is important to understand what cryptocurrency is and is not, how it is used, what economic functions it performs, and what risks it poses for financial services consumers.

This paper is primarily the work of Kateryna Bilous, a digital finance specialist of the USAID/FST project. It was reviewed by FST’s legal team, especially Maksym Burlaka, and by FST’s technology specialist.

Robert Bond
USAID/FST Project
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain</strong></td>
</tr>
<tr>
<td><strong>Coin</strong></td>
</tr>
<tr>
<td><strong>Consensus mechanism</strong></td>
</tr>
<tr>
<td><strong>Cryptocurrency</strong></td>
</tr>
<tr>
<td><strong>Distributed database</strong></td>
</tr>
<tr>
<td><strong>Fork</strong></td>
</tr>
<tr>
<td><strong>Hash function</strong></td>
</tr>
<tr>
<td><strong>Hashrate</strong></td>
</tr>
<tr>
<td><strong>Initial coin offering (ICO)</strong></td>
</tr>
<tr>
<td><strong>Merkle tree</strong></td>
</tr>
<tr>
<td>Term</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>hash</td>
</tr>
<tr>
<td>Miner</td>
</tr>
<tr>
<td>Mining</td>
</tr>
<tr>
<td>Node</td>
</tr>
<tr>
<td>Proof-of-stake</td>
</tr>
<tr>
<td>Proof-of-work</td>
</tr>
<tr>
<td>Smart contract</td>
</tr>
<tr>
<td>Token</td>
</tr>
<tr>
<td>Virtual currency</td>
</tr>
</tbody>
</table>
1. Introduction

At the September 2017 Ukrainian Financial Forum in Odessa, just before the start of a panel discussion on cryptocurrency, an electronic voting question flashed on the hall screens: What is Bitcoin? The possible answers were: a new currency; a share; a derivative; a disruptive technology; or a financial pyramid scheme. In the voting, a disruptive technology barely edged out a financial pyramid scheme for first place among the 150 financial experts voting. By the end of the year, the price of bitcoin would surge to over $19,000 (1,800% increase for the year) before falling in 2018 by about 70%.

Why is cryptocurrency relevant to Ukraine? Somewhat surprisingly, Ukraine is among the world leaders in wealth invested in cryptocurrencies as a percent of GDP. By 2016, Ukraine had developed a significant cryptocurrency community due to a variety of factors: early involvement in cryptocurrency by national IT entrepreneurs; an unstable economy; the conflict with Russia; the lack of investment options beyond foreign currency, bank deposits and government bonds; a large informal sector (40% of the economy); and a culture that is supportive of corruption. Cryptocurrency is unregulated, and indeed there is no definition of it as an asset under Ukrainian law.

Cryptocurrencies are a new entrant to financial markets internationally, and even sophisticated investors might have knowledge gaps concerning technology. Some associate cryptocurrency with money laundering, while others see it as the result of a new technology with transformative possibilities for commercial and financial transactions.

The focus here is on what cryptocurrency is, how it functions, how it is traded on the Ukrainian market, and current proposals for its regulation. The main topics are: the definition of cryptocurrency, mining, international context, Ukrainian exchanges and trading practices, the conduct of the Ukrainian market, and international legal and regulatory treatment of cryptocurrencies. Current Ukrainian legislative proposals to regulate cryptocurrency in Ukraine are also examined.

Our conclusion regarding the best regulatory response to cryptocurrency in Ukraine is twofold: first, caution; second, to approach it based on its function or use. This has been the predominant international regulatory response. Different regulatory authorities are involved depending on the economic function of tokens: i) payment tokens also known as cryptocurrencies that do not entitle you to any claim on profits or decision-making ability inside the system; ii) asset tokens that are equity and debt instruments; and iii) utility tokens that give you access to a service digitally. In the United States, for example, the Commodity Futures Trading Commission (CFTC) regulates the derivatives market for cryptocurrency, the US SEC examines ‘initial coin offerings’ and possible fraud, and the US Treasury FINCEN is concerned with money laundering and financial crime. Individual US states may regulate it under money transfer rules. In terms of Ukraine, it is important to: define cryptocurrency in law; focus on licensing requirements, disclosure, and consumer protection; and apply anti-money laundering (AML) provisions to exchangers.

---

1 Bitcoin, written in upper case, refers to the transaction system, whereas bitcoin, written in lower case, refers to a unit of currency.
2. Key Aspects of Cryptocurrency

The technology at the heart of cryptocurrency is not new. Rather, it is a combination of proven technologies applied in a new way: the Internet, efficient data storage and update, cryptography. The genius of cryptocurrency is in the protocol governing incentives in the system.

Nor is the philosophy behind cryptocurrency new. Many economists have thought and written about the decentralization of money, most notably Friedrich Hayek in his book ‘Denationalization of Money’. Hayek advocates for a free market in the production, distribution and management of money. Some argue that cryptocurrencies are a contemporary form of private money that was popular between the end of the 19th and the beginning of the 20th centuries, especially in the United States and the British Empire.² In that period, private money often circulated in parallel with fiat money. The reasons for the expansion of private money were rapid industrialization, decentralization (states and colonies), and the inability of the central government to meet the demands of a booming economy for money and credit. Since the middle of the 19th century, the tendency for centralization strengthened, and fiat currencies have almost entirely monopolized national markets. Governments have powerful tools to support fiat currencies: regulations that require conducting and reporting domestic transactions in the respective sovereign currencies; collecting taxes, paying social benefits, and government subsidies in fiat currencies; and the exclusive right to issue money.

Cryptocurrency is not a claim on the issuer like fiat currency or electronic system money. Fiat currency is a central bank or commercial bank liability; electronic money is a liability of the issuer that must be converted upon request into fiat currency. Ultimately, the value of cryptocurrency will depend on the development of the underlying technology and the acceptance by the public of cryptocurrency as a means of payment. The current work on scalability of public cryptocurrency networks is vital to the future of cryptocurrency.

Trust in the cryptocurrency system is provided through participants holding identical copies of a full database of ownership positions that is changed only with majority consensus. Cryptocurrency systems use blockchain technology and public-private key cryptography. Blockchain is a way to organize records in blocks resistant to unauthorized modification of the data, where each block points to a previous block in a chain. The data in a block cannot be changed without affecting all months.

---

(http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf)
blocks on top of it as they are all threaded together by means of cryptography. Transactions on existing public blockchains are irreversible.

There are many different cryptocurrencies in the market, but only some are significant. As of June 2018, total US dollar value of issued cryptocurrencies was around US $320 billion. Top cryptocurrencies by market capitalization are: bitcoin (40%), ether (20%), and ripple, which is not really a cryptocurrency (8%).

2.1. Bitcoin

Bitcoin was created after the 2008 global financial crisis by a still unidentified programmer, who used the name Satoshi Nakamoto. The idea was to create an alternative to the existing banking system with a new, decentralized online structure that could not be controlled by central banks. Bitcoin originally was intended as a means of exchange for all sorts of transactions, without the involvement of any financial institution, i.e., money is sent directly between users. Hence, its association with unsavory transactions and money laundering. Times have changed. Bitcoin is now converted and traded on many platforms around the world. It is traded as a derivative on the Chicago Mercantile Exchange (CME). Interestingly, bitcoin futures on the CME have margin requirements that are similar to gold. There is growing interest among established financial market players in building trading platforms that would allow large investors to buy and sell bitcoin. The New York Times reports that the Intercontinental Exchange (parent company of the NYSE) is working on an online platform, and Goldman Sachs has stated its intention to open a bitcoin trading department. Cryptocurrency transactions are cheaper than traditional cross-border remittances, though deposit/withdrawal into fiat currency can be costly.

The currency of Bitcoin network is bitcoin (BTC). Bitcoin is attractive as a store of value, mainly because of its limited supply. The Bitcoin protocol limits the total number of coins to 21 million, of which 3.7 million are already lost or unused for years according to a report produced by Chainalysis. The main risks to Bitcoin are centralization of mining and its ability to scale (to be discussed later in the paper). Most vendors and organizations that accept bitcoin, among them Microsoft and Wikipedia, do not accept it directly. They work through intermediaries to convert bitcoin into fiat currency.

---

3 https://coinmarketcap.com/all/views/all/
5 https://www.ft.com/content/29259448-69b3-11e8-b6eb-4acfcfb08c11
Encryption techniques that use a secret key to transmit information have been around since antiquity. A Bitcoin transaction is also an encrypted message. Public and private key pairs in Bitcoin can be compared to an account and a password: to access coins you have to have a private key corresponding to a public key. Bitcoin is pseudo anonymous because the address is a stable value. The easiest technique to preserve anonymity is to use a new address for every transaction. However, this technique is not perfect because all transactions are linked and stored publicly and permanently on the network. It is clear what goes into every transaction and what emerges. The resulting ‘transaction graph’ can reveal a lot of information, which can be analyzed by specialized companies (like Chainanalysis used by Europol).

Transaction processing in Bitcoin network takes around an hour; a transaction is considered completed when at least several blocks are mined on top of a block that has a transaction (transactions that change ownership positions are added to the chain in blocks). The cost to modify a block increases with every block added to the blockchain because blocks are threaded together, and one has to modify all blocks on top of a target block that has a transaction.

### 2.2. Ethereum

Vitalik Buterin first described Ethereum in a white paper in late 2013 and the system came to life in 2015. Ethereum is a public platform for building decentralized applications. Decentralized applications are web applications that can use the same technology to render a front-end like traditional web applications. However, instead of storing data on centralized servers, the back-end code is running on Ethereum smart contracts.

Ethereum can represent ownership of property and exchange value. In Ethereum, tokens that represent different rights, e.g., a right to access a service digitally, ownership of a physical or intangible asset, a right to participate in the future earnings of a company; and the network currency ether can be exchanged with zero latency and security across one ledger. Ethereum can be used to create markets. Autonomous organizations can be created, and many functions of an organization can be delegated to an Ethereum contract. For example, it can implement a transparent voting process, and provide for transparent funds management. Smart contracts can also be programmed for applications like a mining pool, a dispute resolution system, a relay that can move value between distinct blockchains, a decentralized file storage, and for many other use cases. The system has the capacity to run seamlessly across borders.

---

Storj is an application on Ethereum that uses blockchain to decentralize data storage by breaking up files into pieces, encrypting, and sending them to hard drives located all around the world. Individuals and businesses can rent out their unused hard drive space to make money. Storj launched its own cryptocurrencies (Storjcoin) in order to incentivize usage and to create a market for buying and selling decentralized storage. Similar projects are Swarm, SIA and others. (https://coincentral.com/storj-beginners-guide/)
Smart contract

A smart contract is a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are redistributed automatically among those parties according to a formula based on certain data that is not known at the time the contract is initiated. A smart contract is an account on a blockchain with an autonomous code that is executed when an account receives a payment, and/or other input data for execution, and all network participants agree on the validity of an execution trigger.

Any action on the network (sending ether, interacting with a smart contract, building an application) requires a payment based on how much computation is expended. It is also an incentive that ensures that developers write quality applications (wasteful code costs more).

Ethereum technology is still in development. Coding smart contracts is not easy and there is simply not enough experience yet. Smart contracts can contain bugs. For example, in 2016 one such bug was exploited to drain 3.6 million ether.

An infrastructure needs to develop around the platform used to move value. Only very simple smart contracts, where the assets exchanged exist on a blockchain, can be executed without interaction with the outside world. In many instances, a smart contract will have to rely on external information. For example, an employment agreement where the parties do not agree that the work was finished, would have to involve a judge to decide. A smart contract either has to trust the outside actors or verify the integrity of the information. In some cases, there might be ways for a smart contract to verify external information relying on several external experts and with almost no cost. But in many cases it has to trust an external source of information. Oracles are trusted data feeds that send information into smart contracts. For example, the LINK Network project is working on an Oracle network to provide smart contracts with off-chain data. They are cooperating with SWIFT to create a SWIFT Oracle that will allow smart contracts to get information from 11,000 banks. LINK is a token on Ethereum blockchain, and any account can purchase the Oracle service.

Smart-contracts are tamper-proof and will execute exactly as programmed. Once a smart contract is sent to the system, the code and associated data is replicated on all network nodes. The code will execute only with the network consensus. Each smart contract is isolated from other smart contracts, other processes and node resources, and one can interact with it only through specialized instructions (transactions). A smart contract cannot retrieve information from the outside world. It can only ask outside actors to deliver information.

Decentralization comes at a cost. Storing data and performing calculations on the blockchain is expensive. Part of the cost issue could be resolved with scalability. Computational resources and storage of a contract are restricted because it exists entirely on the blockchain.

Gas limit

Gas is a unit used to measure the computational work of running transactions in the Ethereum network. Gas is paid in ether; gas price in ether is a function of the market. Gas limit refers to the maximum amount of gas one is willing to spend on a particular transaction.

---

7 The meaning of decentralization
9 From Smart Contracts to Courts with not so Smart Judges, posted by Christian Reitwiessner on February 17, 2016
10 https://www.smartcontract.com/link
A smart contract can turn to a dispute resolution system where arbiters are grouped into pools by expertise. A dispute resolution system is agreed between parties at the moment the smart contract is deployed. Arbiters can be randomly selected using random information from both parties as a seed. Parties also have the option of using a specialist or a group of specialists in a certain sphere that they both trust. Jury.Online implements an Ethereum-based platform for dispute resolution for ICOs.\(^{11}\) The jury is analogous to commercial arbitration.

Ether’s exchange rate is highly correlated with that of bitcoin. It is, however, different because in addition to being a currency of its own, it is also used to pay for computational resources in the Ethereum network. Ethereum is more decentralized than Bitcoin: 28% of Ethereum nodes can be positively identified as being in datacenters, while the same number for Bitcoin is 56%.\(^{12}\) Ether is protected from concentrated mining using ASICs (chips customized for a particular use), and it can be mined on GPUs (graphics processing unit). Bitcoin issuance is limited to 21 million coins, at least until the protocol is changed with the network consensus, while ether is intended to be issued in perpetuity. Originally, 60 million ether were allotted to contributors at the pre-sale in 2014, of which 12 million (20%) went to the development fund, most of it going to early contributors, and the remaining amount to the Ethereum Foundation. One ether is divisible by \(10^{18}\) units that are the smallest unit of account on the network.\(^{13}\)

Every year, in perpetuity, up to 18 million ETH will be issued. It is estimated that the amount of ether that will be lost each year caused by transmissions to addresses which are no longer accessible will be on the order of 1% of the base.\(^{14}\) Ether may be lost due to loss of private keys, or by death of owners without transmission of private keys. The inflation rate (rate at which the amount of ethers in the system grows) drops every year because 1% of the total number of coins is lost every year. The idea is to balance inclusiveness of Ethereum with maintaining low inflation so that ether is a good store of value. Inclusiveness is achieved by supplying enough currency to fuel the creation of new services on Ethereum.

A number of other platforms for smart contracts have emerged, for example EOS and Cardano. EOS and Cardano coins are in the top-10 cryptocurrencies by capitalization. Applications and ICOs\(^{15}\) launched on Ethereum still have access to more users and liquidity because the platform has gained the network effect.

**Other coins**

*Ripple* is not a cryptocurrency, it is a network for financial messaging in real time with smooth conversion between currencies. It was created and is controlled by a consortium of private companies. The goal of its creators is to offer an alternative to SWIFT\(^{16}\) as a provider of financial messaging services. It allows banks and non-bank financial services companies to incorporate the Ripple protocol into their systems, and communicate directly, thereby reducing costs. Ripple is used by companies such as UniCredit, UBS, and Santander.

\(^{11}\) https://jury.online/faq
\(^{13}\) http://ethdocs.org/en/latest/ether.html
\(^{14}\) https://blog.ethereum.org/2014/04/10/the-issuance-model-in-ethereum/
\(^{15}\) Initial coin offering (ICO) is a fundraising done by issuing tokens and selling them for cryptocurrency or fiat currency.
Cryptocurrencies based on the CryptoNight algorithm (of them Monero\textsuperscript{17} has the largest capitalization) offer improved anonymity by obscuring the sender, recipient and amount of every transaction. The Ukrainian Karbo is based on the CryptoNight algorithm. The MimbleWimble blockchain protocol potentially addresses gaps of implemented cryptocurrency protocols: upgrades privacy, scalability and fungibility. Grin is an open source software project that implements the MimbleWimble blockchain.\textsuperscript{18}

2.3. Cryptocurrency trade globally

Until the upsurge in interest in cryptocurrency by international financial institutions, most of the action in cryptocurrency trading was in the Far East. China was the epicenter, until the Bank of China’s clampdown on cryptocurrency trading in January 2017. Since then, Japan drives the market: 60\% of all bitcoin for fiat currency trade is in Japanese yen.

In 2017, the market became less fragmented, as exchanges aligned rates to eliminate the profitability of automated arbitrage. In Japan, spot trading accounted for only 18.39\% of trades in cryptocurrencies in 2017 (based on the five most traded currencies: bitcoin, ether, ripple, bitcoin cash, litecoin).\textsuperscript{19} The remaining 81.61\% is margin trading, or so called cryptocurrency forex. As of March 2018, Japan had 3.5 million individual cryptocurrency traders. Approximately 95\% of users have custody deposits of less than ¥1 million ($9,100), of which about 77\% are under ¥100,000 ($910). Fiat funds have flowed into the cryptocurrency ecosystem during the last two years. The cryptocurrency trading market today is driven by Japanese traders in their twenties through fifties.

South Korea is the second largest cryptocurrency market with 5\% of bitcoin for national currency trade (US dollar accounts for 20\% of bitcoin trade for fiat currencies, but since it is an international currency, it is difficult to attribute trade to a nation). South Korea enacted AML regulation for cryptocurrency exchangers effective January 30, 2018.

\textsuperscript{17} https://cryptonote.org/cns/cns008.txt
\textsuperscript{18} MIMBLEWIMBLE, Tom Elvis Jedusor, 19 July, 2016 (https://scalingBitcoin.org/papers/mimblewimble.txt)
https://github.com/ignopeverell/grin/blob/master/doc/intro.md
Bitcoin price started growing in the summer 2017 as the community reached consensus on SegWit, the backward compatible protocol update, which was activated in August 2017. It made transaction processing faster and cheaper by removing witness data that took 60-70% of the memory space from the blockchain. Witness data (signatures and instructions how to apply them) is used to authorize accessing and spending coins. Network participants, or nodes, send witness data along with the core transaction data (sender and receiver data, amounts). Reference to the witness is included into every block for the network to be able to identify and check signatures corresponding to the transactions. Non-SegWit nodes do not receive witness data. SegWit nodes are not required to store witness data and can discard it once the check is completed. SegWit also fixed unconfirmed transaction malleability and so made second-layer protocols that rely on unconfirmed transactions, like the Lightning Network that scales Bitcoin, less complicated to design. At the time of writing, the share of SegWit transactions in the network was already 45%.

Bitcoin price is sensitive to acceptance from the formal financial system and to regulation in important markets. Bitcoin reached the peak price of more than 19,000 US dollars in December 2017. On December 17, 2017, bitcoin futures were launched on the Chicago Mercantile Exchange (CME), the world’s largest commodity trading market. This action, even with high margining requirements and prescribed ‘stops’ for high price volatility, tended to legitimize bitcoin in the minds of speculators. The instrument’s settlements asset is cash. The CBOE Global Markets offers bitcoin futures too.

Nasdaq’s chief executive, Adena Friedman, said this year that the group would consider offering cryptocurrency exchange services in future. Alternative funds are also muscling in. Morgan Stanley data show there is now more than $3.5bn in estimated assets under management across 250 dedicated crypto-funds, although the pace of the creation of new funds has slowed recently. A more formalized over-the-counter market has started to develop, with players such as Cumberland, an arm of Chicago-based DRW, and Goldman Sachs-backed Circle growing rapidly.

There is online media speculation that funds that hold cryptocurrency will be able to obtain an Exchange Traded Fund (ETF) status in the United States and will be able to offer these funds to retail investors. That would probably push bitcoin price far beyond the December 2017 record. However, the US SEC published a letter in January 2018 enumerating a list of requirements the asset lacks to be traded (issues with valuation, liquidity, custody), making it clear it is not an immediate prospect.

Cryptocurrency complemented cash as an instrument for moving value outside of the state purview. The Director of Europol estimated that around 4% of all illicit proceeds in Europe are now turned into cryptocurrencies. Many jurisdictions have issued guidance clarifying that the obligation to comply with AML-related obligations also applies to cryptocurrency exchangers and wallet providers, most obviously those that facilitate transactions between cryptocurrencies and fiat currencies. Several major banks in the US and the UK banned credit card purchases of

20 https://www.ft.com/content/29259448-69b3-11e8-b6eb-4acfebf08e11
cryptocurrencies during the hype in 2017, probably after an urge from regulators. Facebook banned ICO\(^23\) advertisements, and monitors cryptocurrency ads closely before allowing them.

![Figure 2. Bitcoin and ether price, USD](image)


Acquiring and holding cryptocurrency has risks for investors:

- **Price volatility.** Cryptocurrency markets are nascent and volatile, and purchases must be considered as highly speculative. It is simply too difficult to predict future value reliably. For example, bitcoin price grew from $1,700 in May 2017 to a peak of $19,300 in December 2017, dropped to $6,900 in February 2018, and at the time of writing is circa $6,500. Daily bitcoin volatility index was 3.78% over 30 days to May 14, 2018. The 60-day index was 4.2%\(^24\).

- **Security.** To own cryptocurrency, one needs to have a wallet to store it. A wallet does not store the coins itself, but rather the private keys that allow accessing the accounts on blockchain register (which are the public keys). Software run by full nodes has a wallet functionality, as well as lightweight SPV-clients that allow verification of user’s own transactions. Most people use web custody wallets for convenience: they can be accessed from any device and do not require back up of the keys. A good anti-virus program is indispensable in any case.

  i) A full node downloads all blocks and transactions and checks them against consensus rules. It offers the best possible security, but requires storage space and bandwidth. If a full node is offline, for example to protect a large holding, it will take time to update the ledger to transact. This storage type lowers liquidity and needs maintenance.

  ii) SPV client (Simple Payment Verification) lets a user verify his/her own transactions, and only needs to download the block headers, which are much smaller than the full blocks. To verify that a transaction is in a block, SPV client requests a proof of inclusion from the full nodes it trusts. SPV wallets are a trade-off between full nodes and with custody wallets.

---

\(^{23}\) Initial coin offerings (ICO) is a fundraising done by issuing tokens and selling them for cryptocurrency or fiat currency.

\(^{24}\) For comparison, the volatility of gold averages around 1.2%, while other major currencies average between 0.5% and 1.0% ([https://www.buybitcoinworldwide.com/volatility-index/](https://www.buybitcoinworldwide.com/volatility-index/))
They depend on full nodes for transaction verification but do not need to trust one entity like custody wallets. They require back up of the keys, and take more bandwidth and processing than custody wallets.

iii) Cloud-based custody wallets like Blockchain.info, and wallets of exchanges control user funds, who rely on a central server for interaction with the network. One can access the wallet from any device and it requires no maintenance, only trust to a provider. Some providers like Trezor offer an additional security level. To transact with Trezor, a button must be pressed on a device connected to a computer and associated with the cloud-based wallet. As a rule, custody wallets keep most cryptocurrency in a cold storage offline.

- **Liquidity.** Converting cryptocurrency into fiat currency can take from one hour to several days depending on storage type, amounts, venue (on-line versus face-to-face), transaction fee, and the price an owner is willing to accept.

- **Counterparty risk.** Transactions on public blockchains are currently irreversible, and for some exchange methods no established settlement mechanism exists. In some jurisdictions, it is difficult to protect cryptocurrency ownership rights in court.

- **Regulation.** Cryptocurrency dealers (or their activities) do not cleanly nest within traditional financial sector oversight regimes, which in some markets has meant that dealers are not registered or licensed. In case of fraud, a person might not be able to file a complaint, or to get redress.

### 2.4. The challenge of scalability

The rules of public chains (e.g., Bitcoin, Ethereum) cannot be changed, even by developers, without a community consensus. This inspires trust. Public chains, however, have limitations because they have many validators. In particular, low transaction throughput (and thus high fees) and network latency are the problems. Both Bitcoin and Ethereum developers are working on scalability of the networks. Scalable blockchain technology can bring public-blockchain costs closer to more efficient private blockchain systems.

#### 2.4.1. The Lightning Network

The Bitcoin scalability project is called the Lightning Network. It is a proposed solution to use bitcoin for micropayments.

The use of cryptocurrencies in day-to-day transaction is negligible. During 2017, the number of bitcoin transactions in the world was, on average, around 275,000 per day, compared to over nine million card transactions per day in Sweden (Söderberg, 2018) and 295 million traditional transactions per day in Europe in 2014 (EBA, 2014, p.7). As the Lightning Network creator Tadge Dryja indicates in his paper: ‘The payment network Visa achieved 47,000 peak transactions per second (tps) on its network during the 2013 holidays, and currently averages hundreds of

---


millions per day. Currently, Bitcoin supports less than 7 transactions per second with a 1 megabyte block limit. If we use an average of 300 bytes per bitcoin transaction and assume unlimited block sizes, an equivalent capacity to peak Visa transaction volume of 47,000/tps would be nearly 8 gigabytes per Bitcoin block, every ten minutes on average. Continuously, that would be over 400 terabytes of data per year.¹

Joseph Poon and Thaddeus Dryja wrote the Lightning Network (LN) white paper in 2015.²⁷ Test LN node software has been released to GitHub by several groups in the summer 2018: Lit by Digital Currency Initiative at Massachusetts Institute of Technology,²⁸ c-lightning implementation by Blockstream,²⁹ Lightning by Lightning Labs,³⁰ Eclair by ACINQ.³¹

The idea is to deposit bitcoins into a virtual safe, creating a payment channel. Bitcoin changes ownership with every transaction, but new ownership positions are broadcast to the network only when the safe is dissolved. Interaction with the network requires setting up a safe and closing it. Closure can be done at any time by the payer or payee. This process is explained in detail in Annex 3.

Requiring everyone to create channels with everyone else does not solve the scalability problem. By chaining together multiple micropayment channels, it is possible to create a network of transaction paths without the need for any party to have custodial ownership of funds. The obligation to deliver funds to an end-recipient is achieved through a process of chained delegation. Each participant along the path assumes the obligation to deliver to a particular recipient. Each participant passes on this obligation to the next participant in the path. The obligation of each subsequent participant along the path has a shorter time to completion compared to the prior participant.

Creating a network of payment channels enables micropayments down to the satoshi (one bitcoin is divisible by 100 million units called ‘satoshi’ that are the smallest amount that can be recorded on a chain), and near-instant transactions. The Lightning Network fees are paid directly between participants within the channel, and will probably be significantly lower than blockchain transaction fees. The fees are derived mainly from the time-value of locking up funds. Intermediary nodes which have better security will probably be able to out-compete others and conduct greater transaction volume. One of the largest component of fees in the financial system is from the counterparty risk. Core channels in the Lightning Network will potentially conduct billions of transactions without a need for significant storage costs.

Atomic swaps
Distinct blockchains will be intertwined and form a single system. Nodes can open lightning channels across distinct blockchains. Atomic swaps is the technology for cross-chain payments, or exchange of tokens of different chains without an intermediary. So long as there are similar core mathematical functions used in the chains, it is possible for transactions to be routed over multiple

³¹ https://acinq.co/, https://github.com/ACINQ/eclair
chains with different consensus rules. The parties ‘lock-up’ tokens that they want to exchange in safes, each on his/her chain. The safes will either be dissolved automatically and tokens returned to a depositor, or sent to an address of the new owner if the swap takes place. The safes are locked with the same hash generated from a secret key by an initiator. After the parties have both audited the safes created by a counterparty, the initiator unlocks the safe on the counterparty chain with a secret key. As he/she unlocks the safe, the secret is revealed, and the other safe can be unlocked. This is why the swap is called atomic: opening one safe opens the other one. The technology is still new and has not been automated in any wallet.

BTC Relay is building a link between Bitcoin and Ethereum that allows Ethereum contracts to verify Bitcoin transactions, so users can pay with bitcoin to use Ethereum decentralized applications.32

### 2.4.2. Ethereum scalability

A paper on Ethereum network scalability by Vitalik Buterin33 describes a system where consensus is split into two levels, and can be potentially stacked. The idea is to split transactions up into groups which affect disjointed areas of the final state, and thus can be processed in parallel. Bottom-level randomly selected validators check the validity of transactions and apply a cryptographic function to store them in a way that allows easily accessing and checking separate balances. High-level validators see the blockchain as a collection of sub-spaces, they check final sub-space values computed by bottom-level validators and add them into blocks. Validators secure their integrity with deposits in ether, that they risk losing if they break the system rules. A mechanism is proposed to challenge and revert invalid transactions, transferring the malfeasant validators’ security deposit to the challengers as a reward unless the challenge is answered by a confirmation of validity from a much greater number of validators. So the irreversibility problem is solved.

### 2.5. Private blockchains

The concept of ‘private or permissioned blockchains’ has become very popular in the broader technology discussion.34 It is a system in which a few users have the right to modify or even read the blockchain, while still maintaining many kinds of partial guarantees of authenticity and decentralization characteristic of the blockchain. Such systems have been a primary focus of interest from financial institutions. Permissioned chains do not have to maintain decentralization and do not require software to run on laptops, instead they can employ powerful servers. They are also operated by fewer nodes with faster internet connections. Hence, the latency and time-to-finality of permissioned chains will inevitably be lower than of public chains. The consortium or company running a private blockchain can more easily change the rules of a blockchain and resolve mistaken transactions.

---

32 http://btcrelay.org/
33 Notes on Scalable Blockchain Protocols (version 0.3.2), Vitalik Buterin (Ethereum), Reviewers and collaborators: Gavin Wood, Vlad Zamfir (Ethereum), Jeff Coleman (Kryptokit), Matthew Wampler-Doty (independent) John Cohn (IBM), April 14 – May 31, 2015
34 https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
On June 21, 2018, the Cabinet of Ministers of Ukraine approved a decree to transfer the State Land Cadaster to blockchain. The project was developed by Bitfury, with support from Amnesty International as an independent auditor. However, the system is not yet implemented as a fully functioning blockchain that is resistant to unauthorized changes. The challenges include: safe transfer of the registry; implementation of a user authorization mechanism that will allow changes to ownership only with the owner approval; and development of a robust system infrastructure (transmission and data storage). OpenMarket (SETAM), a state system for execution sale, has also signed a memorandum with Bitfury to transfer its system on blockchain. According to information from the Internet, OpenMarket has already carried out successful auctions facilitated by the technology.

Countries like Sweden, the UK, Canada, are exploring creating distributed ledger-based national fiat currency as a third type of central bank obligation (complementing cash and reserves). (The article cited in the footnote provides a good brief explanation of a digital fiat currency.) Shared ledger eliminates the clearance and settlement stage in transactions, and potentially allows direct participation in the payment system for non-banks. One can implement different levels of control and information disclosure for participants. R3 company leads a consortium of more than 200 firms (among them Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street, and UBS) in research and development of distributed ledger usage in financial system. The consortium has created an open-source distributed ledger platform called Corda. The aim of Corda is to provide a platform with common services to ensure that any services built on top are compatible between the network participants, with faster time to market as the underlying infrastructure would be accepted and understood by at least the founding firms. The European Commission has also announced that it will promote the blockchain technology.

3. Cryptocurrency Mining

Agreement among participants in a cryptocurrency network is achieved in a decentralized voting system. Participants agree on the state of the database, a copy of which everyone holds. Security of the system is ensured through technical means that cannot be circumvented (cryptography and protocols) and clever incentive engineering. The resources required to participate in the system maintenance for a reward must be such that no one can monopolize it. In proof-of-work (PoW) systems, the resource is computing power and electricity. In proof-of-stake (PoS) systems, a validator’s integrity is secured by deposits that are at risk if one breaks the system rules. PoS systems are cheaper because no resources are spent outside the system. PoW is useful in the startup phase to establish a sufficiently large base of coins that can later be leveraged by PoS.

3.1. Proof-of-work in Bitcoin

35 https://www.kmu.gov.ua/ua/news/250088298
Bitcoin is a PoW system. A mining puzzle is a core of Bitcoin because it determines the incentive system.

Bitcoin network is supported by computers called miners that compete for the network seigniorage\(^3^9\) (emission of new coins is done with every block as a reward to the miner who added the block). Rewarded mining not only runs the system but also helps achieve network effect as people join to profit. A free-for-all participation must be avoided; participants are incentivized to act honestly because they invest significant resources into mining, and if the system integrity is compromised, the value of their reward falls.

Mining secures the system because it is a competition, and so if the majority of contestants is honest, the chances of an honest participant to win are statistically higher than that of an adversary.

In Bitcoin, new transactions are added to the blockchain in blocks of a maximum size of up to 1MB roughly every 10 minutes. These are the protocol constants. Miners compete over who will first propose a valid block that will be accepted by other participants. To propose a valid block, a miner must find a solution to a mathematical puzzle that can be solved only by trying all possible solutions, and each of them has an equal chance to yield a valid block. However, checking that a solution is valid is very easy. This ‘guessing’ approach requires computing power and electricity. The more computing power one invests, the higher is the probability to succeed. Some say electricity consumption by the network is comparable to that of a small country,\(^4^0\) but most bitcoins are mined with cheap hydropower in China.

The amount of new coins issued to the winner node is halved every four years to gradually slow emission. A miner is currently rewarded 12.5 bitcoins for each mined block. The Bitcoin protocol limits the total number of coins to 21 million bitcoins. Miners also earn transaction fees paid by users. The transaction fee amount in Bitcoin is not fixed and is a function of the market. Miners chose transactions to be included in a block to maximize their profit, and the fee affects the speed of transaction finalization. Fees as a proportion to the total reward have increased in 2017 with the growth of activity in the network\(^4^1\) (in 2015, median transaction fee was 0.6% of the total reward, 2.1% in 2016, and 10.9% in 2017).

Around 80% of bitcoins have been issued. Emission is set to end in 2040. When emission is over, the network will rely on transaction fees only. And the fees might go up. The current Bitcoin transaction fee to have the transaction mined on the next time block (10 minutes) is $0.16 per transaction.\(^4^2\)

Bitcoin mining went through several eras: mining on personal computers, GPUs (graphics processing units that are designed to process large blocks of data in parallel), FPGAs (integrated circuits that can be tweaked for a specific task better than GPUs). Currently, bitcoin mining is a highly professional industry, mining is done on ASICs (application specific programming interface). Fast chips were developed to do nothing but mine bitcoins at an impressive speed. Production was often financed with advance payments from consumers. Valeriy Nebesnyi, a Kievan and one of Bitfury founders, designed a proprietary bitcoin mining chip in 2011. Mining is profitable if the cost of the currency that can be mined with the given proportion of the network’s

---

\(^3^9\) The difference between the value of money and the cost to produce and distribute it.

\(^4^0\) https://digiconomist.net/bitcoin-energy-consumption

\(^4^1\) https://blockchain.info/stats

\(^4^2\) https://bitcoinfees.info/
total hashing power is higher than the cost of hardware and electricity invested. Hashing power is how many times per second the network can run a hash function. Explained in detail in Annex 2.

### 3.2. Proof-of-stake in Ethereum

On October 16, 2017, Ethereum underwent a Byzantium hard fork that made a number of updates to the protocol, including the reduction of block reward from 5 to 3 ether. A hard fork is usually done to fix a bug or introduce new features. It is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid. All nodes meant to work in accordance with the new rules need to upgrade their software. Ethereum has shorter block times (15 seconds). More frequent block creation (which is required in order to increase the transaction throughput) results in more conflicts between blocks (several miners can mine a valid block at roughly the same time). Ethereum rewards miners who mined valid blocks that were not included in the chain. This increases the network security because it incentivizes decentralization; smaller miners that are not part of a big pool usually have less direct peer contact in the network, and so hear about blocks later and are less likely to mine a block to the main chain (a valid block includes a reference to a previous block, so the faster one receives a block, the faster one can start mining). Valid blocks that did not make it to the main chain are called uncles. Ethereum incentivizes miners to include uncles as part of the block when they mine for an extra reward of 0.125 ether per uncle included. Uncles included in a block formed by successful miner receive 7/8 of the full block reward (2.625 ether). A maximum of 2 uncles are allowed per block. If uncles are submitted later than the next block, the reward rapidly diminishes, ending at zero after seven blocks.

Ethereum is soon changing the algorithm from PoW to a hybrid PoW-PoS called Casper FFG. In this version of Casper, miners propose blocks (PoW mechanism) and validators finalize them (PoS mechanism). Casper is an important step to scalability of Ethereum blockchain. In Casper, validators secure their integrity with deposits in ether that they risk losing if they break the system rules. Validators place growing portions of their security deposits against blocks; through iterated rounds of betting, validator bets quickly converge resulting in finalized blocks. When every member of a supermajority of bonded validators (a set of validators who hold between 67% and 90% of all security deposits) bets on a block with a very high (say, > 99.9%) probability, the block is final. Casper regards the consensus process as a cooperative game and ensures that each node is most profitable if they are in a coalition made up of 100% of the consensus nodes.

At the Edcon conference in May 2018, Vitalik Buterin reported new details about Casper. Participating in Casper as a validator will require a minimum of 1,500 ETH because there is a limit to the current number of validators that Casper can support in its current version. Nodes with less ether can participate in a pool. As the protocol develops, this minimum will go down. The reward is proportionate to amount of ether deposited; tentative calculations show it will be 5% annually.

---

43 [https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/](https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/)
45 [Introducing Casper “the Friendly Ghost”, Posted by Vlad Zamfir on August 1, 2015](https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/)
46 [https://www.youtube.com/watch?time_continue=13879&v=N9StTb5ZV, start at 3:51:00, PDF: https://edcon.io/assets/ppt/5.5/5.5am/Vitalik%20Buterin--So%20you%20want%20to%20be%20a%20Casper%20validator.pdf](https://www.youtube.com/watch?time_continue=13879&v=N9StTb5ZV, start at 3:51:00, PDF: https://edcon.io/assets/ppt/5.5/5.5am/Vitalik%20Buterin--So%20you%20want%20to%20be%20a%20Casper%20validator.pdf)
if 10 million ETH is deposited (or 0.22 ETH per block).\textsuperscript{47} The reward for the miners for the production of ether (block proposal mechanism remains PoW in this version of protocol) will decrease fivefold – from the current 3 ETH to 0.6 ETH.\textsuperscript{48} Validator returns are proportionate to the inverse square root of total deposits. That is, if total deposits go up 2\%, validator interest rates go down 1\%, and the total issuance goes up 1\%. Being offline is penalized. If a node is always offline it might lose up to 10\% annually. Nodes that break the protocol rules are logged off and can be penalized by up to 1\%-100\% of their deposit. Individual rewards not only depend on one’s behavior, they also depend on everyone else’s behavior. The point is to dis-incentivize coalitions. This is achieved through slashing individual deposits based on a formula $3p \times \text{deposit}$, where $p$ – is the percentage of nodes that got slashed in four month from the node that is being slashed. If a node does not vote, it gets penalized, and it gets penalized even more if many other nodes do not vote. If more than 1/3 of validators stop voting correctly, so that blocks stop finalizing, non-voting validators’ deposits start to ‘leak’ much quicker until blocks start finalizing again. Deposits are slashed if a validator submitted two contradictory votes. Of course, voting is automatic, and a validator cannot break the rules unless it is deliberate or it gets hacked. The system is designed to encourage validators to utilize ‘failure modes’ that are maximally uncorrelated from other validators’ failure modes. The wealthier nodes would need to invest more in security. When validators leave, their deposits are returned with a delay of four months. That way, deposits remain unsettled until it is determined whether a leaving validator has broken the rules in coordination with other validators.

3.3. Improvements in processing power of personal devices

The spread of public, decentralized cryptocurrency systems is facilitated by advances in computing power of personal computer devices. Chips used in mining devices in 2013 were 55 nm generation, in 2015 – 28 nm, and since 2016 – 14-16 nm. Power requirements are proportional to the area of transistors. In 2019, next generation miners will use 10nm-7nm chips, and so on to 3 nm that is projected in 2025. When silicon transistors approach atomic scale, they will stop performing due to quantum effects of small dimensions such as tunneling, leakages, and heat issues. But the progress will not stop there. New materials are being investigated that allow greater efficiency. Graphene might replace silicon in 10 years from now.\textsuperscript{49}

3.4. Pooled mining

Finding a valid solution to a PoW puzzle is a probabilistic process. To reduce returns variance, miners join into mining pools to share rewards. A pool operator distributes computation tasks to miners which have much lower difficulty than the full PoW puzzle. Each solution to the task has a probability of yielding a solution to the full puzzle, so the more miners who are trying to solve tasks, the higher is the probability of success. A solution for a pool puzzle is called a share.

\begin{itemize}
\item Network hashrate
\end{itemize}

The number of times per second a cryptocurrency network can run a hash function (Annex 2).

\textsuperscript{47}https://ethresear.ch/t/a-simple-and-principled-way-to-compute-rent-fees/1455
\textsuperscript{48}https://gist.github.com/djrtwo/bc864c0d0a275170183803814b207b9a
\textsuperscript{49}https://www.mckinsey.com/industries/semiconductors/our-insights/graphene-the-next-s-curve-for-semiconductors
A pool administrator is a full node on the network, and, in theory, it performs an independent validation of all transactions and blocks. Other miners work outside of the network and communicate only to the pool administrator, instead of being independent validators in the system. Pool administrators dictate which transactions are included in blocks, thus increasing the threat of transaction censorship. Although some pools allow miners to choose their own transactions (with some rules enforced by the pools) via the `getblocktemplate` protocol, all major pools use the old `getwork` template. Poole mining protocols guarantee that a miner cannot claim a reward for himself or any other miner. A pool does not give the whole block out to miners, just a template for a header. When a miner submits a solution that yields a valid block, a pool operator announces it to the network and obtains a reward. Pools collect a fee for administration service (around 2%), and use different payout models. But generally they distribute rewards proportionally based on contributed hashpower, and the reward can be withdrawn when a certain amount is earned. The pool operator randomly verifies a small portion of the work submitted by each member of the pool. Miners can prove how much work they are doing, the rate at which individual miners are finding shares, gives an indication of the work they are performing.

Major pools not only have individual participants from all over the world, but invest a lot in their own equipment that they house in large data centers. Determining where to set up a mining facility is based on three main considerations: access to low-cost electricity, ability to send and receive large amounts of data quickly on the Internet, and an environment that keeps equipment from overheating. Nearly three-quarters of all major mining pools are based in just two countries: 58% of mining pools with greater than 1% of the total Bitcoin hash rate are based in China, followed by the US with 16%. Other popular locations are Iceland, Georgia, and Eastern Europe. Many pools operate multiple servers in different geographic regions to improve fault tolerance and latency. Pools may choose to mine anonymously, without disclosing their gateways, hiding their true mining power by paying out to different keys: 5% of blocks are mined by anonymous pools.

### 3.4.1. The risks of mining centralization

The major risk of Bitcoin is the centralization of mining: around 2% of the nodes represent three quarters of the mining power. A relatively few groups control bitcoin issuance and have the power to change the ledger, which poses risks to Bitcoin integrity. And some of the risks have already materialized:

- 2/3 of bitcoin mining power is located in one country, China. The mining business in China is not immune to political risks. The country banned access to any cryptocurrency and ICO-related website within the mainland’s borders.

- Equipment production is also concentrated in the hands of the pools: 82% of large mining pools are hardware manufactures.

---

50 https://en.bitcoin.it/wiki/Comparison_of_mining_pools
54 Global cryptocurrency benchmarking study, Cambridge Centre for Alternative Finance, 2017
• In 2015, roughly half of the network hashrate was mining without fully validating blocks. Pools did this to save time – latency matters a lot on the network. As a result, they mined invalid blocks exposing users to a threat of losing their bitcoins. The Bitcoin blockchain forked three times.55

• An interesting illustration of centralization is a case that happened to bitcoin mining in 2013.56 The pools updated their software to BitcoinQt 0.8, while most users remained with the old BitcoinQt 0.7 client. A block was produced that was treated as invalid according to the old clients’ rules, and the blockchain forked. Pools came together and agreed to switch onto the chain where most users were, and after six hours, this chain overtook the pools’ chain. Thus, there was a deliberate 51% attack which was seen by the community as legitimate.57

• Decision-making for Bitcoin management (like SegWit) is influenced by the pools, as well as by core developers.

• The majority of miners pursue a default strategy: which block to accept in case of a fork (heard about first), which block to mine on (the longest valid chain), which transactions to include (maximize fees), when to inform the network about a newly generated block (immediately). It might be rational for a large pool to pursue a non-default strategy.58 A 51% hashrate attack is irrational (51% is a way of describing it, in effect it can be conducted with network power approaching a majority), because it can destroy bitcoin by severely undermining trust. However, rational attacks where a miner benefits are possible. In a block withholding attack, a miner starts mining on top of a newly found block without announcing it to the network. As soon as someone finds a new block, a miner will announce his first block and hope the network hears about it first. It is basically trying to find two blocks before the network finds one. A good network position is critical here. This attack is possible with even a third of the network hashrate. There have been allegations that slowness in block propagation by the dominant Chinese pools makes other miners continue mining on top of an old block, wasting time, electricity, and computing power.

Network position

The paper ‘Discovering Bitcoin’s Public Topology and Influential Nodes’ prepared at the University of Maryland (https://www.cs.umd.edu/projects/coinscope/coinscope.pdf) discusses the role that Bitcoin’s peer-to-peer broadcast plays in ensuring fairness of the network. Some nodes provide an exceptional network advantage for broadcast by creating low latency connections to the influential set of nodes: as long as a transaction (block) reaches these nodes, it is far more likely to be included in a block (extended in the blockchain).
3.4.2. Can decentralization be strengthened?

- Decentralization of cryptocurrency mining can be strengthened by using ASIC resistant puzzles. ASIC resistance is based on a well-known phenomenon of processing capacity and memory capacity gap. Advances in memory capacity have been much slower. An example of a memory hard puzzle is scrypt ('scrypt') function. It fills the memory with random values and then reads from memory in random order, thus a hash can be computed using a fixed amount of memory, or less memory but doing so increases the amount of time it takes to compute. Litecoin uses scrypt puzzle. ASICs for scrypt exist but are more expensive to produce. The weakness of the function is that checking the puzzle also requires memory. Cuckoo Cycle\(^{39}\) is a memory-hard PoW algorithm that can potentially make cryptocurrency mining even on consumer devices feasible. MimbleWimble blockchain is implementing this logic.\(^{60}\)

- Decentralization can also be promoted by implementing non-outsourcable puzzles. For example, requiring signing each puzzle solution with a private-public key pair. Private keys will be used to spend a reward later.

- Non-outsourcable puzzles prohibit centralized mining, and it might be better to just offer alternatives, like decentralized pools. The first attempt to implement a decentralized pool was the P2Pool. It runs another consensus protocol on top of the main Bitcoin protocol to build a sharechain among all miners in the pool. To compromise this arrangement, an attacker will only need 51% of the pool's hashing power, which is less than 0.1% of the network hashrate. To save bandwidth, the pool sets higher share difficulty that takes miners more time to find shares, which increases reward variance.

- Another attempt at a decentralized pool is SmartPool.\(^{61}\) It replaces a pool manager with Ethereum smart contract,\(^{62}\) which is maintained by miners on the Ethereum network. The smart contract verifies validity of the shares submitted by the pool miners and adds them into the list of verified shares with an identifier of a miner who found them. To compromise it, an attacker would need 51% of hashpower on Ethereum network.

4. Ukrainian Cryptocurrency Market

Ukrainians with resources have increasingly diversified their portfolios to include cryptocurrency. Fifty-seven (57) public officials declared cryptocurrency as an intangible asset\(^{63}\) in 2015-2017,\(^{64}\) for a total of BTC 21,027 (about US$200 million at current prices). Less wealthy Ukrainians were

---


62 Smart contracts is an account on a blockchain with an autonomous code that is executed when an account receives a payment, and/or other input data for execution, and all network participants agree on validity of an execution trigger.

63 Intangible asset is an object of intellectual property rights, as well as other similar rights. (Paragraph 4 of Article 1 of the Law of Ukraine ‘On state regulation of activities in the field of technology transfer’)

64 [https://opendatabot.com/blog/135-bitcoin-rada](https://opendatabot.com/blog/135-bitcoin-rada)
drawn to cryptocurrency actively in 2017 when bitcoin price increased rapidly. Nevertheless, cryptocurrency ownership is not widespread among the general Ukrainian public.

Cryptocurrency trade is not regulated in Ukraine, and the majority of cryptocurrency dealers are not registered. Ukrainian banks are wary of processing transfers related to cryptocurrency, in the absence of an official stance and implied possible risks (the NBU issued a general risk warning on cryptocurrency trade in December 2014, later rescinded in March 2018).\(^6\) Dealers (exchanges, exchange shops, p2p platforms/individuals) accept and make bank transfers below the AML threshold of UAH 15,000 (circa $550). Many dealers trade online with individual accounts, with most trades going via Privatbank. Some dealers accept fiat transfers via cash machines. In April 2017, after allegations about the use of cryptocurrency to launder money, some dealers strengthened user verification procedures. Larger amounts are apparently traded offline. Dealers recruit clients online for bigger trades offline, which take place face-to-face.

In a December 2017 paper, Citi estimated that Ukraine has one of the world’s largest proportions of wealth in bitcoin as a percent of GDP, around 2.4%\(^6\) (or US$2.2 billion). Citi arrived at its estimate by dividing the total issued bitcoins value at its price peak in December 2017 (over $19,000) by country, based on some unidentified data from LocalBitcoins.com (a p2p marketplace). Citi’s calculations may not be completely reliable, and bitcoin has lost about two-thirds of its value since the December price peak.

According to Ukrainian cryptocurrency market sources, around 90,000-95,000 Ukrainians own cryptocurrency. The core community that holds larger amounts is around 25,000 people. Approximately 65,000-70,000 Ukrainians made smaller purchases of cryptocurrency during the hype in 2017-2018.

Only daily trading volumes are available online. Annual UAH/cryptocurrency trading volumes, based on daily reports in April 2018, is around US $775 million. Around two thirds of users of exchange services make repeat transactions. We cite this figure with several caveats:

- Exchanges can be used for speculative trading, and actual volumes may not correspond with deposits into cryptocurrency.
- Daily volumes in April 2018 can be lower than the hype volumes in summer-winter 2017. However, the prices were lower in summer-early autumn of 2017.
- LocalBitcoins features 4,632 registered Ukrainian bitcoin traders in 96 cities and towns. However, only around ten of them are active online and offer acceptable market rates. Some traders work offline and through private referrals.

<table>
<thead>
<tr>
<th>$$</th>
<th>Exmo (Coinhills(^6))</th>
<th>Kuna (Coinhills)</th>
<th>BTC Trade UA (Digitalcoinprice(^6))</th>
<th>Exchange shops (FST estimate)</th>
<th>LocalBitcoins (Coinhills)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTC/UAH</td>
<td>574,000</td>
<td>175,000</td>
<td>163,000</td>
<td>152,000</td>
<td>95,000</td>
<td>1,159,000</td>
</tr>
<tr>
<td>ETH/UAH</td>
<td>486,000</td>
<td>148,000</td>
<td>62,000</td>
<td>103,000</td>
<td>-</td>
<td>799,000</td>
</tr>
<tr>
<td>XRP/UAH</td>
<td>-</td>
<td>30,000</td>
<td>6,000</td>
<td>-</td>
<td>-</td>
<td>36,000</td>
</tr>
</tbody>
</table>


\(^6\) Early and mid-2017. The NBU issued a general risk warning on cryptocurrency trade in December 2014 (https://ir.citi.com/6E2oHPhzWm1Wv%2F1FqjcywZsI349qEsO61g8k8zK98dhnVHGrTwg%3D%3D)

\(^6\) For BTC Trade UA (https://digitalcoinprice.com/exchange/btc-trade-ua/bch/UAH)
From a regulatory standpoint, ownership of cryptocurrency is not widespread, and the amounts are not large enough to pose a systemic risk. However, there are concerns that cryptocurrency can be used to facilitate money laundering, large amounts are transferred offline outside of the state purview.

---

### Exchange Venues Compared

<table>
<thead>
<tr>
<th>Exchange Shops</th>
<th>Exchanges (EXMO, BTC Trade UA, Kuna)</th>
<th>p2p (LocalBitcoins.com)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin price[^69] excluding the network transaction fee and deposit/withdrawal fee at exchanges</td>
<td>UAH 228,123 ($8,707)</td>
<td>UAH 223,412 ($8,527) BTC Trade UA</td>
</tr>
<tr>
<td>UAH 228,999 ($8,740)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average transaction amount</td>
<td>$600</td>
<td>$250</td>
</tr>
<tr>
<td>Spot conversion between cryptocurrencies, cryptocurrencies and fiat currencies</td>
<td>$700 (Exmo)</td>
<td>$1,400</td>
</tr>
<tr>
<td>Conversion between cryptocurrencies and fiat currencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Used for</td>
<td>Conversion between cryptocurrencies, Privatbank and other banks’ money, electronic money systems’ money (AdvCash, Payeer, PerfectMoney), currency of exchanges: EXMO codes[^70]</td>
<td>Spot conversion between cryptocurrencies, cryptocurrencies and fiat currencies</td>
</tr>
<tr>
<td>Transaction value range</td>
<td>$100 – $2,000 Offline from $500</td>
<td>from $10</td>
</tr>
<tr>
<td>Single transfer value in fiat currency</td>
<td>Up to an AML monitoring threshold of UAH 15,000 (circa $550)</td>
<td>Up to an AML monitoring threshold of UAH 15,000 (circa $550)</td>
</tr>
</tbody>
</table>

[^69]: For reference, bitcoin price at an international exchange shop Coinbase was $8,465. International exchangers require an international passport, a bank statement or utility bill for residence address verification.

[^70]: Currencies of exchanges let deposit/withdraw any instrument from an exchange without a commission (which will be paid when converting the instrument into fiat currency).
<table>
<thead>
<tr>
<th>Exchange Venues Compared</th>
<th>Exchange shops</th>
<th>Exchanges (EXMO, BTC Trade UA, Kuna)</th>
<th>p2p (LocalBitcoins.com)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online/offline</strong></td>
<td>Online</td>
<td>Online/offline for big clients</td>
<td>Online/offline conversion for US dollars or euro in Kiev, Odesa, Kharkiv, Lviv, Mykolaiv, Kherson, Cherkassy</td>
</tr>
<tr>
<td><strong>Deposit fee</strong></td>
<td>n/a</td>
<td>Exmo: 1%-2.75% (AdvCash, Visa/MasterCard UAH)</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BTC Trade UA: 2.5% Privatbank card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2% Visa/MasterCard UAH</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kuna: 1% + 5 UAH (Privatbank cards additionally 0.5%)</td>
<td></td>
</tr>
<tr>
<td><strong>Withdrawal fee</strong></td>
<td>n/a</td>
<td>BTC Trade UA: 1% Privatbank card</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3% Visa/MasterCard UAH</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kuna: 1%</td>
<td></td>
</tr>
<tr>
<td><strong>Trade verification</strong></td>
<td>Bank/electronic money system transfer confirmation</td>
<td>Bank/electronic money system transfer confirmation</td>
<td>Bank/electronic money system transfer confirmation</td>
</tr>
<tr>
<td></td>
<td>Blockchain</td>
<td>Blockchain</td>
<td>Blockchain</td>
</tr>
<tr>
<td><strong>Wallet</strong></td>
<td>Do not provide a wallet services as a rule</td>
<td>Provide a custody wallet service</td>
<td>Provide a custody wallet service</td>
</tr>
<tr>
<td><strong>Cryptocurrency liquidity</strong></td>
<td>Two stages:</td>
<td>Instant at spot price if cryptocurrency is on an exchange</td>
<td>Two stages:</td>
</tr>
<tr>
<td></td>
<td>1. Sending bitcoins to a dealer. Transaction must get minimum 3 network</td>
<td>1. Sending bitcoins to a dealer. Transaction must get minimum 3 network</td>
<td>1. Sending bitcoins to a dealer. Transaction must get minimum 3 network</td>
</tr>
<tr>
<td></td>
<td>confirmations for a dealer to send fiat money. It will take from 30 minutes</td>
<td>confirmations for a dealer to send fiat money. It will take from 30 minutes</td>
<td>confirmations for a dealer to send fiat money. It will take from 30 minutes</td>
</tr>
<tr>
<td></td>
<td>to several hours.\textsuperscript{72}</td>
<td>to several hours.</td>
<td>to several hours.</td>
</tr>
<tr>
<td></td>
<td>2. Sending fiat. This stage might take from several minutes to several days</td>
<td>2. Sending fiat. This stage might take from several minutes to several days</td>
<td></td>
</tr>
<tr>
<td></td>
<td>depending on a transfer method.</td>
<td>depending on a transfer method.</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{71} A payment system will take a fee for the transfer.

\textsuperscript{72} Transaction fee level in Bitcoin is not fixed, but is a function of the market. Transaction processing time depends of the fee level. Miners choose transactions to include into blocks to maximize profit, transaction fees are evaluated by satoshi/byte (1/100 million part of bitcoin/byte). Current transaction fee can be taken from the specialized sites (e.g., https://jochen-hoenicke.de/queue/#1,24h). Custody web wallets offer a user friendly transaction fee choice marked low/normal/high. Insufficient commission can result in suspended transaction that will take 1-7 days to be processed, or will be denied if your wallet is so configured. You can cancel a stuck transaction by sending it to another wallet you control with an extra fee. If a transaction got at least one confirmation on the network, it cannot be canceled.
Exchange Venues Compared

<table>
<thead>
<tr>
<th>Customer protection</th>
<th>Exchange shops</th>
<th>Exchanges (EXMO, BTC Trade UA, Kuna)</th>
<th>p2p (LocalBitcoins.com)</th>
</tr>
</thead>
<tbody>
<tr>
<td>complaints on referral web-sites (BestChange.ru)</td>
<td>Internal support service</td>
<td>E-mail (BTC Trade UA requires phone number and name)</td>
<td>Escrow service for transactions initiated via LocalBitcoins.com tools</td>
</tr>
<tr>
<td><strong>Customer due diligence (CDD)</strong></td>
<td>E-mail, some require phone number and name. An exchange shop may selectively request documents, or require to see your online bank via Skype or TeamViewer.</td>
<td>To use Visa/MasterCard USD/EUR at Exmo, user verification is required: color scan of a national ID, or an international passport. Bank statement or utility bill for residence address verification.</td>
<td>E-mail or direct contact without registration on the platform</td>
</tr>
<tr>
<td><strong>Traded currencies</strong></td>
<td>bitcoin, ether, ripple, EOS, litecoin, bitcoincash, tether, doge, dash, monero, XEM, karbo, zcash, ether classic</td>
<td>bitcoin, ether, bitcoincash, ripple, zcash, litecoin, tether, dash, bitcoingold, EOS, ether classic</td>
<td>bitcoin, ether</td>
</tr>
<tr>
<td><strong>Legal form</strong></td>
<td>Can be registered as legal entities in different jurisdictions</td>
<td>Registered as legal entities in different jurisdictions</td>
<td>Transactions are made between individuals</td>
</tr>
<tr>
<td><strong>Automation</strong></td>
<td>Manual/automated</td>
<td>Automated</td>
<td>Manual</td>
</tr>
</tbody>
</table>

**Exchange shops**

Exchange shops allow conversions between cryptocurrencies, electronic money (denominated in dollars and euros), currencies of exchanges (WEX, Exmo), and fiat currencies. Some exchanges do not allow deposit or withdrawal into fiat currency (Poloniex, Bittrex), and exchange shops can be used to convert into fiat. Currencies of exchanges (EXMO codes) are convertible into ‘bank money’ via shops.

In an online exchange shop, cryptocurrency is bought and sold directly from a dealer. Shops do not store user funds as a rule. (Some international exchange shops, like Coinbase, offer a wallet service with the in-built exchange.) Orders can be settled with a delay due to manual operation and waiting time for network confirmation. Because of these delays, the actual sales price can be different from an order. Exchange shops in the Ukrainian market typically verify that the payment is made from an account owned by the payer to prevent fraud. An exchange shop may selectively request documents, or require that a customer show his/her online bank via Skype or TeamViewer. Exchange shops check IP address, confirm e-mail and phone number, and may match the name provided with a phone and bank card number.

Exchange shops and LocalBitcoins trade at 2-5% premium to exchanges. Some exchange shops can be cheaper overall if one takes into account transaction and deposit/withdrawal fees at exchanges. Some exchange shops offer to exchange amounts starting from UAH 2,500, but many start at UAH 10,000. Top online trade amount is UAH 50,000. Amounts in excess of $500 are converted offline in Kiev, Kharkiv, Odesa, Dnepr, Poltava, Lviv, Mykolaiv, Kherson, Cherkassy.

There are about six shops with reasonable exchange fees servicing the Ukrainian market, most of them from one-and-a-half to three years old. Exchange shops are often registered in jurisdictions

73 BestChange.ru (https://www.bestchange.ru/)
that are more favorable to cryptocurrency trade (Netherlands, Germany, Estonia), where they get access to bank accounts used to purchase cryptocurrency from international exchange platforms, and receive customer funds from offshore accounts. In Ukraine, most online transactions are via Privatbank. Bitcoin and ether are the most popular cryptocurrencies. Some shops also sell and buy ripple, litecoin, bitcoin cash, and other coins.

Several shops advertise the possibility to invest $500-$1,000 with a 20-42% annual return. Deposits are made via electronic money systems or Bitcoin for a maximum period of one year. Customer complaints can be posted on BestChange.ru web-site that is used as a reference tool. Exchangers try to resolve customer issues to ensure their reputation.

Exchanges
Exchanges store user cryptocurrency funds centrally in an offline cold wallet, and fiat currency in a dedicated account at a bank. (This is a practice that is enforced in some countries that have enacted regulation.) Funds needed to support ongoing operations are stored in an online hot wallet. Trades are recorded on an exchange internal ledger. Until a user deposits or withdraws, transactions are not reflected on a blockchain. You can exchange funds instantly at a spot rate, or post a trade with a target price. Exchanges are generally used for trading. Professional trading platforms like Bitfinex that facilitate margin trading and funding, are attractive for experienced traders. Bitfinex requires minimum account equity of $10,000 in cryptocurrency, and charges an inactivity fee. Exchanges that have UAH currency pairs have limited functionality for an experienced trader, and are chosen for ease of deposit/withdrawal in hryvnia, and relaxed user verification. High value individuals can be serviced on special terms. BTC Trade UA offers the most favorable exchange rate (better by 2%). Exmo has the highest trading volume in UAH, perhaps because of its perceived security due to international status (the company is registered in the UK), wider choice of trading pairs and deposit/withdrawal methods.

Ukrainian exchanges require an email address and phone number for registration. They do not service US citizens or accept payments from the United States. Deposit/withdrawal is made with a bank card transfer. Exchanges limit onetime bank transfer for deposit/withdrawal to an amount below the AML monitoring threshold of UAH 15,000. To use Visa/MasterCard USD/EUR to deposit/withdraw from Exmo, user verification is required (color scan of a national ID or international passport, bank statement or utility bill for residence address verification). On Exmo, withdrawal into AdvCash USD is 0%. AdvCash USD can then be withdrawn into Privat24 via an exchange shop with a 2% commission. Any instrument can be converted into Exmo code denominated in USD, EUR, UAH. Exmo does not charge a commission for depositing and withdrawing with codes. The codes can be converted into fiat currency via shops.

In addition to bitcoin and ether, Ukrainian exchanges facilitate trade in ripple, litecoin, and other coins. BTC Trade UA trades karbo, a cryptocurrency created by Ukrainian developers based on the CryptoNight algorithm.

p2p/LocalBitcoins
p2p service LocalBitcoins.com facilitates cash and online bitcoin and ether conversion. Cryptocurrency can be purchased online for hryvnia, with the money transferred via Privatbank cards. Limits range from UAH 2,500 to UAH 50,000. E-mail address is required to order currency from a trader via the web-site tool. LocalBitcoins requires a minimum deposit BTC 0.04 (UAH 10,000) to post a trade. Conversions initiated via the web-site tools use an escrow mechanism.
Bitcoin can also be purchased offline for US dollar and euro in Kiev, Odesa, Kharkiv, Lviv, Zhytomyr, and Poltava. Several traders aim at high value individuals and offer deals starting from $5,000. Meetings take place in restaurants, guarded halls of residential buildings, and offices. Bank departments are used for large cash transactions. LocalBitcoins records trades initiated through its tools, whereas many traders encourage direct contact providing phone number and messenger nickname.

Self-service terminals
Btcu.biz web-site offers to sell bitcoin and ether for cash via EasyPay and iBox cash machines (8,550 and 6,042 terminals all over Ukraine). A payment is made with WebMoney, a terminal issues a check with a code that is entered on Btcu.biz to confirm payment.

5. Mining in Ukraine

Strong IT skills and relatively low electricity tariffs combine in Ukraine. However, mining in Ukraine is a relatively small sector. Even cheap Ukrainian electricity cannot compete by price with hydropower used in China or Iceland, the big pools invest more and more into hardware increasing competition and slashing incomes of individual miners joining the pools, and Ukrainian climate is too hot for a large mining facility.

In Ukraine, average electricity price for a second class non-household consumer\(^74\) is around 0.09 $/kWh without VAT,\(^75\) which is lower than in the European Union countries.\(^76\) But it is still high for mining on an industrial scale.

According to market sources, businesses invest $25,000-$1,000,000 in a mining facility. Mining rigs produce a level of noise that is above what is advisable to be exposed to on a constant basis. ‘Hotels for miners’ are used, a service provider houses and maintains mining equipment for a fee. Total capacity of Ukrainian mining data centers is around 50 MW. The latest generation Antminer S9 consumes 1.5 kWh and makes 13.5 TH/s (it can run 13.5 trillion hash functions per second).\(^77\) Miners work 24/7, so the industry consumes around 1,200 MWh daily, which accounts to approximately 0.3%\(^78\) of the daily generation in Ukraine. By comparison, a household uses around 3,500 kWh per year. An estimated $50 million has been invested in mining in the country.

Mining centers mine different coins, but bitcoin can be used to illustrate the economics of the business. With the current Bitcoin network hash rate of around 30 million TH/s, Ukrainian data centers can ‘earn’ up to 9,800 BTC annually (calculated as a percentage of new coins issued annually).\(^79\) Hashare is explained in the Annex 2. With an average bitcoin price at $7,000, this translates to US$68.6 million annually. The average electricity cost for a non-household consumer

\(^74\) With an average monthly electricity consumption of less than 150 million kW per year, National Regulatory Commission for Energy and Utilities Decree (http://zakon0.rada.gov.ua/rada/show/v1052227-98)

\(^75\) National Regulatory Commission for Energy and Utilities web-site (http://www.nerc.gov.ua/?id=31814)

\(^76\) Eurostat, Electricity prices for non-household consumers - bi-annual data, Band ID: 2 000 MWh < Consumption < 20 000 MWh

\(^77\) Mining equipment arms race is slowing down, energy efficiency of an announced 7-10 nanometer chip will improve by 20% only compared to a previous 14-16 nm chip generation.

\(^78\) http://uaenergy.com.ua/post/30490/proizvodstvo-elektroenergii-v-ukraine-v-2017-g/

\(^79\) Ministry of Energy and Coal Mining (http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245265130&cat_id=245183225)

https://en.bitcoin.it/wiki/Controlled_supply
is 0.1 $/kWh including VAT. This means miners sell 64% of mined coins to cover electricity costs. They sell cryptocurrency on international exchanges and use accounts in Georgian banks. They then receive funds from a company in Georgia for equipment lease to pay for electricity in Ukraine.

The ability to mine cryptocurrency at home depends on availability of space remote from living areas to reduce noise impact, and connected capacity that is limited by transformers, safety devices, wiring. Connected capacity is higher in modern apartments and houses. Total capacity of electric devises connected to the network in a modern apartment must not exceed around 10kW, in an older apartment – 4.4 kW. Ether, monero, zcash, and other coins can be mined using GPUs (graphics processing unit) with a smaller investment from around $2,500. GPUs are also easier to sell than ASICs because they can be used for different computing tasks.

A number of companies sell mining equipment: MiningNetUa, Case.Kiev.Ua, Asic Trade, Hotmine, Bitmintech, Asic Kiev.Ua, Ukraine Mining Technology, Crypto-Farm, and others. Some of them also provide equipment housing and maintenance services, and set up turnkey data centers. There are currently 2,500 mining rigs sales advertisements on OLX, an online p2p marketplace. Hotmine designed a system that uses heat produced by a miner to heat water for apartments and private houses.

A Ukrainian is one of the founders of Bitfury, a manufacturer of mining equipment that operates large-scale mining centers in Iceland and Georgia. It is also a software developer. Today, its share in the disclosed Bitcoin network hashrate is less than 1%. An early adopter, in 2015-2016 Bitfury had 15% of the total mining power. Block reward at the time was 25 BTC. Bitfury signed memorandums with the Ukrainian government for implementation of land cadaster and state execution sale systems on blockchain.

6. Cryptocurrency and ICO Regulation Internationally

The Financial Action Task Force (FATF), an intergovernmental body that sets standards for the fight against money laundering, defines ‘virtual currency’ as a digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status. Cryptocurrency is a kind of virtual currency secured with cryptography.

Cryptocurrencies do not pose a systemic risk to any financial system, nor are they a rival to fiat currencies. Regulatory concerns about cryptocurrency are mostly about consumer protection, money laundering, and ‘scams’ or fraud. Most cryptocurrency regulation is conducted in the framework of existing financial markets legislation. Regulators issue consumer warnings, caution banks to implement enhanced monitoring for transactions related to purchase/sale of

---

80 What To Mine is a useful resource for a miner: [https://whattomine.com/](https://whattomine.com/)
81 [https://bitfury.com/](https://bitfury.com/)
82 [https://btc.com/stats/pool](https://btc.com/stats/pool)
84 [https://btc.com/stats/pool](https://btc.com/stats/pool)
cryptocurrencies, and impose standard provisions on tokens that are debt or equity instruments, and on cryptocurrency derivatives.

Initial Coin Offerings (ICO) are fundraising done by issuing tokens and selling them for either cryptocurrency or fiat currency. ICOs can be structured as a securities issue to give financial rights to participants, or as a crowdfunding and avoid regulation. Regulators monitor the ICO market to prevent fraud, and more closely regulate those that have securities issue features. In most developed markets, institutional investors are not allowed to own cryptocurrency assets for lack of price discovery, liquidity and transparency issues, and because blockchain is not legally recognized to generate a valid ownership ledger.

**Anti-Money Laundering**

Many countries, like Japan, Germany, Estonia, Sweden, the USA, Canada, Switzerland, South Korea, Singapore, Hong Kong require cryptocurrency exchangers and custody wallet providers to become ‘reporting entities’ under the AML regulation.

On May 30, 2018, the European Parliament adopted the fifth AML Directive that designated custody wallet providers and exchange service providers as obliged entities: they must be licensed/registered, apply customer due diligence controls including identification of beneficiaries, implement preventive measures and report suspicious transactions. The member states will have until the end of 2019 for implementation.

The commentary to the amendments to the AML Directive stated that current supervision instruments are not tailored sufficiently to ensure effective enforcement. For example, to combat the risks related to anonymity, national Financial Intelligence Units (FIUs) should be able to associate virtual currency addresses to the identity of their owners. By June 26, 2019, the European Commission shall assess and submit a report to the European Parliament and to the Council on the powers necessary to set-up and maintain a central database registering users’ identities and wallet addresses, accessible to national Financial Intelligence Units (FIUs).

FATF indicated in its report that convertible virtual currencies that can be used to move value into and out of fiat currencies, are likely to present money-laundering risks. FATF recommends that counties target points of intersection that provide a gateway to the regulated financial system rather than seek to regulate users who obtain virtual currency. Countries should also consider regulating institutions that send, receive, and store virtual currency.

Additional information on AML and cryptocurrency is provided in Annex 4.

**USA**

Cryptocurrency exchange platforms are regulated as money-transmission services that are obliged entities under the AML legislation, and fall under Financial Crimes Enforcement Network (FinCEN) purview. They need to be registered, maintain records, comply with reporting requirements, conduct customer due diligence, perform ongoing monitoring, etc.

---


The Federal District Court of New York adopted an important decision on cryptocurrency in a ruling on March 6, 2018 stating that:

‘In 2015, the CFTC (Commodity Futures Trading Commission) determined that virtual currencies, such as bitcoin, met the definition of ‘commodity’ under the CEA (Commodity Exchange Act). It should be noted that the definition of a ‘commodity’ under US law is extremely broad. Nevertheless, the CFTC does NOT have regulatory jurisdiction under the CEA over markets or platforms conducting cash or ‘spot’ transactions in virtual currencies or other commodities or over participants on such platforms. In fact, current law does not provide any U.S. Federal regulator with such regulatory oversight authority over spot virtual currency platforms operating in the United States or abroad. However, the CFTC does have enforcement jurisdiction to investigate through subpoena and other investigative powers and, as appropriate, conduct civil enforcement action against fraud and manipulation in virtual currency derivatives markets and in underlying virtual currency spot markets.’

This decision allowed the CME to go forward with cryptocurrency derivatives, under the supervision of the CFTC.

A division of the Securities and Exchange Commission (SEC) dedicated to ICOs (known as the Cyber Unit) in December 2017 filed charges in Brooklyn federal court targeting a scam that reportedly raised $15 million from thousands of investors by promising a 13-fold profit in less than a month.

At that time, SEC Chairman Jay Clayton issued a Statement on Cryptocurrencies and Initial Coin Offerings:

On cryptocurrencies: ‘Speaking broadly, cryptocurrencies purport to be items of inherent value (similar, for instance, to cash or gold) that are designed to enable purchases, sales and other financial transactions. They are intended to provide many of the same functions as long-established currencies such as the U.S. dollar, euro or Japanese yen but do not have the backing of a government or other body. It has been asserted that cryptocurrencies are not securities and that the offer and sale of cryptocurrencies are beyond the SEC’s jurisdiction. Whether that assertion proves correct with respect to any digital asset that is labeled as a cryptocurrency will depend on the characteristics and use of that particular asset. In any event, it is clear that, just as the SEC has a sharp focus on how U.S. dollar, euro and Japanese yen transactions affect our securities markets, we have the same interests and responsibilities with respect to cryptocurrencies. This extends, for example, to securities firms and other market participants that allow payments to be made in cryptocurrencies, set up structures to invest in or hold cryptocurrencies, or extend credit to customers to purchase or hold cryptocurrencies.’

On ICOs: ‘These offerings can take many different forms, and the rights and interests a coin is purported to provide the holder can vary widely. A key question for all ICO market participants: “Is the coin or token a security?” As securities law practitioners know well, the answer depends on the facts. For example, a token that represents a participation interest in a book-of-the-month club may not implicate our securities laws, and may well be an efficient way for the club’s operators’

---

to fund the future acquisition of books and facilitate the distribution of those books to token holders. In contrast, many token offerings appear to have gone beyond this construct and are more analogous to interests in a yet-to-be-built publishing house with the authors, books and distribution networks all to come. It is especially troubling when the promoters of these offerings emphasize the secondary market trading potential of these tokens. Prospective purchasers are being sold on the potential for tokens to increase in value – with the ability to lock in those increases by reselling the tokens on a secondary market – or to otherwise profit from the tokens based on the efforts of others. These are key hallmarks of a security and a securities offering.

Clayton went on to state: ‘By and large, the structures of initial coin offerings that I have seen promoted involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws. Generally speaking, these laws provide that investors deserve to know what they are investing in and the relevant risks involved.’

**Europe**

The Netherlands has adopted a ‘wait and see’ approach to the use of cryptocurrency. The Dutch Ministry of Finance published a letter on cryptocurrencies on March 8, 2018.90 The Minister warned on the associated risks for investors, and pledged to consult with the banks regarding cryptocurrency purchases on credit (British and US banks have banned the use of credit cards to buy cryptocurrencies). Referring to ICOs, the Minister said he would be consulting with the financial market supervisors to consider enforcement within the existing regulatory framework, and participate in developing an approach to ICOs at a European level. The letter also said that individual and business income on cryptocurrencies is taxable, but no guidance was issued. Half a million Dutch households hold cryptocurrency, and the investment in cryptocurrency amounts to 0.1% of their total savings.91 The Dutch government, including the Ministry of Finance, is experimenting with blockchain pilots, which focus on the implementation of government processes on smart contracts.92

The securities market regulator of France – the Autorité des Marchés Financiers (AMF), published a letter on April 5, 2018 with a generally favorable view of crypto-assets.93 AMF analyzes ICOs on a case-by-case basis and regulates those that fall under the definition of securities. Crypto-asset

---

90 https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/08/kamerbrief-over-de-ontwikkelingen-rondom-cryptovaluta
91 The ratio of people holding cryptocurrency to the total population in the Netherlands coincides with the Japanese figure, and is 3%. Kantar TNS survey of 8 February 2018: http://www.tnsnipo.com/nieuws/persberichten/aantal-nederlandse-beleggers-cryptovaluta-geexplod. A survey conducted by Kantar TNS in January involved 44,494 households. Since August 2017, the number of households that own cryptocurrency has exploded from 135,000 to 490,000 in February 2018. In some households, several people own cryptocurrencies, and a total number of crypto-investors is 580,000. Three in four households have invested in 2017 or 2018. In January 2018 alone, more Dutch people stepped in than in the whole 2016. Nevertheless, it is a very small part of the total savings and investments of Dutch households: barely 0.1% has been put in cryptocurrencies. The Dutch are cautious and invest low amounts: only one in four (24%) put in more than €1,000, although six months ago only 15% invested more than €1,000. Investors in cryptocurrencies are relatively young (38 years) and highly educated (68% have an HBO+, 30.1% of the population 15-75 years old have HBO+).
92 www.blockchainpilots.nl
93 http://www.amf-france.org/en_US/Actualites/Prises-de-paroles/Archives/Annee-2016%26xter=1&itsSearch=true&docId=workspace%3A%2F%2FSpacesStore%2F14de7c7-a7c37-44a8-13e-a8675023205&lastSearchPage=http%3A%2F%2Fwww.amf-france.org%2FmagnoliaPublik%2Famf%2Fen%2FResultat-de-recherche%3FTEXT%3Dcryptocurrency%3Den%25isSearch%3Dtrue%26simpleSearch%3Dtrue%26val id_recherche%3DOK%26xtmc=crypto&docVersion=1.0
derivatives are also subject to regulation. The AMF has said that the regulation of crypto-assets must be done ‘in a spirit of openness’ since they are a phenomenon of which we have yet to take full measure. It has also emphasized the need to develop a national and an international approach in parallel (crypto-assets are inherently cross-border).

At this stage, AMF proposes to give ICOs its optional approval/label when certain conditions are met. An issuer must be an identified legal entity registered in a country that is not on the EU ‘blacklist’. Subscribers must be more clearly identified than just by IP address or personal key, and the issuer must conduct complete customer due diligence. A transparent and secure issuance procedure must be in place with: a fixed issue price, an issue duration, size, including the treatment of oversubscription, comprehensive information on the role of the issuer, subscriptions held in escrow until the closing of the ICO. Information on the asset issued and the project financed must also include: a white paper describing in detail the rights acquired, a business plan, the technology used (possibly with an opinion from an independent expert). The information document carrying the AMF label accompanying an ICO would be more appropriate than a traditional prospectus and would provide additional guarantees against the specific risks of these transactions. Its optional nature would make it possible to develop more serious projects in France.

According to the AMF, the secondary market for crypto-assets is extremely opaque and thus more open to abuse. Platforms carrying out crypto-asset transactions must be regulated and supervised, and MiFID-II (Markets in Financial Instruments Directive) inspired transaction protection mechanisms must be applied, including pre-trade and post-trade transparency. There should also be a legal framework for the holding and transfer of ownership of crypto-assets. Blockchain technology is not recognized at present as being able to generate a ledger attesting the ownership of an asset, this is one of the reasons the AMF has not allowed regulated funds in France to invest in crypto-assets. Once satisfactory supervision has been established, the market for crypto-assets can be opened to collective investment schemes and, in so doing, to a wider group of investors.

In Germany, BaFin has classified cryptocurrency as a financial instrument comparable to foreign currency but not recognized as a legal tender by any country, and individuals and businesses that trade in cryptocurrencies are subject to licensing (including trading platforms that bring together buyers and sellers, like p2p web-sites). Although mining virtual currency in itself does not trigger an authorization requirement, if mining pools offer shares in proceeds from mined and sold virtual currency on a commercial basis, for instance, in exchange for computing power of a user, they generally are subject to authorization. The Federal Ministry of Finance issued an explanatory note that said speculative income and corporate income on cryptocurrency is taxed, mining is exempt, and cryptocurrency transactions are VAT exempt.

The Swiss regulator FINMA published its Guidelines on February 16, 2018. It regulates tokens based on their economic function:

- Payment tokens: Payment tokens (synonymous with cryptocurrencies) are tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods

---

94 A detailed analysis of the regulation in Germany (supervision and taxation) is given in the Annexes 4 and 5.
95 In accordance with the BaFin publication of 19 December 2013, virtual currencies are financial instruments within the meaning of section 1 (11) sentence 1 of the German Banking Act (KWG) https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html
96 https://www.finma.ch/en/authorisation/fintech/
or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer.

- **Utility tokens:** Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.

- **Asset tokens:** Asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on a blockchain also fall into this category.

The individual token classifications are not mutually exclusive. Asset and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). In these cases, the requirements are cumulative; in other words, the tokens are deemed to be both a security and a means of payment.

The exchange of a cryptocurrency for fiat money or a different cryptocurrency falls under Art. 2 para. 3 of the AML Act. The same applies to the offering of services to transfer tokens if the service provider maintains the private key (custody wallet provider).

*Sweden* and *Estonia* subjected cryptocurrency exchangers and custody wallet providers to the AML regulation as financial institutions.97 Financial market supervisors of the *United Kingdom,*98 *Finland,* *Denmark,* *Ireland,* *Belgium* and others have warned on the risk of ICOs and cryptocurrencies. The general consumer risk warnings issued by the regulators of the EU countries can be found on the EBA web-site (European Banking Authority).99

**Asia**

*China,* the biggest bitcoin producer with around 60-70% of the total mining power, has closed Chinese exchange platforms for cryptocurrency, and blocked foreign exchange platforms’ websites. However, major cryptocurrency exchanges like OKEx, Binance, Bitfinex, Huobi are headquartered or have offices in Hong Kong.100

*Hong Kong* regulates exchange and remittance service providers in virtual currencies as money service operators; it banned the trade in tokens that are ‘securities’. Hong Kong financial market supervisors urged financial institutions to carry out enhanced CDD and ongoing monitoring for accounts of customers that operate in the cryptocurrency field.

*Japan,*101 the biggest buying market, has introduced specific anti-money laundering and consumer protection regulation: exchangers must get registered, foreign exchange platforms must have an office in Japan to offer services. CDD and ongoing monitoring requirements were imposed, along with reporting requirements, cybersecurity, and segregation of user and own funds.

*Singapore*102 does not have a specific regulation governing virtual currency exchange service providers and custody wallet providers. Monetary Authority of Singapore (MAS) has published a general warning on cryptocurrencies on February 7, 2018. There are general safeguards in place

---

98 A detailed analysis of the regulation in the UK (supervision and taxation) is given in the Annexes 4 and 5.
100 A detailed analysis of the regulation in Hong Kong (supervision and taxation) is given in the Annexes 4 and 5.
101 A detailed analysis of the regulation in Japan (supervision and taxation) is given in the Annexes 4 and 5.
102 A detailed analysis of the regulation in Singapore (supervision and taxation) is given in the Annexes 4 and 5.
against AML risks connected with cryptocurrencies: enforcement agencies are taking precautionary measures, obliged entities report transfers to/from cryptocurrency dealers.

*South Korea*, the second largest market, has enacted AML regulation for cryptocurrency exchange platforms.\(^{103}\)

**Taxation and mining licensing**

Taxation will probably follow AML regulation, which will create a database for the tax authorities. Mining activity does not require a license in any country.

A more detailed analysis of international tax treatment of cryptocurrency in Canada, the UK, Germany, USA, Poland, Singapore, and Hong Kong is provided in the Annex 5. Reports on international regulation have been prepared by Axon Partners law firm and ForkLog Research.\(^{104}\)


## 7. Cryptocurrency Regulation in Ukraine

### 7.1. Cryptocurrency Definition / Status

Ukraine has not yet defined the term ‘cryptocurrency’. In 2014, the National Bank of Ukraine (the NBU) classified bitcoin cryptocurrency as a ‘surrogate currency’\(^{105}\) that has no real value and cannot be used by individuals and legal entities on the territory of Ukraine as a means of payment.\(^{106}\) Moreover, the NBU classified bitcoin as a ‘financial pyramid scheme’, and operations with bitcoin as suspicious transactions under the AML legislation.\(^{107}\)

In 2017, the NBU revised its approach to cryptocurrencies. The NBU, the National Securities and Stock Market Commission (NSSMC), and the National Commission for Financial Services (NCFS) issued a joint press release stating that cryptocurrency cannot be classified as funds, as a currency, as electronic money, or as a ‘surrogate currency’.\(^{108}\) In March 2018, the NBU repealed its letter of 2014 defining bitcoin as a ‘surrogate currency’.\(^{109}\)

The declaration of the Ukrainian financial authorities is essentially a negative definition. Ukrainian financial regulators need to define legally what cryptocurrency is if they are going to regulate it. It is difficult (sometimes impossible) to use cryptocurrencies for making/accepting payments in

---


\(^{105}\) [Based on para. 10 of Article 1 of the Law on the National Bank of Ukraine ‘surrogate currency’ is any documents in the form of banknotes that are different from the monetary unit of Ukraine, issued in circulation not by the National Bank of Ukraine and made for the purpose of making payments in economic turnover, except currency valuables.](https://www.bank.gov.ua/control/uk/publish/article?art_id=59735329)


\(^{107}\) [See NBU letter of December 8, 2014 No.29-208/72889 available at:](https://zakon2.rada.gov.ua/laws/show/v2889500-14)


Ukraine in a lawful manner, and the absence of a clear definition of cryptocurrency in the Ukrainian law is one of the key reasons.

### 7.2. Cryptocurrency Mining

Individuals and businesses in Ukraine engaged in mining are currently unregulated. The State Service of Special Communication and Information Protection of Ukraine has issued an official clarification that mining does not require a license. The Cabinet of Ministers is considering to classify cryptocurrency mining in the Classifier of Types of Economic Activity (KVED) but has not yet done so.

In recent years Ukrainian law enforcement agencies have raided business premises and confiscated mining equipment, encouraged by the unofficial status of cryptocurrency in Ukraine. The Secretary of the National Security and Defense Council of Ukraine at the meeting of the National Cybersecurity Coordination Center stated that unsupervised cryptocurrency circulation poses a money laundering threat, and that cryptocurrency can be used to facilitate the trade in arms and drugs, and finance terrorism, including in the temporarily occupied territories of Ukraine.

Ukrainian law enforcement officials typically apply the following Articles of the Criminal Code of Ukraine as a basis for the raids:

- Violation of copyright and related rights – for the use of unlicensed software.
- Appropriation, embezzlement or possession of property by way of abuse of official position – if mining equipment is found in the premises of state-owned enterprises.
- Smuggling – if mining equipment has been imported illegally.
- Fictitious entrepreneurship.
- Legalization (laundering) of proceeds from crime.
- Evasion from payment of taxes, fees, other mandatory payments.
- Financing of terrorism.

Such raids have stopped the activities of some mining companies, and the investigation and examination process can last for years. Frequently, cases are never submitted to courts.

---


114 Article 176 of the Criminal Code of Ukraine.

115 Article 191 of the Criminal Code of Ukraine.

116 Article 201 of the Criminal Code of Ukraine.

117 Article 205 of the Criminal Code of Ukraine.

118 Article 209 of the Criminal Code of Ukraine.

119 Article 212 of the Criminal Code of Ukraine.

120 Article 258-5 of the Criminal Code of Ukraine.

Thus, although it may not be necessary to regulate cryptocurrency mining more stringently than an ordinary business activity, the legal and regulatory framework should be clarified to make mining a legal entrepreneurial activity and establish clear taxation rules.\footnote{For our views on the subject see below \textit{Some thoughts on regulation} section.}

### 7.3. Sale and purchase / Settlements in cryptocurrency

Ukrainian courts have rejected claims to enforce payment obligations to transfer bitcoins in exchange for the services provided under a software development agreement.\footnote{\url{http://www.reyestr.court.gov.ua/Review/56686444}, \url{http://www.reyestr.court.gov.ua/Review/62052778}}

The District court of Kyiv ruled, in particular, that ‘a court decision cannot oblige the defendant to convey to the plaintiff things that have no signs of the material world’.\footnote{\url{http://www.reyestr.court.gov.ua/Review/56686444}} The panel of judges of the Appeal court confirmed the District court decision and rejected the arguments of a plaintiff that bitcoins are ‘property rights’. The Appeal court made a reference to the term ‘property rights’ defined in the law as any rights related to \textit{property}, other than property, including rights that are a constituent parts of property (rights of possession, disposal, use), as well as other specific rights (rights to conduct activities, use of natural resources, etc.) and rights of claim.\footnote{\url{http://www.reyestr.court.gov.ua/Review/62052778}} Thus, the Appeal court ruled that bitcoin had \textbf{no attributes of property rights}.\footnote{\url{http://www.reyestr.court.gov.ua/Review/62052778}}

Based on the Ukrainian Commercial Code, ‘property’ means a \textit{set of things and other valuables (including intangible assets)} that have a determined value, are produced or used in the activities of business entities and are reflected in their balance sheet or accounted for in other statutory accounting forms of these entities.\footnote{\url{http://www.reyestr.court.gov.ua/Review/56686444}} Based on accounting standards, an ‘intangible asset’ is a non-monetary asset that is non-material but identifiable.\footnote{\url{http://www.reyestr.court.gov.ua/Review/56686444}} At the same time, based on another legislative definition, ‘intangible asset’ means an object of intellectual property rights, as well as other similar rights, recognized in accordance with the procedure established by law, as the object of property rights.\footnote{\url{https://regulation.gov.ua/book/91-zeleno-kniga-reguluvanna-rinku-kriptovalut}}

The Civil Code of Ukraine defines the term ‘property’ more narrowly as a separate \textit{thing, a set of things}, as well as \textit{property rights} and responsibilities.\footnote{Section 1 of Article 190 of the Civil Code of Ukraine.} Cryptocurrency may not qualify as a ‘thing’ and, if one uses the arguments made by the Appeal court in the case described above, it would not qualify as a ‘property right’. Currently it is not clear whether cryptocurrencies may be attributed to \textit{property} under the Ukrainian legislation.

In May 2018, the EU-funded Better Regulation Delivery Office (BRDO) published a paper on legal/regulatory issues of cryptocurrency in Ukraine (Green Book on Cryptocurrency Markets Regulation).\footnote{\url{https://regulation.gov.ua/book/91-zeleno-kniga-reguluvanna-rinku-kriptovalut}}
The BRDO paper highlighted that:

- Cryptocurrency transactions are *neither prohibited nor regulated* in Ukraine;
- The exchange of cryptocurrency for fiat money is a *sale/purchase of ‘intangible assets’*;
- The exchange of one cryptocurrency for another cryptocurrency or goods/services is a *barter transaction*.

According to BRDO, cryptocurrencies are ‘intangible assets’ and ‘property’ under Civil and Commercial Codes.

BRDO suggests that an official confirmation should be issued by the Ministry of Finance/State Fiscal Service of Ukraine stating that cryptocurrency is a ‘property’, ‘intangible asset’ and ‘item of goods’ under the Ukrainian law so that transactions with cryptocurrencies receive official status in Ukraine.

### 7.4. Taxation by VAT

The Main Department of the State Fiscal Service (SFS) in the Kharkiv region, by letter No 5226/10/20-40-14-11-11 dated 09.09.2016, stated: ‘If transactions conducted by a taxpayer are not attributed to transactions that are tax-exempt or transactions that are subject to a zero or 7 percent VAT tax rate, then they are subject to value added tax at the basic rate in accordance with Article 194 of the Tax Code of Ukraine. Transactions for the supply of virtual currencies whose place of supply is located in the customs territory of Ukraine … are subject to taxation by value-added tax on the basis of Section V of the Tax Code of Ukraine.’

This letter/consultation was disputed in court, and it was resolved that the individual tax consultation/decision of the SFS should be cancelled. The Ukrainian court referenced the decision of the European Court of Justice (ECJ) – Supreme Court of the European Union in matters of European Union law of October 22, 2015. This ECJ ruling established that the exchange of traditional currencies for units of the ‘bitcoin’ virtual currency, and vice versa, performed in return for payment of a sum equal to the difference between, on the one hand, the price paid by the operator to purchase the currency and, on the other hand, the price at which he sells that currency to his clients, are transactions exempt from VAT, within the meaning of the EU Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

At the same time, the Higher Administrative Court of Ukraine accepted the SFS cassation appeal to the proceedings, so the decision of the Ukrainian courts on this issue may still be reconsidered.

If we assume that cryptocurrency is an *‘intangible asset’*, it would fall into the category of *goods* based on the Tax Code of Ukraine. The object of VAT taxation includes operations on the supply of goods, the place of supply of which is located in the customs territory of Ukraine. Supply of

---

133 http://www.reyesr.court.gov.ua/Review/62075942
135 Goods – tangible and intangible assets, including land plots, land shares, as well as securities and derivatives used in any operations, except for transactions of issue and redemption; see para. 14.1.244 of section 14.1 of Article 14 of the Tax Code.
136 Section 185.1 of Article 185 of the Tax Code.
goods means ‘any transfer of the right to dispose of goods as owner, including sale, exchange or donation of such goods, as well as supply of goods by a court decision.’

The place of supply of goods is determined as:

a) the actual location of the goods at the time of their delivery (except as provided in subparagraphs ‘b’ and ‘c’);

b) the place where goods are at the time of the start of their carriage or shipment, in case goods are transported or shipped by the seller, buyer or a third person;

c) the place where the assembly, mounting or installation is carried out, if goods are assembled, mounted or installed by the seller or on his behalf.

Cryptocurrencies are characterized by the absence of actual location – they neither exist in a physical place, nor are transported or sent (downloaded). They exist within the blockchain system distributed between the participants all around the globe. Thus, it is hardly possible to determine the place of supply of cryptographic goods. Consequently, it is disputable if any transaction for the supply of cryptographic goods can be an object of VAT taxation.

7.5. Corporate tax / simplified tax system, personal income tax

Corporate income from a source of origin in Ukraine and abroad, which is determined by adjusting financial result before tax (profit or loss) as determined in the financial statements of an enterprise in accordance with national or international financial reporting standards, is subject to income tax in Ukraine. Therefore, profitable transactions with cryptocurrencies may be viewed as subject to corporate income tax under the Ukrainian law.

Taxpayers of the first – third groups in the simplified tax system may accept payments for goods/works/services only in cash or cashless funds, which excludes the possibility to accept cryptocurrencies from customers as a payment. Such commercial entities would lose their single tax payer status for violation of this rule. It is, however, unclear whether or not tax payers of the simplified tax system may buy or sell cryptocurrency for cash/cashless funds in Ukraine.

Since the Tax Code of Ukraine does not exempt income on cryptocurrency transactions from taxation by personal income tax, such incomes may be viewed as taxable.

7.6. Anti-money laundering (AML) legislation

---

138 Section 186.1 of Article 186 of the Tax Code.
139 Para. 134.1.1, section 134.1, of Article 134 of the Tax Code.
140 Tax payers of the first group – private entrepreneurs selling goods in retail on the markets and/or household services individually with an annual turnover of less than UAH 300,000; second group – private entrepreneurs providing services, engaged in manufacturing and sale of goods, and restaurant business, with an annual turnover of less than UAH 1,500,000; and third group – other private entrepreneurs and legal entities with the annual turnover of less than UAH 5,000,000 (cira USD 200,000). See para. 291.4 of Article 291 of the Tax Code.
141 Para. 291.6 of Article 291 of the Tax Code.
142 Section 4 of para. 298.2.3 of Article 298 of the Tax Code.
143 Section 165.1, of Article 165 of the Tax Code.
The anti-money laundering regimen in Ukraine is instituted by the law ‘On prevention and counteraction to legalization (laundering) of the proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction’ (the ‘AML Law’). Financial institutions and certain types of business entities are treated as reporting entities and are obliged to comply with provisions of the law.

Article 9 of the AML Law prescribes obligatory customer due diligence (CDD) for one-time transfers executed without an account opening for the value equal to and above UAH 15,000 (circa $550), and other one-time transactions executed without establishment of business relations for the value equal and above UAH 150,000 ($5,500). Transactions for the value equal and above UAH 150,000 (circa $5,500) are subject to financial monitoring according to Article 15 of the AML Law.

Cryptocurrency exchangers and wallet providers operating in Ukraine are not treated as reporting entities under the AML Law and, thus, are not obliged to comply with CDD requirements. At the same time, under the EU-Ukraine Association Agreement, Ukraine is obliged to implement the AML Directives. The Fifth AML Directive adopted in May 2018, designates custody wallet providers and exchange service providers as reporting entities. The EU member states will have until the end of 2019 for implementation.

7.7. Currency control legislation

As of today, the currency control regulations of the National Bank of Ukraine are fragmented and cumbersome. The Decree on Currency Control is still the foundation for capital controls/foreign currency regulation in Ukraine. The Decree was implemented in 1993 to prevent the flight of foreign currency in the years of hyperinflation, and has been used since as an effective, albeit cumbersome, control system. The NBU has adopted more than one hundred regulations and instructions in order to implement the provisions of the Decree and other legislative acts in the area of capital controls.

As stated above, the NBU does not have a definition of cryptocurrency, and therefore does not treat it as a ‘currency valuable.’ It does not regulate the operations with cryptocurrencies to any extent. As the current currency control rules are based on the principle ‘everything which is not allowed is forbidden’, the exchange of cryptocurrencies into foreign currency and vice versa by the financial institutions registered in Ukraine and having the currency license of the NBU is not allowed.

The new law ‘On Currency and Currency Operations’ (the ‘Currency Law’) recently adopted by Verkhovna Rada will take effect as of February 7, 2019. The Currency Law is designed to simplify currency control regulations, and sets a general rule that all foreign exchange operations can be conducted freely if not prohibited by applicable legislation (‘everything which is not forbidden is allowed’ principle). The Currency Law empowers the NBU to enact detailed regulations by the NBU Resolutions as well as temporary ‘protection measures’ if a situation arises.

---

147 http://zakon0.rada.gov.ua/laws/show/2473-19
that threatens the stability of the financial system. Today it is unclear whether the NBU will enact any limitations for conversion between foreign currencies and cryptocurrencies.

### 7.8. ICO Tokens, Crypto Derivatives

The Initial Coin Offering (ICO) is an innovative funding model that allows bypassing the hurdles and costs of traditional investment models by way of issuing blockchain-based tokens and selling them for cryptocurrency or fiat money. There are at least two types of tokens issued via ICOs:

- **asset tokens** – asset tokens represent assets such as a debt or equity claim on the issuer. At least in some jurisdictions asset tokens are treated as securities;

- **utility tokens** – tokens intended to provide digital access to an application or service, and are not financial assets.\(^{148}\)

These terms are not yet defined in the Ukrainian legislation.

ICOs are regulated in other countries on a case-by-case basis. Many ICOs are structured as crowdfunding to avoid regulation. According to the Ukrainian Venture Capital and Private Equity Overview 2017, companies with ‘Ukrainian roots’ raised US $160.3 million via ICOs in 2017.\(^{149}\) These ICOs were not done in Ukraine, however.

Existing Ukrainian legislation does not allow for a security to be issued in the form of a token in a blockchain register. As the National Securities and Stock Market Commission (NSSMC) Chairman Timur Khromaev has noted:

‘In other countries, securities commissions can establish the status of certain investment assets. Unfortunately, the NSSMC does not have such a mandate.’\(^{150}\) This regulatory mandate was contained in the Draft Law No.7055, but this bill was rejected by the Rada on July 3, 2018, and will have to be resubmitted.

As for crypto derivatives, they may be classified as follows:\(^{151}\)

- **Cryptocurrency future** – a cash-settled derivative contract in which each party agrees to exchange cryptocurrency at a future date and at the agreed price.

- **Cryptocurrency contracts for difference (CFD)** – a cash-settled derivative contract in which the parties to the contract seek to secure a profit or avoid a loss by agreeing to exchange the difference in price between the value of the cryptocurrency CFD contract at its outset and at its termination.

- **Cryptocurrency option** – a contract which grants the beneficiary the right to acquire or dispose of cryptocurrencies.

Importantly, parties signing the derivative contracts do not need to own cryptocurrency itself.

---

\(^{148}\) See, for instance, the classification used by Switzerland’s FINMA in https://www.wengervieli.ch/WEVI/media/MediaLibrary/ICO/180216-Wegleitung-ICO-EN.pdf


\(^{150}\) https://news.finance.ua/ua/news/-/416004/status-kyrovalytut-ogolosheno-u-rozshuk

\(^{151}\) https://www.fca.org.uk/news/statements/cryptocurrency-derivatives
In Ukraine, an unsuccessful attempt was made to bring bitcoin futures to market. "The derivative contract failed because there was no market maker, and thus no liquidity. A Ukrainian resident company cannot be the market maker, as there is no possibility to legally buy bitcoin."\(^{152}\)

### 7.9. Legislative initiatives

As of October 2018, four cryptocurrency draft laws have been submitted to the Verkhovna Rada.

1. **The Draft Law No.9083\(^{153}\) of September 14, 2018 ‘On amendments to the Tax Code of Ukraine regarding the taxation of virtual assets in Ukraine’ submitted by MP O.Mushak.

The Draft Law No.9083 defines certain major terms as follows:

- **Virtual asset** – any form of a record within a digital distributed register, which can be used as a *means of exchange*, a *unit of account* or as a *store of value*. The term ‘virtual asset’ includes ‘cryptocurrencies’ and ‘asset tokens’;
- **Cryptocurrency** – a *virtual asset* in the form of a *token* that functions as a *means of exchange* or as a *store of value*;
- **Token** – a digital *unit of account* within a digital distributed register that has cryptographic protection;
- **Asset token** – a virtual asset in the form of a *token* that certifies the *proprietary* and/or *non-proprietary rights* of the owner of the token that correspond to the obligations of the *issuer of the token*;
- **Issuer of a virtual asset** – a person who, on its own behalf, disposes the virtual assets to their first owners and assumes the obligation under them to the owners of such virtual assets;
- **Mining** – an activity of a tax payer in conducting mathematical calculations aimed at maintaining a distributed ledger of digital records, including in order to receive virtual assets;
- **Distributed register** – a systematic database of records in the form of data that is stored, created and updated on the basis of algorithms that ensure its identity on all data carriers that create such a database.

For the purposes of personal income tax and corporate tax, profit from transactions with virtual assets is calculated as a positive difference between the income received by the taxpayer from the sale/exchange of virtual assets into currency valuables, and the expenses for their acquisition and/or mining. Exchange of one type of virtual asset into another virtual asset is not considered a virtual asset sales transaction and therefore is not taxed. The financial result of transactions with virtual assets is calculated separately and does not affect the financial result of other activities.

*Corporate tax* on the profit from operations with virtual assets is set at 5 percent for the period of 5 years (until January 1, 2025). After that period, a general corporate tax rate of 18 percent shall apply.

---

\(^{152}\) Said by Managing director of IG ‘Univer’ Oleksiy Sukhorukov (https://news.finance.ua/ua/news/-/416004/status-kryptovalyut-ogolosheno-u-rozhuk)

\(^{153}\) http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64597
Corporate entities can carry over losses from transactions with virtual assets to reduce the positive financial result in the next periods.

*Personal income tax* on the profit from operations with virtual assets in the reporting period is set at 5 percent.

Virtual assets transactions (issue of virtual assets, exchange of virtual assets of one type into another, sale of virtual assets (except of exchange/sale of asset tokens, which certify the rights to goods, the supply of which is subject to taxation)) are *exempt from VAT*.

Exchange of virtual assets for objects of civil law relations other than virtual assets is considered a virtual assets sale transaction at a price equal to a contract value of the object (objects) that are exchanged for virtual assets. If a certain tax rate is set for profit from transactions with asset tokens, which certify the rights to goods, the supply of which is subject to taxation, then this tax rate is applied to profit from transactions with such virtual assets.

A companion law to *Draft Law No. 9083* has been developed by MP O. Mushak and other stakeholders, but it has not yet been submitted to the Rada. This draft law provides that the National Securities and Stock Market Commission (NSSMC) will have regulatory powers over the virtual assets market (issuing regulatory acts, setting licensing requirements, conducting inspections, and imposing administrative and monetary penalties, etc.) and that professional participants in the market are designated as obliged entities under the AML legislation. The analysis below is based on the June 2018, version of the draft.

Professional participants in the market include:

1. **Licensed participants**: cryptocurrency exchanges and exchange shops. Licensed activities – activities on organization of trading of virtual assets for Ukrainian hryvnia, foreign currencies, other financial assets; exchange of virtual assets for Ukrainian hryvnia, foreign currencies, other financial assets.

2. **Custody wallets or wallet software providers** that control the private keys to access customer’s virtual assets.

3. **Self-regulatory organizations (SRO)** that regulates and controls the market under NSSMC supervision.

The following activities should *not be subject to licensing* under this Law:

- market activities of exchange of cryptocurrencies and other tokens if they involve the exchange (conversion) of cryptocurrencies or other tokens for other types of tokens only;
- storage of access keys to cryptocurrencies or other tokens owned by third parties;
- provision of software for storing access keys to cryptocurrencies or other tokens;
- activities of maintaining the work of a blockchain register (mining), regardless of the receipt of remuneration.

The draft law also amends the Civil Code of Ukraine to give a smart contract the status of a binding legal agreement. A smart contract is defined as an agreement in electronic form, the exercise of rights and obligations under which occurs by changing digital records in a distributed register. Execution of contract terms is automatic and happens in a defined sequence when conditions specified in a contract are met.
2. **Draft law No.7183**

Draft law No.7183 of October 6, 2017 ‘On cryptocurrency turnover in Ukraine’ was submitted by four MPs from the People’s Front political party (I.Yefremova, L.Denisova, I.Kotvitsky, S.Voytsekhovska) and one MP from the Petro Poroshenko Block (I.Rybak). The Draft Law 7183 establishes a relatively brief legal framework:

- ‘cryptocurrency’ is defined as a software code (a set of characters, numbers, and letters) that is an object of ownership, and functions as a means of exchange, the details of which are entered and stored in the blockchain system as data (software code);
- cryptocurrency exchangers and the cryptocurrency market in general should be regulated by the NBU;
- mined cryptocurrency is a property of a miner, mining income is taxed;
- cryptocurrency can be freely exchanged/converted into another cryptocurrency, electronic money, currency valuables, securities, services, goods, etc.

3. **Draft law No.7183-1**

Draft law No.7183-1 of October 10, 2017 ‘On stimulating the market of cryptocurrencies and their derivatives in Ukraine’ was submitted by MP S.Rybalka from the Radical Party of Oleg Liashko.

The Draft Law 7183-1 defines ‘cryptocurrency’ as a decentralized digital unit of value that functions as a means of exchange and saving, unit of account, which is based on mathematical calculations, and is a result of them, and has cryptographic protection. Cryptocurrency is a ‘financial asset’ for regulatory purposes.

The Draft Law 7183-1 proposes to stimulate cryptocurrencies mining by:

- implementing state, regional and local programs for mining stimulation;
- setting lower electricity tariffs for miners;
- providing preferential taxation.

The Draft Law 7183-1 designates the National Commission for Financial Services regulation (FSR) as the regulator of the cryptocurrency market, and delegates some powers to a self-regulatory organization (SRO). Cryptocurrency exchangers must get a license and comply with the rules set by the regulator. The Draft Law also sets a requirement to exchanges that at least 51% of their capital is owned by Ukrainian citizens, and a minimum statutory capital requirement at UAH 5 million ($200,000).

The Draft Law 7183-1 amends the AML Law of Ukraine in order to make cryptocurrency exchangers reporting entities. The Draft Law also raises the one-time transaction thresholds for CDD procedures: from UAH 15,000 to UAH 50,000 for money transfers without account opening, and from UAH 150,000 to UAH 500,000 for other transactions. The Draft Law 7183-1

---

154 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684
155 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710
156 The Tax Code does not have a definition of ‘financial asset’, the Code defines ‘financial investment’ as acquisition of corporate rights, securities, derivatives, other financial instruments (paragraph 14.1.81, section 14.1 of Article 14 of the Tax Code). Accounting standard 13 ‘Financial instruments’ lists financial assets: 1) monetary funds and equivalents; 2) a contracts that entitles to monetary funds or other financial assets; 3) a contract that grants a right to exchange financial assets on potentially favorable terms; 4) an equity instrument (https://bank.gov.ua/control/uk/publish/article?art_id=123706).
also amends the Law ‘On the Levy for Mandatory State Pension Insurance’ and imposes a levy on cryptocurrency sale transactions of individuals and businesses other than exchangers.

A companion draft law No.7246157 of October 30, 2017 ‘On amending the Tax Code for the cryptocurrencies market stimulation’ exempts cryptocurrency transactions of VAT, mining and cryptocurrency transactions are not an object of taxation, profit on cryptocurrency transactions is exempt of corporate tax and personal income tax (income of cryptocurrency exchangers is taxed at normal rates).

4. Draft law No.7485158 of January 15, 2018 ‘On digital economy development’ was submitted by MP S.Kaplin of the Petro Poroshenko Block.

The Draft Law 7485 defines cryptocurrency as bitcoin or other digital token used as a universal means of exchange in international turnover.

The Draft Law 7485 establishes very little in the way of regulation for the cryptocurrency market:

- cryptocurrency exchanges and exchange shops are allowed to hold accounts in Ukrainian banks and financial institutions abroad for settlements related to cryptocurrency transactions;
- cryptocurrency transactions are exempt from VAT, mining income and income on cryptocurrency transactions are not taxed;
- bitcoins and other cryptocurrencies (tokens) are exempt from the AML legislation;
- the Ministry of Finance of Ukraine sets accounting standards for cryptocurrency transactions – but there is no other regulation/oversight by the Ministry of Finance or other entities;
- any inspections of cryptocurrency businesses by the state authorities should be pre-approved with the Ministry of Finance.

To summarize, the cryptocurrency phenomena has attracted a great deal of attention from Ukrainian legislators recently. These initiatives are timely, given the rapid development of cryptocurrencies globally, and the extent of the market in Ukraine. The definition, legal status, and regulatory treatment of cryptocurrency needs to be addressed. However, the purposes of the laws vary significantly, as do the underlying concepts. Some of the draft laws are more detailed and logical in their development of the regulatory framework than others, but all of them lack clear reasoning regarding the choice of a regulator. For example, Draft Law 7183-1 does not provide any explanation at all as to why the National Commission for Financial Services should regulate the cryptocurrency market.

157 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62816
158 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63316
8. Some Thoughts on Regulation

8.1. Definition of cryptocurrency

Cryptocurrency in Ukraine poses some interesting challenges because of its legal status: neither prohibited nor regulated. Simply put, it is not defined in Ukrainian legislation. This is an essential first step in deciding who should regulate what and how. What kind of financial asset is cryptocurrency, how is it used, what are its functions? As US SEC Chairman Clayton suggests, the choice of regulator depends on the characteristics and uses of a particular financial asset.

The cryptocurrency draft laws discussed above all address the issue of the definition of cryptocurrency. All have slightly different formulations.

- Draft Law 9083 defines ‘cryptocurrency’ as a ‘token’ that functions as a means of exchange and saving value. ‘Token’ – a digital unit of account within a distributed ledger of digital records that has cryptographic protection.

- Draft Law 7183 defines ‘cryptocurrency’ as a software code that functions as a means of exchange, and the details of which are entered and stored in the blockchain system as a unit of data.

- Draft Law 7183-1 defines ‘cryptocurrency’ as a decentralized digital unit of value that functions as a means of exchange, saving value, and unit of account, is based on mathematical calculations, and is the result of them, and has cryptographic protection. Cryptocurrency is a ‘financial asset’ for regulatory purposes.159

- Draft Law 7485 defines ‘cryptocurrency’ as bitcoin or another digital token used as a universal means of exchange.

Cryptocurrency is defined somewhat differently in each of the four draft laws. This reflects the fact that there is no universally accepted definition of cryptocurrency. Nevertheless, there are some common elements to the definitions. First, ‘cryptocurrency’ functions as a ‘means of exchange’. Second, blockchain technology guarantees proper protection of data and accounting of tokens. Third, two definitions mention the cryptocurrency function of ‘saving value’.

These various definition all contain elements of the definition of money (currency), which is classified in terms of the three functions or services it provides: (i) it serves as a medium of exchange, as (ii) a store of value, and as (iii) a unit of account. Moreover, the underlying logic of cryptocurrency is for it to serve as a means of exchange of value. If it does not gain public acceptance as a currency, then it is likely to fail as a ‘financial instrument or asset’. It is also important to remember that most regulators internationally are regulating cryptocurrency based on its use and main characteristics. In Germany, BaFin has classified cryptocurrency as a financial instrument comparable to foreign currency but not recognized as a legal tender by any country.

159 The Tax Code does not have a definition of ‘financial asset’, the Code defines ‘financial investment’ as acquisition of corporate rights, securities, derivatives, other financial instruments (paragraph 14.1.81, section 14.1 of Article 14 of the Tax Code). Accounting standard 13 ‘Financial instruments’ lists financial assets: 1) monetary funds and equivalents; 2) a contracts that entitles to monetary funds or other financial assets; 3) a contract that grants a right to exchange financial assets on potentially favorable terms; 4) an equity instrument (https://bank.gov.ua/control/uk/publish/article?art_id=123706).
One problem common to the Ukrainian cryptocurrency draft laws is that they fail to distinguish ‘tokens’ by their underlying economic function. Only payment tokens are what is commonly called ‘cryptocurrency’.

- Payment tokens: Payment tokens (synonymous with cryptocurrencies) are tokens intended to be used as a means of value transfer. Cryptocurrencies give rise to no claims on their issuer. For example, bitcoin and ether do not entitle one to any claim on profits or decision-making ability inside the system.

As stated in the recently published report on virtual currencies, requested by the European Parliament’s Committee on Economic and Monetary Affairs, ‘virtual currencies are a contemporary form of private money’.

- Utility tokens: Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure. These are not regulated by financial markets regulators.

- Asset tokens: Asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on a blockchain also fall into this category.

These token classifications are not mutually exclusive. Asset and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). In these cases, the requirements are cumulative; in other words, the tokens are deemed to be both securities and means of payment.

8.2. Regulatory approach to payment tokens (cryptocurrencies)

Cryptocurrency should be regulated based on its economic characteristics and uses: a means of exchange/store of value/unit of account. In the case of Ukraine, cryptocurrency should be considered as having characteristics/uses that are more like a US$ or Euro than an equity. Viewed more as a ‘currency valuable’ (’valyutni tsinnosti’), cryptocurrencies should fall within the authority of the NBU. NBU regulation would probably mirror its current activities regarding currency exchanges, and could be based on the new Currency Law.

The new Currency Law lists currency valuables as: Ukrainian national currency (hryvnia), foreign currencies, electronic money denominated in hryvnia and foreign currencies, and bank metals. The main characteristic of currency valuables is liquidity. Cryptocurrencies are relatively liquid, are used for international settlements, and serve as a store of value.

Using cryptocurrencies as a ‘means of exchange’ for settlements may be viewed as blocked by current Ukrainian law which establishes the hryvnia as the only legal tender in Ukraine. In

---

161 http://zakon0.rada.gov.ua/laws/show/2473-19
particular, based on the Constitution of Ukraine ‘the monetary unit of Ukraine is the hryvnia’, and based on the Civil Code ‘The legal tender, mandatory for acceptance at nominal value throughout the territory of Ukraine, is the monetary unit of Ukraine – the hryvnia.’ At the same time, based on the same Article of the Civil Code ‘Foreign currency may be used in Ukraine in cases and in the manner prescribed by law.’

According to the recently adopted Currency Law, all settlements on the territory of Ukraine are conducted exclusively in hryvnias, except for settlements for: (1) foreign investment operations; (2) operations of banks to provide banking and other financial services on the basis of a banking license; (3) financial services operations, provided by non-bank financial institutions; (4) operations for placement of bonds denominated in foreign currency; (5) transactions in the sale and purchase of government securities denominated in foreign currency; and (6) other operations determined by the Customs Code of Ukraine and/or regulations of the National Bank of Ukraine.

Thus, if changes were introduced to the new Currency Law so that the definition of ‘currency valuables’ would include ‘cryptocurrencies’, then the NBU could issue regulations for settlements in cryptocurrencies, much the same as for foreign currencies.

With regard to the supervision over transactions in ‘currency valuables’, the Currency Law is designed based on the two-tier supervisory model. According to this model, two-tier regulation means that there are:

(i) licensing authority (the NBU) and Tax Authority (SFSU), the so called ‘currency supervision agencies’ and

(ii) banks and non-bank financial institutions with the Currency Licenses issued by the NBU in accordance with the Law, the so called ‘currency supervision agents’.

‘Currency supervision agencies’ and ‘currency supervision agents’ shall carry out ‘currency supervision’ over compliance of the relevant currency operations with the legislation, based on risk-oriented approach. The ‘currency supervision’ shall be carried out by the ‘currency supervision agencies’ and ‘currency supervision agents’ without interference in the relevant currency operations and activities of entities engaged in such operations, except in cases of detection and documentary evidence of violations by such entities of the requirements of currency legislation. ‘Currency supervision agents’ are accountable to the NBU, which establishes the rules and procedures for currency supervision.

The NBU as a ‘currency supervision agency’ may be assigned with regulatory powers for cryptocurrency conversion into fiat currency, other currency valuables, and vice versa, as well as for using cryptocurrency for payments/settlements under the Currency Law and underlying NBU regulations. Due to the money laundering potential of cryptocurrency as a funds transfer vehicle, the NBU may also act as AML ‘state financial monitoring’ entity setting appropriate AML policies in the field of payments / settlements / conversion of cryptocurrency into fiat currencies. The recent EU AML5 Directive designated custodial wallets and exchange services providers that

---

162 Article 99 of the Constitution of Ukraine
163 Part 1 of Article 192 of the Civil Code of Ukraine
164 Part 2 of Article 192 of the Civil Code of Ukraine
165 Section 2 of Article 11 of the Currency Law
166 Article 11 of the Currency Law
involve fiat currencies as obliged entities (EU states will implement the Directive until the end of 2019).

Enactment of the AML regulation will probably mean websites like LocalBitcoins will not be permitted (as is the case in Germany and in New York because of licensing requirements). The potential number of obliged entities in Ukraine is probably eight to ten: around six competitively positioned exchange shops that will consider taking on the costs of compliance, and two exchanges—BTC Trade UA and Kuna. The Exmo exchange that accepts transfers in Ukrainian hryvnia is registered the UK. The UK has not yet enacted the AML legislation for cryptocurrency, but it is possible that it will in the future.

8.3. Regulatory approach to asset tokens

The NSSMC is the logical choice as a regulator for the asset tokens. Professional actors that issue or trade asset tokens, must be licensed and supervised by the NSSMC.

In this regard, the Securities Commission should pay special attention to fraud, disclosure, and investor protection. In particular, the NSSMC should require professional market participants engaged in asset tokens to:

- clearly disclose to existing and potential clients information about: (i) their license for the activities, (ii) the conditions and rules for the provision of services, (iii) all the fees applicable to the transactions, (iv) the possible risks and consequences for customers arising from the conclusion, execution and termination of contracts with such market participant;
- have a written policy for handling customer complaints, and to report to the appropriate regulator. These procedures should be clear and posted prominently on their websites;
- meet basic requirements concerning management capability, risk management and financial soundness, and client fairness;
- conduct customer / investor due diligence;
- keep records on the individual transactions/personal data of their participants;
- implement measures to identify and manage potential conflicts of interest;
- meet minimum disclosure requirements and publish the financial reports on the regular basis;
- protect customer funds in cryptocurrency and fiat currency, and other assets;
- satisfy the requirements on the IT systems being in place and not prone to failure.

‘Asset tokens’ issued in ICOs by Ukrainian legal entities, should be regulated on par with other securities traded on Ukrainian exchanges (requirements to issuers, etc.). The same applies to derivative transactions with cryptocurrencies as an underlying asset.

Due to the inherent risks of asset tokens, the NSSMC should be empowered to impose capital requirements and/or other economic standards of prudential supervision. The NSSMC should
also act as AML ‘state financial monitoring’ entity setting appropriate AML policies for the professional actors on the asset tokens market.

8.4. Other important issues

Other important legal/regulatory issues that should be addressed include:

*Data protection and cybersecurity:* The regulation for data protection and cybersecurity should be focused on setting the requirements and reviewing internal controls (access and management of user funds and data, intrusion detection, malware protection, data back-up practices). For custody wallets (exchanges), requirements to segregate customer fiat- and cryptocurrency funds may apply; as well as keeping cryptocurrency (private keys) other than what is needed for day-to-day operations, in cold wallets with protected access and no availability from an online platform. Personal data protection measures might be based on the GDPR Regulation.\(^{167}\)

*VAT:* When cryptocurrency is used to pay for goods and services, it may be treated as an equivalent of a ‘currency valuable’. VAT should be due from the suppliers of any goods or services sold in exchange for cryptocurrencies. The value of the supply of goods or services on which VAT is due should be the hryvnia value of the cryptocurrency at the point the transaction takes place. When cryptocurrency is exchanged for hryvnia or foreign currencies, no VAT should be due (the current treatment of foreign currency exchange transactions).

*Corporate/Personal Income Tax/*Single tax for private entrepreneurs (CIT/PIT) on cryptocurrency transactions: An approach taken in many countries is that cryptocurrencies should be taxed similarly to similar financial assets.\(^{168}\) In Ukraine, one might consider establishing that the profits and losses of a company entering into cryptocurrency transactions should be reflected in their accounts and taxable under corporate income tax rates applicable to transactions with currency valuables. Alternatively, a more preferential taxation regime could be introduced for such transactions. If the Currency Law is amended so that the list of currency valuables includes cryptocurrency, income on exchange of cryptocurrency into fiat currency, and vice versa, will be exempt from personal income tax (PIT) according to Article 165.1.51 of the Tax Code. Additionally, in order to allow taxpayers in the simplified tax system to accept payments for provided goods/works/services in cryptocurrencies, one might consider making relevant changes to Article 291.6 of the Tax Code.

*Mining:* Cryptocurrency mining should not require a special license. However, some legislative provisions are needed to declare mining a legal entrepreneurial activity are needed (e.g., introducing a KVED). Transaction fees are paid to the miners on a voluntary basis and are not directly related to the service provided by the miners (system maintenance). The reward in the form of newly minted coins should not be considered a payment to the miners, since there is no exchange of service with an identifiable beneficiary.

*Smart contracts:* Amendments in the Civil and/or Economic Codes of Ukraine are required to set the rules for the ‘smart contracts’ form and enforceability in courts. The recently adopted Law of

---

\(^{167}\) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Ukraine ‘On Electronic Trust Services’,\textsuperscript{169} which defines the legal and organizational principles for the provision of the electronic trust services, including cross-border ones, as well as legal and organizational principles of electronic identification might be amended to cover ‘electronic keys’ and ‘authentication’ of the parties to ‘smart contract’.

\textsuperscript{169} http://zakon5.rada.gov.ua/laws/show/2155-19
**Annex 1. Bitcoin block structure**

<table>
<thead>
<tr>
<th>Bitcoin block:</th>
<th>Blockheader:</th>
<th>Blocksize</th>
<th>Prev blockheader hash: H( )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magic no: identifier of Bitcoin network message, always 0xD9B4BEF9</td>
<td>Software version</td>
<td>mrkl_root: H( )</td>
<td></td>
</tr>
<tr>
<td>Blockcounter</td>
<td></td>
<td>timestamp: Mar 28, 2018 11:43:25 AM</td>
<td></td>
</tr>
<tr>
<td>Transactions</td>
<td></td>
<td>Bits: target 17514a49</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>nonce: 573485735</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hash: 00000000000000000021f844fe...</td>
<td></td>
</tr>
</tbody>
</table>

Transactions are stored in a block in a merkle tree. It is a data structure in which each node is the hash of the concatenation of hashes of its children nodes (see the illustration below). The root of a merkle tree is a single hash representing all transactions. Merkle root is included in the block header. If a single detail in any of the transactions changes, so does the merkle root. Using a merkle tree is preferable over a hash chain or a hash of concatenated transactions because it allows for a much simpler test of whether a particular transaction is included in the block, and in the creation of Bitcoin addresses to improve security.

A hash function is a mathematical operation run on a digital data. It takes an input of any length and returns an output of a fixed length of 256 bits. SHA-256 is collision free: you cannot find two inputs that hash to the same value. If one sign is changed in the input, it results in a completely different value. The function was developed by NSA, and is the US government official standard. SHA-3 standard published in 2015 does not derive from SHA-2, but the latter satisfies current cryptographic security requirements in applications.

When a miner assembles a block header, she starts looking for a nonce value to have the block header hash to the value below the target value. The ‘nonce’ is a 32-bit field, so you try all 2^32 possible values of a nonce. But the current network difficulty is such that 2^32 or 4,294,967,296 tries will not ‘pay’ for a valid block. A miner then varies the block timestamp, extranonce field in the coinbase transaction that pays reward to the miner, or transaction set. And start over trying 2^32 nonce values. A solution for a valid block is difficult to obtain but easy to verify.
Bitcoin block header

<table>
<thead>
<tr>
<th>prev:</th>
<th>H( )</th>
</tr>
</thead>
<tbody>
<tr>
<td>mrkl_root:</td>
<td>H( )</td>
</tr>
<tr>
<td>timestamp:</td>
<td>Mar 28, 2018 11:43:25 AM</td>
</tr>
<tr>
<td>Bits:</td>
<td>target 17514a49</td>
</tr>
<tr>
<td>nonce:</td>
<td>573485735</td>
</tr>
<tr>
<td>hash:</td>
<td>0000000000000000021f844fe..</td>
</tr>
</tbody>
</table>

prev: | H( ) |
mrkl_root: | H( ) |
timestamp: | Mar 28, 2018 11:42:44 AM |
Bits: | target 17514a49 |
nonce: | 1655171816 |
hash: | 00000000000000000298aded.. |

12.5 BTC new coins + transaction fees
Coinbase transaction that issues new coins as a reward to a miner

**Bitcoin network hashrate, January 2015 – March 2018**

Source: [https://blockchain.info/charts/hash-rate?timespan=all](https://blockchain.info/charts/hash-rate?timespan=all)
Annex 2. Bitcoin network difficulty and hashrate

**Target**

- Is a 256-bit integer (a very large number)
- To be valid, a block header must hash to a value below the target
- The lower is the target, the lower is the probability for a block header to hash to a valid value
- There are $2^{256}$ possible values of a block hash
- Target is stored in each block header in the bits field in compact notation
- Used to keep block intervals at 10 minutes with the varying hashrate
- Target answers a question: what must be the probability of running a hash function once to result in a valid hash to keep the network trying for 10 minutes?
- The network is made one entity through a competition, like a lottery: the more people are buying tickets, the faster a lucky ticket will be drawn
- Target is automatically adjusted every 2016 blocks, or every two weeks
- Retarget formula: Next target = previous target * actual time it took to mine the last 2016 blocks / expected time to mine the last 2016 blocks (2 weeks, a constant)
- Initial target was set so that going through all $2^{32}$ possible values of a nonce field in a block header would yield a valid block.

**Network hashrate**

- Hashrate is how many times per second the network runs a hash function
- Difficulty is a ratio that shows by how many times it is more difficult to mine a block today than when Bitcoin started
- Difficulty = original target / target
- Difficulty at the time of writing: 3,462,542,391,192
- It answers a question: how many times should you go through all possible values of a nonce to find a valid block
- It is not used in Bitcoin code, but for people’s comprehension
- As more hashpower is added to the network, the difficulty automatically increases every 2 weeks to keep a constant parameter true that blocks must be found by the network every 10 minutes
- Network hashrate value is an approximation
- Hashrate/s = Difficulty * possible values of a nonce ($2^{32}$) / blocktime (600 seconds)
- Network hashrate at the time of writing is 24.49 EH/s (1 EH/s is 1,000,000,000,000,000,000 (one quintillion)) hashes per second
- A normal PC is useless here
- Antminer S9 makes 13TH/s. With current difficulty, it would be looking for a block for 34.5 years.
Annex 3. The Lightning Network

To create a one-way payment channel, Alice\textsuperscript{170} makes an opening transaction that deposits money into the channel and publishes it to the blockchain. The deposit can only be recovered if a transaction that releases it is signed by both Alice and Bob (or Alice alone after a timeout in case Bob is uncooperative). Let’s say Alice deposited 1 BTC and wants to pay Bob 0.1 BTC. She sends Bob a signed transaction, which spends the opening transaction output, and has two outputs: 0.1 BTC for Bob and 0.9 BTC ‘change’ for herself. (Bitcoin transactions include a reference to a previous transaction ‘output’ that is used as an ‘input’ into a new transaction, an ‘output’ is what emerges from a transaction.) She then decides to pay Bob another 0.1 BTC, a new transaction that spends the deposit has two outputs: 0.2 BTC for Bob and 0.8 BTC for Alice. Now both transactions that spend the deposit are valid and can be signed and published by Bob. Bob is interested in publishing the last transaction that gives him more money. Once he publishes a transaction to the blockchain, the payment channel is closed.

For a one-way payment channel like the one we have just described, we do not have to revoke or cancel old transactions. To implement a two-way channel, however, we need to be able to invalidate old transactions when we update the channel balance, because it can change in favor of either party. The parties must also be able to unilaterally take their money from the channel without having to wait until a timelock expires. Before the Lightning Network, the only way to invalidate an unconfirmed transaction was to spend one of its inputs, and get that transaction into the blockchain before the transaction one is trying to invalidate. That does not work if one wants to update the channel balance continuously with only the final balance hitting the blockchain (when a transaction reaches blockchain, the payment channel is closed).

The solution described in the Tadge Dryja’s white paper is to use a pair of revocable transaction outputs that spend from the opening transaction. They are a mirror image of each other. Suppose Alice and Bob each deposited 0.5 BTC into a multisignature safe. They now want to update their current balances from 0.5 BTC each to 0.6 BTC for Bob and 0.4 BTC for Alice. First, both parties create a new pair of commitment transactions. The commitment transaction that only Alice can broadcast has two outputs: one that pays Bob 0.6 BTC immediately on broadcast, and a revocable output that pays Alice 0.4 BTC with a locktime. Bob has a mirror transaction paying Alice 0.4 BTC immediately and 0.6 BTC himself with a delay. A delay is needed to give parties time to detect that a counterparty has broadcasted an old invalid commitment transaction and take all the money as described below.

Parties sign the revocable outputs using private keys specifically generated for this single transaction and exchange the signatures. When both parties have the revocable transactions, they exchange signatures for the commitment transactions. They then disclose their private keys used in previous commitment transaction. They do not disclose private keys used in transaction held by a counterparty as it would permit coin theft, only in a transaction that they hold. If a party incorrectly broadcasts an old commitment transaction, then the counterparty can take all the money because she has all the private keys used in the outputs of that transaction. To prevent this coin theft risk, they should destroy all old commitment transactions. One should monitor the blockchain to see if one’s counterparty has broadcast an invalidated commitment transaction, or delegate a third party to do so for a fee. Since the third party is only able to take action when the counterparty is acting maliciously, this third party does not have any power to force close of the channel. When

\textsuperscript{170} Alice and Bob are the names of fictional characters used for convenience and to aid comprehension.
parties wish to close out a channel cooperatively, they will be able to do so by broadcasting an output of the most current commitment transaction with no encumbering conditions.
### Annex 4. Supervisory regimens / AML regulation internationally

<table>
<thead>
<tr>
<th>Country</th>
<th>Supervising body</th>
<th>Supervision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)</td>
<td>In 2014, the Federal Government included dealers in virtual currency within the definition of Money Service Business (MSBs).(^{171}) Persons and entities that are “dealing in virtual currency” shall be financial entities or other entities deemed domestic or foreign MSBs, as the case may be. As required of all MSBs, persons, and entities dealing in virtual currencies would need to implement a full compliance program and register with FINTRAC under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). MSBs are required to register with FINTRAC and if successfully registered, to implement a complete anti-money laundering compliance regime. The Act captures foreign MSBs targeting Canada. Banks are prohibited from opening and maintaining accounts for MSBs that are not registered with FINTRAC (Bill C-31). MSB obligations include registering with FINTRAC (registration and update of information is done in an online system, registration must be renewed every two years), having a compliance program, identifying clients, keeping records, and reporting(^{172}). Compliance program – An MSB must develop and apply written compliance policies and procedures (and review it every two years), appoint a compliance officer responsible for the implementation and oversight of the compliance program, conduct and document a risk assessment of transactions and clients, mitigation measures and strategies, develop and maintain a written training program for employees, agents. CDD – An MSB must identify individuals and confirm the existence of entities (incl. obtaining information about the beneficial owners of an entity) for: opening an account, issuing or redeeming negotiable instruments of $3,000 CAD or more, making a remittances or transmissions of $1,000 or more, a foreign currency exchange of $3,000 or more, cash transactions of $10,000 or more (incl. multiple cash transactions of less than $10,000 each that total $10,000 or more within a 24-hour period, conducted by, or on behalf of the same individual or entity), suspicious transactions. To receive an EFT (electronic funds transfer) of any amount, an MSB must ensure it includes the originator information. In this context, reasonable measures could include contacting the institution that sent the payment instructions. For non-account-based relationships, MSBs are considered to be in a business relationship with every individual they have had to identify at least twice, and with every entity whose existence they had to confirm at least twice. If an MSB has not identified an individual or confirmed the existence of an entity because an exception applied, they are still considered to be in a business relationship, and must conduct ongoing monitoring and keep records.</td>
</tr>
</tbody>
</table>


MSB recordkeeping requirements – MSBs must keep the following records for at least five years from the date the report was submitted/record created:

- Suspicious transaction report records
- Large cash transaction records
- Records for transactions of $3,000 or more
- Records of remitting or transmitting funds of $1,000 or more
- Foreign currency exchange records
- Internal memorandum received or created in the normal course of business
- Records about ongoing service agreements
- Reasonable measures records.

Ongoing monitoring – MSBs must conduct ongoing monitoring for: detecting suspicious transactions that are required to be reported to the FINTRAC; keeping client identification, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date; re-assessing client's risk based on their transactions and activities; and determining whether the transactions or activities are consistent with information and risk assessment of that client. MSBs must conduct ongoing monitoring of any client that holds an account or of any person or entity once an MSB have conducted two transactions or activities, within five years, where they were required to verify the identity of the individual or confirm the existence of the entity. The frequency of ongoing monitoring activities is determined by the risk assessment. MSBs must keep a record of the ongoing monitoring measures taken for five years from the date they were created. The processes to monitor business relationships must be part of an MSB’s policies and procedures. During a FINTRAC examination, policies and procedures will be reviewed to ensure that the ongoing monitoring process is documented, MSBs are asked to demonstrate how the processes are implemented for every client risk-level. For example, a list of higher risk clients, the procedures, and the schedule used to monitor those business relationships.

Enhanced measures can include:

- Obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, Internet, etc.).
- Obtaining information on the source of funds or source of wealth of the client.
Reporting – MSBs are required to submit suspicious transaction reports to FINTRAC within 30 days of detecting a suspicious transaction or an attempt. Large cash transactions are reported within 15 calendar days. Electronic funds transfers: MSBs that send or receive client-initiated instructions to transfer $10,000 CAD or more internationally; either in a single transaction or in multiple transactions within a 24-hour period, must submit a report within 5 business days. All reports are submitted to FINTRAC electronically.

Penalties for non-compliance – FINTRAC can issue an administrative monetary penalty to reporting entities that are in non-compliance with PCMLTFA. FINTRAC may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance. Penalties may include the following:

- Failure to report suspicious transactions: up to $2 million and/or 5 years imprisonment.
- Failure to report a large cash transaction or an electronic funds transfer: up to $500,000 for the first offence, $1 million for subsequent offences.
- Failure to meet record keeping requirements: up to $500,000 and/or 5 years imprisonment.
- Failure to provide assistance or provide information during compliance examination: up to $500,000 and/or 5 years imprisonment.
- Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.

In accordance with the BaFin publication of 19 December 2013, virtual currencies are financial instruments within the meaning of section 1 (11) sentence 1 of the German Banking Act (KWG).

‘Currency exchanges’ offering to exchange legal tender for virtual currency or virtual currency for legal tender carry out trading for own account. This then constitutes trading for own account that requires authorization. This may be the case, for instance, when a person publicly advertises regular purchases and sales of virtual currency.
Those buying and selling virtual currency commercially in their own name for the account of others carry out principal broking services, which are subject to authorization. If no principal broking services are carried out by platforms, they may instead be operating a multilateral trading facility. This brings together, in the system and in accordance with pre-determined provisions, multiple third-party buying and selling interests in financial instruments in a way that results in a contract for the acquisition of these financial instruments. It is irrelevant whether the contract is then executed within the system or not. (LocalBitcoins does not operate in Germany due to licensing requirements.)

Although mining virtual currency in itself does not trigger an authorization requirement, if mining pools offer shares in proceeds from mined and sold virtual currency on a commercial basis, for instance in exchange for computing power of the user, they generally are subject to authorization.

Regulatory Acts: Money Laundering Act (Geldwäschegesetz – GwG), the Banking Act (Kreditwesengesetz – KWG), the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG)

All companies in the financial sector are expected to have formal AML policies. According to sections 4-6 of the GwG, obliged parties have to conduct and document risk assessment and implement preventive measures commensurate with risk profile. Obliged parties have to conduct customer due diligence, identifying customers and beneficiaries, politically exposed persons, relatives of such persons or known close associates. Obliged parties can apply simplified due diligence measures if they determine that there is a low ML risk, they have to take into account the risk factors listed in Annex 1 of the GwG. According to section 15 (2) of the GwG obliged parties have to apply enhanced due diligence measures if they determine in the course of their risk analysis or in individual cases that there might be a higher risk of money laundering, the risk factors are listed in Annex 2 of the GwG. Information on the purpose and the type of business relationship must be obtained and evaluated where it is not self-explanatory. A continuous monitoring of the business relationship or transactions processed must take place. As part of this continuous monitoring, the obliged parties must ensure that the relevant documents, data or information are updated within an appropriate timeframe taking into account the relevant risk. Ongoing monitoring is an important instrument for detecting unusual and suspicious activity. Suspicious transactions must be reported to the Central Customs Authority’s Financial Intelligence Unit (section 43 of the GwG and the BaFin’s “Auslegungs- und Anwendungshinweise”).

Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk.
Country | Supervising body | Supervision
--- | --- | ---
USA | Financial Crimes Enforcement | FinCEN issued a guidance and several rulings on virtual currencies: FIN-2013-G001, March 18, 2013 (Guidance)
FIN-2014-R011 and FIN-2014-R012, October 27, 2014 (Administrative Ruling)

The guidance describes the methodology for risk assessment, sources of information, customer and beneficial owner risk factors.

Risk factors may include: does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defense, the extractive industries or public procurement? Does the customer or beneficial owner have links to sectors that are associated with higher ML risk, for example certain Money Service Businesses, casinos or dealers in precious metals? Does the customer or beneficial owner have links to sectors that involve significant amounts of cash? Where the customer is a legal person or a legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business? Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example are any of the customer’s directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, or individuals who are known to influence the government and other senior decision-makers? Is the customer a credit or financial institution acting on its own account from a jurisdiction with an effective AML regime? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML obligations or wider conduct requirements in recent years? Is the customer’s or the beneficial owner’s background consistent with what the firm knows about their former, current or planned business activity, their business’s turnover, the source of funds and the customer’s or beneficial owner’s source of wealth? Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense? Is the customer’s ownership and control structure transparent and does it make sense? Can the customer’s or beneficial owner’s source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments? Is the explanation plausible?

FIN-2014-R001: Virtual currency exchangers and payment processors were designated as money service businesses (MSB) (money transmitter). The term “money transmission services” means “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”

FIN-2013-G001: Virtual currency exchangers and payment processors were designated as money service businesses (MSB) (money transmitter). The term “money transmission services” means “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”

A Money Services Business Guide to implementation of Bank Secrecy Act (BSA):

Registration Requirements – An MSB must register with FinCEN by the end of the 180-day period beginning on the day after the date it was established. MSBs are required to renew their registration every two years by December 31 at the end of the two-calendar year period following their initial registration. In addition, MSBs that are required to register are also required to prepare and maintain a list of agents, if any, each January 1 for the preceding 12-month period.

Civil and criminal penalties can be imposed for violations of anti-money laundering laws and regulations. Penalties can result in substantial fines and in prison terms. Any MSB that fails to comply with BSA reporting and record keeping requirements faces possible civil penalties of up to $500 for negligent violations and the greater of the following two amounts for willful violations: the amount involved in the transaction (up to $100,000) or $25,000. Under certain circumstances, businesses can also be held criminally liable for the acts of their employees. The maximum criminal penalty for violating a BSA requirement is a fine of up to $500,000 or a term of imprisonment of up to 10 years, or both.

AML Compliance Program – All MSBs are required to develop and implement an AML compliance program as required by section 352 of the USA PATRIOT Act and implemented by regulation at 31 CFR 103.125. Each AML compliance program must

176 31 CFR § 1010.100(ff)(5)(i)(A)
be in writing and must incorporate policies, procedures and internal control, and provide training of appropriate personnel. Strict customer identification and verification policies and procedures can be a financial institution’s most effective weapon against money laundering.

Funds Transfer Rules – An MSB that accepts an instruction to send a money transfer of $3,000 or more must verify the identity of the send customer and receiving customer and create and maintain a record of the money transfer, regardless of the method of payment (31CFR103.33(f)). The requirement to record funds transfers requires a money transmitter to: verify customer ID, record customer information, record transaction information, retain the record for five years from the date of the transaction.

Currency Transaction Report (CTR) – MSBs must file CTRs on transactions in currency involving more than $10,000, in either cash-in or cash-out, conducted by, through, or to the MSB on any one day by or on behalf of the same person. The CTR requirement requires an MSB to: verify and record customer ID, transaction information, retain the record for five years from the date of the transaction.

Currency Exchange Record – Each currency exchanger must create and maintain a record of each exchange of currency in excess of $1,000 (currency-in greater than $1,000, or currency-out greater than $1,000). The requirement to record funds transfers requires a money transmitter to: verify and record customer ID and information, record transaction information, retain the record for five years from the date of the transaction.

MSBs are required to file Suspicious Activity Reports (SAR). A SAR must be filed by an MSB when a transaction is both: suspicious, and $2,000 or more. A suspicious transaction is one or more of the following: involves funds derived from illegal activity, appears to serve no business or apparent lawful purpose, is designed to evade BSA requirements. A SAR must be filed within 30 days of detection of the suspicious transaction. It is illegal to tell any person involved in a transaction that a SAR has been filed. Some suspicious transactions require immediate action. A BSA provision (called a “safe harbor”) provides broad protection from civil liability to MSBs and their employees that file SARs or otherwise report suspicious activity. MSBs must maintain a copy of all SARs filed as well as the original or business record equivalent of any supporting documentation for a period of five years from the date of the report. Supporting documentation must be identified as such, and, although it is not to be filed with the report, supporting documentation is deemed to have been filed with the report. Upon request, MSBs must make all supporting documentation available to FinCEN and any other appropriate law enforcement or supervisory agencies (including the IRS in its capacity as BSA examination authority).

Examples of Some Common Red Flags: activity not consistent with the customer’s business or occupation, patterns (e.g., a customer receives a number of small money transfers and the same day, or within several days, initiates one or more send money
transfers to a person in another city or country in about the same amount), major changes in customer behavior, customer uses false ID, customer who presents any unusual or suspicious identification document or information, an individual customer without a local address, who appears to reside locally because he or she is a repeat customer, customer alters transaction upon learning that he/she must show ID, a customer who spells his/her name/address differently or uses a different name each time he/she initiates or receives a money transfer, uses a different numeration in address. A customer or group of customers who attempt to hide the size of a large cash transaction by breaking it into multiple, smaller transactions by, for example, conducting the smaller transactions: at different times on the same day, with different MSB cashiers/branches on the same day or different days. A customer or group of customers who conduct several similar transactions over several days, staying just under reporting or recordkeeping limits each time. A customer who receives payment of multiple money transfers that appear to have been purchased in a “structured” manner – organized in a way to evade reporting and recordkeeping requirements. MSBs should also watch out for the employee behavior: an employee whose lifestyle cannot be supported by his/her salary, an employee who is associated with unusually large numbers of transactions or transactions in unusually large amounts.

Record Retention – All BSA records must be retained for a period of five years and must be filed or stored in such a way as to be accessible within a reasonable period of time.

Reports That Can Help MSBs Identify Suspicious Transactions – Such reports can help identify customers who may be structuring transactions to evade BSA reporting and recordkeeping requirements or who are engaging in other unusual activity. Many money transmitters have established identification requirements at levels below the $3,000 threshold. Money transfer companies prepare, or have systems that generate, daily transaction reports and other reports that identify different groupings of transfer activity processed through their systems (e.g., corridor reports showing all transfers from country A to country B in a specific time period). These reports can help identify unusual patterns that may suggest possible money laundering.

United Kingdom Financial Conduct Authority (FCA)

FCA statement on the requirement for firms offering cryptocurrency derivatives to be authorised:178

‘Cryptocurrencies are not currently regulated by the FCA provided they are not part of other regulated products or services. Cryptocurrency derivatives are, however, capable of being financial instruments under the Markets in Financial Instruments Directive II (MiFID II), although we do not consider cryptocurrencies to be currencies or commodities for regulatory purposes under MiFID II. Firms conducting regulated activities in cryptocurrency derivatives must, therefore, comply with all applicable rules in the FCA’s Handbook and any relevant provisions in directly applicable European Union regulations.

<table>
<thead>
<tr>
<th>Country</th>
<th>Supervising body</th>
<th>Supervision</th>
</tr>
</thead>
</table>
| Japan   | Financial Services Agency (FSA) | Virtual currency exchange service providers are regulated by the Payment Service Act and Act on Prevention of Transfer of Criminal Proceeds. FSA issued lower level regulations detailing the requirements set in the Acts: Cabinet Office Ordinance concerning Virtual Currency Exchange Service Provider, and Guidelines for Administrative Processes Regarding Virtual Currency Exchange Service Providers. Payment Services Act (Act No. 59) 

Article 2 (5):

(i) property value (limited to one that is recorded on an electronic device or any other object by an electronic means, and excluding the Japanese currency, foreign currencies, and Currency-Denominated Assets) which can be used in relation to unspecified persons for the purpose of paying consideration for the purchase or leasing of goods or provision of services and

---

179 https://www.fca.org.uk/news/statements/initial-coin-offerings
180 https://www.fca.org.uk/news/statements/initial-coin-offerings
182 http://www.japaneselawtranslation.go.jp/law/detail/?dn=4&ex=56&y=13&ft=1&rc=02&co=01&ia=03&ky=payment+services+act&page=97
can also be purchased from and sold to unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system; and

(ii) property value which can be mutually exchanged with what is set forth in the preceding item with unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system.

Article 63-2, 63-3: Requires virtual currency exchange service provider to register with the FSA.

Article 63-5 (1): (i) A virtual currency exchange service provider must be a stock company, a foreign virtual currency exchange service provider must have a business office in Japan, and (ii) a representative domiciled in Japan. And (iv) and a system established for the proper and secure provision of services. (iii) Capital requirement.

Article 63-8: A virtual currency exchange service provider must take measures to protect customer’s personal data.

Article 63-11 (1): Virtual currency exchange service provider must separately manage own and customer’s fiat currency and virtual currency.

Article 63-12 (1): (i) Virtual currency exchange service provider must have a contract with a dispute resolution organization with expertise in virtual currency exchange. (ii) In the case where no such dispute resolution organization exists, to have the Operational Rules for Complaint Processing Measures and Dispute Resolution Measures in place.

Article 63-13: Bookkeeping requirement.

Article 63-14: Annual and on-request reporting requirement, including disclosing amount of customer funds under the management and transaction volumes.

Article 63-15: FSA can conduct special and on-site inspections.

Article 63-16: FSA may, within the limits necessary, order a virtual currency exchange service provider to take measures to improve the operation of its business or its financial conditions or other measures necessary.

Act on Prevention of Transfer of Criminal Proceeds (Act No. 22)\(^{183}\):

Article 2, Paragraph 2, Item 31: Virtual currency exchange service providers are subject to regulation under the Act.

\(^{183}\) http://www.loc.gov/law/foreign-news/article/japan-Bitcoin-to-be-regulated/
On May 30, 2018, the European Parliament adopted the fifth AML Directive\(^1\) that designated custody wallet providers and exchange service providers as obliged entities. The member states will have until the end of 2019 for implementation.

The AML Directive requires obliged entities to conduct customer due diligence (CDD) when establishing a business relationship, when carrying out an occasional transaction that amounts to EUR 15,000 or more (whether that transaction is carried out in a single operation or in several operations which appear to be linked), or constitutes a transfer of funds exceeding EUR 1,000. CDD is carried on the basis of documents and data from independent sources. Obliged entities must identify beneficial owners (the Member States are obliged to establish a central register that contains information about beneficial ownership), the source of funds where necessary, ensuring that CDD information is kept up-to-date (Articles 10 to 24).

Suspicious transactions reporting (Articles 33 to 35): all suspicious transactions, including attempted transactions, shall be reported to Financial Intelligence Units (FIU). Reported information could also include threshold-based information. Obliged entities must provide FIU, at its request, with information.

Record-retention (Article 40): CDD records and the supporting evidence and records of transactions are kept for a period of five years after the end of the business relationship or after the date of an occasional transaction.

Supervision (Article 47 and 48): the Directive requires that obliged entities be registered, regulator has to have adequate powers and financing.

Sanctions (Article 59): a public statement which identifies the natural or legal person and the nature of the breach, an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct, withdrawal or suspension

---

\(^1\) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
<table>
<thead>
<tr>
<th>Country</th>
<th>Supervising body</th>
<th>Supervision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singapore</td>
<td>Monetary Authority of Singapore (MAS)</td>
<td>Singapore does not have specific regulation governing virtual currency exchange service providers and custody wallet providers. MAS has published a general warning on cryptocurrencies on February 7, 2018. There are general safeguards in place against AML risks connected with cryptocurrencies: enforcement agencies are taking precautionary measures, obliged entities report transfers to/from cryptocurrency dealers. MAS currently regulates various types of payment services under the Payment Systems (Oversight) Act (Cap. 222A) (&quot;PS(O)A&quot;) and the Money-Changing and Remittance Businesses Act (Cap. 187) (&quot;MCRBA&quot;), enacted in 2006 and 1979 respectively. MAS wants to introduce a new payments legislation in the form of the proposed Payment Services Bill and implement a single payment services license. Virtual currency custody wallet providers and exchangers will fall under the regulation. MAS proposed that the regulation of licensees be calibrated according to their activities based on the risks or regulatory concerns that they pose, namely: money-laundering, user protection, interoperability, and technology risk. Virtual currency services will be regulated to introduce AML requirements for all providers, and oversight over technology risk management (technology risk management framework; system security, resiliency, and recoverability; strong authentication to protect customer data, transactions and systems). AML controls and procedures that financial institutions are obliged to institute include customer identification (including beneficial owners); keeping CDD files and transaction history for a period of at least 5 years after relationship termination; employee trainings; monitoring and reporting suspicious transaction to the Suspicious Transaction Reporting Office (STRO) in the Commercial Affairs Department (CAD), part of Singapore Police Force. The requirements on financial institutions are set out in MAS’ AML Notices.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Country</th>
<th>Supervising body</th>
<th>Supervision</th>
</tr>
</thead>
</table>
| Hong Kong | Customs and Excise Department (CED) | Non face-to-face CDD, Circular No.: AMLD 01/2018, 08 January 2018\(^{190}\)  
In Singapore, financial institutions (FI) can use a central state database MyInfo to access verified identity information. Where MyInfo is used, MAS will not require FIs to obtain additional identification documents. Where identity is obtained electronically through other non-face-to-face means including through transmission of scanned documents, FIs should apply additional checks to mitigate the risk of impersonation (real-time video conferences, biometric technologies, verifying customer identity through the document a customer signed with a secure digital signature issued by the Certificate Authority under the Electronic Transaction Act). |
| Hong Kong | Securities and Futures Commission (SFC) | Hong Kong does not regulate virtual currencies specifically, but existing laws provide sanctions against money laundering, fraud and cyber-crimes, whether or not virtual currencies are involved. The Hong Kong Government released a press statement on 14 March 2014,\(^{191}\) whereby exchange service providers and remittance service providers in virtual currencies are required to apply to the Customs and Excise Department (CED) for a money service operator license and fall under the Anti-Money Laundering Ordinance (Cap. 615) (AMLO).\(^{192}\) AML Ordinance is complemented by the Guidelines published by the relevant authorities.  
The Hong Kong Monetary Authority, the Securities and Futures Commission, the Office of the Commissioner of Insurance, and the Customs and Excise Department (CED) have issued circulars respectively to banks, securities brokers, insurers, and money service operators to urge them to carry out enhanced CDD and ongoing monitoring for customer accounts that operate in virtual currencies business. Financial institutions are also reminded of their statutory duty to report suspicious transactions to the Joint Financial Intelligence Unit. An example of such circular issued by CED on 21 March 2014: MSSB/MIS_2/2014.\(^{193}\)  
Following a statement on ICOs\(^{194}\) released on 5 September 2017, the Securities and Futures Commission (SFC) has sent letters to seven cryptocurrency exchanges in Hong Kong or with connections to Hong Kong warning them that they should not trade |

\(^{191}\)Hong Kong Government press release (http://www.info.gov.hk/gia/general/201403/14/P201403140751.htm)
\(^{194}\)ICOs are fundraising done by issuing tokens and selling them for cryptocurrency or fiat currency. ICO issuers are typically assisted by market professionals such as lawyers, accountants and consultants for advice to structure the offering as utility tokens to fall outside the purview of the SFO and to circumvent the scrutiny of the SFC. (http://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/statement-on-initial-coin-offerings.html)
cryptocurrencies which are “securities” as defined in the Securities and Futures Ordinance (SFO) without a license. The SFC has also written to seven ICO issuers. Most of them confirmed compliance with the SFC’s regulatory regime or ceased to offer tokens to Hong Kong investors.

AML Ordinance

Part 2 CDD requirements

Financial institutions are required to have established procedures. CDD measures must be carried out before establishing a business relationship, before carrying out an occasional transaction for $120,000 HKD or above (whether the transaction is carried out in a single operation or in several operations that appear to be linked), before carrying out a wire transfer or a money remittance for $8,000 or above (whether in a single operation or in several operations that appear to be linked). Financial institutions must continuously monitor business relationship with the customer ensuring CDD file is up-to-date, and monitor unusual and large transactions. Identification must be done against documents. When a customer is not physically present for identification, provided information must be additionally verified against available data. Financial institutions must ensure that the first payment is made from an account opened in the customer’s name with an authorized institution/institution that has measures in place to ensure compliance with requirements similar to those imposed under the Ordinance. For transactions identified as high risk, approval form senior management, identification of source of wealth and source of funds is required. Contravention of the Ordinance entails a fine of $500,000-$1,000,000 or imprisonment for 6 month -7 years.

The CED and other agencies have agreed to remove the address verification requirements currently set out in the AML Guidelines. As a result, FIs are only required to collect address information of customers and/or beneficial owners without the need to collect documentary evidence.

---

196 https://www.elegislation.gov.hk/hk/cap615
197 Customs and Excise Department, Guideline on Anti-Money Laundering and Counter-Terrorist Financing – Address Verification Requirements, MSSB/Guide_01/2017, 11 October 2017
Part 3 Recordkeeping requirements

An original or a copy of documents, and a record of the data and information obtained in the course of identifying and verifying a customer or beneficial owner, files relating to a customer account and business correspondence with a customer, transaction details are kept for a period of at least 5 years.

Part 4 Disciplinary Actions

CED may take disciplinary actions: publicly reprimand a financial institution, order to take any action to remedy a contravention, order to pay a pecuniary penalty not exceeding the amount that is the greater of (i) $10,000,000; or (ii) 3 times the amount of the profit gained, or costs avoided as a result of contravention.

Part 5 Regulation of Operation of Money Service, Part 3 Supervision and Investigations

CED can revoke or suspend the license. CED approval is required to appoint directors. A licensee must not operate at any premises other than specified in the license. And notify CED of any significant changes in the business. CED can carry routine inspections, and make information inquiries. By court order, CED officer can enter and search the premises, seize documents, cash, other articles, make copies of documents and files. Detain people. Noncooperation and attempts to defraud investigators can entails a fine of $1,000,000 or imprisonment for 6 month -7 years.

Part 6

The “Anti-Money Laundering Review Tribunal” has the same powers as the Court of First Instance in the AML related cases.
### Annex 5. Taxation internationally

<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada Revenue</td>
<td>CRA Factsheet 2015: What you should know about digital currency[^198]</td>
<td>CRA Factsheet does not designate the treatment of mining. Provided here is a possible interpretation of the legislation. Where a taxpayer mines digital currency in a commercial manner, in computing the taxpayer’s income from the business for a taxation year, the value of property described in the inventory at the end of the year must be determined. Goods and services tax/Harmonized sales tax (GST/HST) obligations may potentially arise in mining.</td>
<td>Exempt</td>
</tr>
<tr>
<td>Agency (CRA)</td>
<td>1/ Where digital currency is used to pay for goods or services, the rules for barter transactions apply. Barter transactions are within the purview of the Income Tax Act. Such transactions can therefore result in income or expense as contemplated by sections 3 and 9 thereof or can result in the acquisition or disposition of capital property, eligible capital property, personal-use property or inventory. Goods and services tax/Harmonized sales tax (GST/HST) also applies on the fair market value of any goods or services you buy using digital currency. For example, paying for movies with digital currency is a barter transaction. The value of the movies purchased using digital currency must be included in the seller’s income for tax purposes. The amount to be included would be the value of the movies in Canadian dollars (CRA Interpretation Bulletin IT-490, Barter Transactions). 2/ Digital currency can also be bought or sold like a commodity. Any resulting gains or losses could be taxable income or capital for the taxpayer. Transactions on income account: transactions of a trader or dealer in digital currency, gain or loss on a “short sale”. On capital account: long-term investment (Paragraphs 9 to 32 of Interpretation Bulletin IT-479R, Transactions in Securities).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>Income denominated in virtual currency is always recorded in fiat</td>
<td>Mining is a nontaxable activity. Transaction fees are paid to the</td>
<td>Virtual currency conversion into fiat currency and fiat currency into virtual currency is designated as turnover and facilitation of turnover of the legal means of payment, and as such is exempt of VAT according to VAT Act (UstG), § 4 Tax exemptions, no.8 letter b.</td>
</tr>
<tr>
<td>Central Tax</td>
<td>currency equivalent at the time of goods or service supply in accordance with the EU VAT Directive. Article 91 (2): The exchange rate applicable shall be the latest selling rate recorded, at the time VAT becomes chargeable, on the most representative exchange market or markets of the Member State concerned, or a rate determined by reference to that or those markets. For individuals, virtual currency sale is designated as a private sale within the meaning of Income Tax Act (Section 23(1) no. 2, EStG). Private sales that do not exceed a total of EUR 600 annually (for all types of private sales) are tax exempt. Private sale of property held for more than one year is tax exempt. Otherwise, capital gains tax arises. Capital gains realized by an enterprise from disposal of business assets are treated as ordinary business income. Tax exemption for one year holding does not apply.</td>
<td>The reward in the form of newly minted coins is not a payment to the miners (system maintenance). The exchange rate applicable shall be the latest selling rate recorded, at the time VAT becomes chargeable, on the most representative exchange market or markets of the Member State concerned, or a rate determined by reference to that or those markets.</td>
<td>Trading platforms provide electronic data processing services that are taxed. However, if an operator of such platform buys and sells virtual currency as intermediary in his/her own name, these transactions are exempt of VAT (VAT Act (UstG), § 4, no. 8, letter b). Digital wallets offered for a fee qualify as the “other services provided electronically” that are taxed if the place of supply is in Germany according to VAT Act (UstG), § 3a paragraph 2 and paragraph 5 sentence 1.</td>
</tr>
<tr>
<td>Central Tax</td>
<td>Income denominated in virtual currency is always recorded in fiat</td>
<td>Mining is a nontaxable activity. Transaction fees are paid to the</td>
<td>Virtual currency conversion into fiat currency and fiat currency into virtual currency is designated as turnover and facilitation of turnover of the legal means of payment, and as such is exempt of VAT according to VAT Act (UstG), § 4 Tax exemptions, no.8 letter b.</td>
</tr>
<tr>
<td>Office</td>
<td>currency equivalent at the time of goods or service supply in accordance with the EU VAT Directive. Article 91 (2): The exchange rate applicable shall be the latest selling rate recorded, at the time VAT becomes chargeable, on the most representative exchange market or markets of the Member State concerned, or a rate determined by reference to that or those markets. For individuals, virtual currency sale is designated as a private sale within the meaning of Income Tax Act (Section 23(1) no. 2, EStG). Private sales that do not exceed a total of EUR 600 annually (for all types of private sales) are tax exempt. Private sale of property held for more than one year is tax exempt. Otherwise, capital gains tax arises. Capital gains realized by an enterprise from disposal of business assets are treated as ordinary business income. Tax exemption for one year holding does not apply.</td>
<td>The reward in the form of newly minted coins is not a payment to the miners (system maintenance). The exchange rate applicable shall be the latest selling rate recorded, at the time VAT becomes chargeable, on the most representative exchange market or markets of the Member State concerned, or a rate determined by reference to that or those markets.</td>
<td>Trading platforms provide electronic data processing services that are taxed. However, if an operator of such platform buys and sells virtual currency as intermediary in his/her own name, these transactions are exempt of VAT (VAT Act (UstG), § 4, no. 8, letter b). Digital wallets offered for a fee qualify as the “other services provided electronically” that are taxed if the place of supply is in Germany according to VAT Act (UstG), § 3a paragraph 2 and paragraph 5 sentence 1.</td>
</tr>
<tr>
<td>USA</td>
<td>IRS Notice 2014-21&lt;sup&gt;200&lt;/sup&gt;</td>
<td>IRS Notice 2014-21 A-8: When a taxpayer successfully “mines”</td>
<td>In the US, sales tax is governed at the state level and no federal sales tax exists.</td>
</tr>
<tr>
<td>Internal Revenue</td>
<td>IRS Notice 2014-21&lt;sup&gt;200&lt;/sup&gt;</td>
<td>IRS Notice 2014-21 A-8: When a taxpayer successfully “mines”</td>
<td>In the US, sales tax is governed at the state level and no federal sales tax exists.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service (IRS)</td>
<td>A-1: For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.</td>
<td>virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A-3: A taxpayer who receives virtual currency as payment for goods or services must, in computing gross income, include the fair market value of the virtual currency, measured in U.S. dollars, as of the date that the virtual currency was received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A-6: If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A-7: The character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer. A taxpayer generally realizes capital gain or loss on the sale or exchange of virtual currency that is a capital asset in the hands of the taxpayer. For example, stocks, bonds, and other investment property are generally capital assets. A taxpayer generally realizes ordinary gain or loss on the sale or exchange of virtual currency that is not a capital asset in the hands of the taxpayer. Inventory and other property held mainly for sale to customers in a trade or business are examples of property that is not a capital asset.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A-12: A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property. For example, a person who in the course of a trade or business makes a payment of fixed and determinable income using virtual currency with a value of $600 or more to a U.S. non-exempt recipient in a taxable year is required to report the payment to the IRS. Examples of payments of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Income taxes</td>
<td>Mining</td>
<td>VAT</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>--------</td>
<td>-----</td>
</tr>
</tbody>
</table>

For businesses which accept payment for goods or services in cryptocurrency there is no change to when revenue is recognized or how taxable profits are calculated. VAT will be due from suppliers of any goods or services sold in exchange for cryptocurrency. The value of the supply of goods or services on which VAT is due will be the sterling value of the cryptocurrency at the point the transaction takes place.

If a profit or loss is within trading profits:

1/ The profits and losses of a company entering into transactions involving cryptocurrency would be reflected in accounts and taxable under normal corporation tax (CT) rules.

2/ The profits and losses of a non-incorporated business on cryptocurrency transactions must be reflected in their accounts and will be taxable on normal personal income tax (IT) rules.

If a profit or loss is not within trading profits:

Gains and losses incurred on cryptocurrencies are chargeable or allowable for capital gains tax (CGT)\(^{202}\) if they accrue to an individual or, and for CT if they accrue to a company.

1/ Income received from mining activities will be outside the scope of VAT because there is an insufficient link between any services provided and any consideration received.

2/ Income received by miners for other activities, such as for the provision of services in connection with the verification of specific transactions for which specific charges are made, will be exempt from VAT under Article 135(1)(d) of the EU VAT Directive as falling within the definition of ‘transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments’.

3/ When cryptocurrency is exchanged for Sterling or for foreign currencies, no VAT will be due on the value of cryptocurrency itself.


<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan National Tax Agency (NTA)</td>
<td>NTA Letter “Calculation methods of income on virtual currency” of December 1, 2017203</td>
<td>NTA Letter of 1 December 1, 2017</td>
<td>Cabinet Order for Partial Revision of the Order for Enforcement of the Consumption Tax Act of March 31, 2017205</td>
</tr>
<tr>
<td></td>
<td>(2), (3) When virtual currency is used to pay for goods or services, or converted into another virtual currency, the difference between the acquisition price in yen and the price of virtual currency in the payment transaction, is a taxable loss or gain. (Example) Purchased 4 bitcoins at 2,000,000 yen (including fee) on March 9th. Used 0.3 bitcoins on September 28 (including fee) to purchase 155,000 yen. The income amount is 5,000 yen: 155,000 yen − (2,000,000 yen ÷ 4 BTC) × 0.3 BTC = 5,000 yen. (4) For multiple sales and purchases, a moving or total average method is used to determine virtual currency price. (5) When virtual currency is acquired as a result of a hard fork,204 income will be generated at the time of use (it has no market value at the time of branching). Acquisition price will be zero. (6) Income arising from transactions with virtual currency is classified based on transaction substance, as subject to business income tax or miscellaneous income tax for individuals (Income Tax Law Article 35). (7) Losses incurred in transactions with virtual currencies cannot be used to offset other income types.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

204 When a new currency is created as a branch of existing currency through a hard fork (or a non-backward compatible protocol update), holders will have an equal amount of both old and new currency if their wallet supports the newly created currency. Bitcoin Cash and Bitcoin Gold are examples of such forks of Bitcoin. 205 https://kanpou.npb.go.jp/old/20170331/20170331t00007/20170331t000070250f.htm?utm_campaign=newsletter&utm_source=newsletter&utm_medium=email
### Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poland</td>
<td>The Ministry of Finance statement of 4 April 2018^206 (now suspended after protests)</td>
<td>n/inf</td>
<td>The Ministry of Finance statement of 4 April 2018^210 (now suspended after protests)</td>
</tr>
</tbody>
</table>
| National Revenue Administra on                        | The use of cryptocurrency to pay for goods or services is considered as a property disposal, as well as conversion between cryptocurrencies, and cryptocurrency and fiat currencies. Poland charges a 1% Civil Law Activities Tax (CLAT) on the sale or exchange of property rights from the buyer. Polish investors in cryptocurrency protested against this treatment and draw up a petition.\(^{207}\) The Ministry suspended taxation to conduct an in-depth analysis.\(^{208}\) **PIT (PIT Act^209\)**  
  **Income obtained through sale/exchange of cryptocurrency is taxed as either income on sale of private property (18%, 32% (applied to income exceeding $24,000 for all types of income), or as business income (if trading activity is of a paid nature, is carried out in an organized and continuous manner). Natural persons conducting business activity are taxed according to the tax scale. These individuals, at their request, may tax their income with the 19% flat-rate tax.** |

---

\(^{206}\) [Source](https://www.mf.gov.pl/ministerstwo-finansow/wiadomosci/aktualnosci/ministerstwo-finansow2/-/asset_publisher/M1vU/content/skutki-podatkowe-obrotu-kryptowalutami-w-pit-vat-i-pcc#)  
\(^{207}\) [Source](https://www.change.org/p/polish-goverment-stop-regulacjom-rynk-kryptowalut-stop-for-cryptocurrencies-market-regulations?i=284532&sfmtc_sub=625158731&i=32_HTML&u=51482402&mid=7233052&jb=43934)  
\(^{208}\) [Source](https://stooq.pl/n/?f=1235115)  
\(^{210}\) [Source](https://www.mf.gov.pl/ministerstwo-finansow/wiadomosci/aktualnosci/ministerstwo-finansow2/-/asset_publisher/M1vU/content/skutki-podatkowe-obrotu-kryptowalutami-w-pit-vat-i-pcc#)
Depending on the scale of business conducted, upon meeting specific criteria, the taxpayer may request the application of simplified taxation forms, i.e.:

- tax on registered income (tax calculated without deducting tax-deductible costs);
- fixed tax rate (the rate is determined by the tax office depending on the type of business).

Printout of transaction history obtained from an online exchanger and confirmed with a signature, and a bank statement are accepted as supporting documents. The statement specifies tax declaration lines where income/loss on cryptocurrency transactions is reported.

**Singapore Inland Revenue Authority of Singapore**

Income Tax Treatment[^211]

Accepting virtual currency as a payment

Businesses that accept virtual currencies as a payment are subject to normal income tax rules. They should record the sale based on the market value of the goods or services in Singapore dollars. The same applies for businesses which pay for goods or services using virtual currencies. If the market value of the goods or services in Singapore dollars cannot be determined (e.g. the good or service is only traded in exchange for virtual currencies), the virtual currency exchange rate at the point of the transaction may be used.

Trading

Income Tax Treatment[^213]

Profits derived by businesses that mine and trade virtual currencies in exchange for money are also subject to tax.

Goods and Services Tax (GST)[^214]

The supply of virtual currency is treated as a supply of services, which does not qualify for GST exemption. Paying for goods and services with virtual currencies is considered as a barter trade. There are two supplies made – one by the supplier who supplies the goods and services, and another by the one who uses virtual currencies to pay the supplier. GST will need to be charged on each supply if the respective supplier is GST-registered. If you use virtual currencies to pay a supplier outside Singapore, you

Businesses that buy and sell virtual currencies in the ordinary course of their business will be taxed on the profit derived from trading in the virtual currency.

Investment

Businesses that buy virtual currencies for long-term investment purposes may enjoy a capital gain from the disposal of these virtual currencies. As there are no capital gains tax in Singapore, such gains are not taxed.

Whether gains from disposal of virtual currencies are trading or capital gains depends on the facts and circumstances of each case. Factors such as purpose, frequency of transactions, and holding periods are considered when determining if such gains are taxable.\(^\text{212}\)

Selling Virtual Currencies

If you are a GST-registered business and you sell virtual currencies as a principal, you will have to charge GST on the sale of virtual currencies, unless the sale is made to a person belonging outside Singapore. If you act as an agent for another party when selling the virtual currencies, you need to charge GST on the commission fees you receive, unless the service is supplied to a person belonging outside Singapore.

Trading fees charged by a virtual currency exchange located in Singapore are subject to GST if that exchange is GST-registered.

Importing Goods Paid by Virtual Currencies

Goods imported and paid for using virtual currencies are subject to the same import GST rules and reliefs as those paid for using fiat currencies.

---

<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong</td>
<td>No special guidance on taxation was issued.</td>
<td>n/inf</td>
<td>No VAT tax in Hong Kong.</td>
</tr>
<tr>
<td>Inland Revenue</td>
<td>Businesses that accept virtual currencies as a payment or pay for goods or services using virtual currencies are subject to normal income tax rules.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country</th>
<th>Income taxes</th>
<th>Mining</th>
<th>VAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Hong Kong (IRD)</td>
<td>Companies and sole proprietors pay a profit tax at 16% and 15% respectively (provided that the profits are earned in Hong Kong).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hong Kong has no capital gains tax, no withholding tax on dividends and interest.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>