Summary of the Cyber and Law Conference, April 22nd, 2018

The participants at the conference included several experts in the field of cryptocurrencies: representatives of the Securities Authority, researchers from HUJI's Cyber Center, attorneys from several law firms (including Shibolet, a partner firm of the Faculty), and representatives from the fields of regulation and law.

Key Points

- Attorneys have a role to play as gatekeepers: they filter out potential clients who are not related to the field, not ready to start talking about issuing virtual currencies, etc. Before the regulator enters the picture, law firms bear a commitment to the public and to their firm's reputation and serve as de facto gatekeepers until the regulator springs into action.

- Regulators in Germany and the G20 have begun to discuss the need for global regulation.

- Experience proves that people do not know how to opt out of innovative technology. Maybe new regulation is needed, and perhaps securities regulations is inappropriate for cryptocurrencies.

- How does the regulator determine whether a cryptocurrency issue constitutes the issuing of a security? We need to recall that there are significant knowledge gaps between the regulator and the community; it takes the regulator time to understand the process. There is a lot of background noise on the crypto issue and it's important to learn to filter this out. The regulator remembers that there were financial actions in the past that harmed investors, such as binary options or the dot com bubble, and cannot avoid asking whether electronic currencies won't end up the same way. Accordingly, the regulator tends to be cautious, leading to market uncertainty.

- The Securities Authority has been monitoring the issue of electric currencies for over a year. Bitcoin is not a security, but DAO certainly is. The dominant approach around the world was to issue a general warning to the public to bear in mind that the issuing of a cryptocurrency

may constitute a public issue. The question as to when a cryptocurrency is a security is one that many fine minds are trying to tackle. Since September 2017, the Securities Authority in Israel has held numerous meetings to formulate its position on this issue. Its goal was to clarify the regulatory field in Israel in order to enable activities. Alongside legal analysis, the report also addressed the entire Blockchain issue.

- In many cases, cryptocurrency offers create fertile ground for fraud. Negative elements have entered the field and are attempting to bypass the existing regulation.

- The Security Authorities' approach seeks to balance the different interests: To protect investors and to prevent cryptocurrency offers from bypassing regulation, but at the same time not to block innovation. The interim report has reached a relatively clear position by comparison to other countries. Alongside the legal analysis, we also decided to recommend specific recruitment tracks for cryptocurrency offers (similar to crowdfunding). The report also mentions the possibility of relying on foreign regulation.

- Any financial regulation seeks to correct market failures – the less failures there are in a market, the less need for regulation/ accordingly, the industry has an interest in ensuring strong self-regulation, which will avoid the need for regulation by a regulator.

- Cryptographic (electronic) currencies are ones issued and stored electronically. Users can trade in them with each other in real or virtual commodities without need for clearing houses.

- One of the reasons why these currencies are attractive is that they have a decentralized character and do not require financial mediators for trading.

- However, all the different cryptocurrencies were not born equal. The differences between them should be reflected in differential regulation.

- Some cryptocurrencies actually function as a currency, while others are really a security issued without a prospectus and without registration. The determining test is whether there is an expectation to secure profit based on others' efforts.

- All cryptocurrencies should be inspected in order to provide protection against fraud. When a currency becomes systematically dangerous, there is also a need to inspect it to prevent systematic danger.

- A currency should meet three key functions: storage of value; medium of exchange; and functioning as a yardstick for evaluating other things. All three aspects are present in the case of the fiat currencies.

- Why do we need non-fiat currencies? One approach argues that governments are corrupt, so if we can solve problems and offer solutions through an electronic system, this is preferable. Another approach suggests that these currencies have no place, because it is the state that should control the issuing of money. Saga proposes a third approach… Supra-state and sub-state communities have emerged, and where they emerge there is a need for a community currency. In the past, the state provided this service. Today, however, the nation state is unable to cope with communities that have developed a need to exchange value and have a global character. This approach argues that the nation-state needs a complementary mechanism. The economy and currency of a state are influenced by politics, monetary policy, and other factors. If the pound loses 20% of its value, then the economy has also lost 20% and my rent has also gone down by 20%. But if I buy something on eBay, it's value is not affected by what happens to a specific pound. So here there's room for other instruments for the storage of value. Saga is developing a non-anonymous global currency that does not claim to replace fiat currency. The interesting question is, what is the scope of the currency issue and what is its goal? When Saga began to design their currency a year ago, there were only 1,000 tokens. The question is, why is there still no currency? We reached three main conclusions. Firstly – knowledge. This field is being driven by technologists, not by economists or central bank officials. The second is fluctuation: a trader needs to prioritize the currency over another, and to do this there is a need for stability. They need to be able to move gradually from a fiat currency to a virtual one, just as at first fiat currencies were backed up by gold, until this was no longer necessary. Accordingly, the goal should be to develop a reserve mechanism (a transfer of trust model). The third aspect is that there is one contract the constitutes the nation-state, and this is the contract of mutual accountability. So those using the currency need to be identified – the logic

of the social contract needs to apply here. This is why we shouldn't be surprised that the nation-state does not jump to welcome cryptocurrencies when they are anonymous. The last aspect established by Saga is the institute aspect – corporate governance. The attempt is to address the issue from several angles in order to formulate a proposal for governance, since Blockchain is not an attractive option in this respect.

- Cryptocurrencies have become a mechanism for releasing pressure for criminals, money launderers, speculators, and citizens of countries such as Venezuela who want to protect their money during periods of inflation.

- The Telegram Channel Bitcoin Israel – Trading features numerous offers to purchase Bitcoin or Ether in cash (classic money laundering).

- The Great Crypto Robbery – hackers stole $530 million worth of a coin called NEM from the Japanese stock exchange Coincheck.

- Currencies such as Zcash and Monero make it harder to track money – all the transfers store the information on Blockchain in an encrypted form.

- Other changes are occurring in Bitcoin, including on the systemic level. Not all transfers pass through Blockchain. An example are lightning network channels: Bob transfers money to Alice repeatedly through the lightning channel, but all that is recorded in Blockchain is the final transaction. In other words, there's a good chance that we won't be able to track the Bitcoin transfers.

- The future of cryptocurrencies will be unlike their present. The main reason for this is that Bitcoin has a serious problem of scalability – it can transfer 3-6 transactions per second, whereas Ten Bis has 30 transactions a second at peak times. Accordingly, there could be three scenarios: 1. Electronic currencies will disappear (so that there is no need for regulation). 2. Bitcoin will develop in order to solve the problem. 3. Bitcoin will be replaced by another more scalable currency. Whatever happens, Bitcoin as it exists today will not become a mainstream currency.

- A general observation regarding the structure of systems: 1. A completely open system enabling monitoring of everything that happens has a privacy problem. 2. A completely private system such as Zcash or Monero is hard to break. 3. There are private systems that create a back door for the government and for enforcement agencies (open code projects do not work in this manner and need a guiding hand to make such a decision). 4. Something that can protect privacy while providing to the government that the person I received money from or transferred money to is on a whitelist. This can be achieved through zero-knowledge proof, but this requires cooperation with regulators, so it may not happen.

- If cryptocurrencies secure broad take-up, regulators will face an almost binary decision: either there will be no regulation or we will see the total closure of cryptocurrencies.