DECENTRALIZED FINANCE (DeFi) AND DECENTRALIZED AUTONOMOUS ORGANISATIONS (DAOs)

Stéphane BLEMUS, Paris 1 Panthéon-Sorbonne Law School, Kalexius law firm

Fin-Tech H-2020 project webinar on “Blockchain & Governance”
Event hosted by the Autorité de contrôle prudentiel et de résolution (ACPR)
Paris, 12 January 2021
SUMMARY

1. Decentralized finance: key concepts
2. Decentralized finance: main use cases
3. Organizations and decentralization
4. Opportunities and risks
5. Questions
**Decentralized Finance (DeFi)**

**Definition:** “open financial infrastructures built upon public smart contract platforms, such as the Ethereum blockchain (...). In contrast to the traditional financial sector, DeFi does not rely on intermediaries and centralized institutions. Instead, it is based on open protocols and decentralized applications (DApps).” (F. Schär, 2020)

DeFi protocols facilitates activity between peers and the transfers of assets and dispute resolutions can potentially be enforced using smart contracts.

**What are the main components of DeFi?**

- Decentralization
- Distributed ledger technologies
- Smart contracts
- Disintermediation
- Open banking / finance
What are the Blockchain and Distributed Ledger Technologies (DLT)?

- Behind the crypto-assets problematic, their underlying protocols and infrastructures: distributed ledgers. The most famous being blockchain.

- A distributed ledger is:
  - **Ledger**: A database of digital data which is
  - **Decentralization / P2P**: Decentralized, replicated, shared/distributed and maintained accessible to a network of computers/nodes connected on a peer-to-peer basis,
  - **Immutability / security**: such that the network participants can share and retain identical, cryptographically secured, chronological and immutable records in a decentralized manner.

  - **Key element**: a distributed ledger is maintained by its participants, and not by a central database administrator or third party. Every network participant can have an identical copy of the distributed ledger.

  - **Public DLT, consortium DLT or (fully) private DLT?**
**What is a ‘smart contract’ (in French: ‘programme informatique automatisé’)?**

- Smart contracts are computer codes designed to execute automatically pre-determined consequences upon the occurrence of pre-determined events.

- A smart contract is neither smart, nor a contract (in the legal sense).

- There is no unanimous definition of what is a smart contract, due to a lack of current regulation and to the perception gap between computer and legal experts on what a contract is.

- Nick Szabo, 1994: « a computerized transaction protocol that executes terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs. »

- Clack, Bakshi and Braine, 2016: « a smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code. »
Disintermediation through DLT and DeFi: a potential cryptographical solution to the double spending and byzantine general problems.

What is Double Spending
and why is it such a problem?
(Source: bitpanda.fr)

- Peer-to-peer networks grew around the transfers of non-financial data (music, movies, pictures...).
- The second stage of peer-to-peer networks is to secure transfers of financial data/assets (money, equities, bonds, fund units...).
1. Decentralized finance: key concepts

2. Decentralized finance: main use cases

3. Organizations and decentralization

4. Opportunities and risks

5. Questions
What are the main use cases of DeFi?

- Stacking (using digital assets to participate in a Proof-of-Stake (PoS) network governance, e.g. Tezos, Cardano)

- Decentralized Exchanges (DEX): crypto-asset exchanges partially (w/ an order book managed by an intermediary) or fully decentralized

- Lending Platforms for crypto-assets (loan amount vs overcollateralization)

- Market Making

- Hedge funds

- Decentralized Insurance (especially to cover rare/black swan events)

- Yield / Liquidity Farming (locking existing crypto-assets to mint new crypto-assets)
Decentralized Finance (DeFi) | Main use cases

- Current state of market infrastructures and intermediaries for the secondary market of financial instruments
Objectives of Decentralized Exchanges

- Lessen the number of intermediaries, facilitate peer-to-peer exchanges of native crypto-assets

Various potential models for Decentralized Exchanges

- Criterion: Fully decentralized or partially decentralized exchanges?
Various potential models for Decentralized Exchanges

- Criterion: With or without an intermediary (broker) acting on behalf of the investors?
Various potential models for Decentralized Exchanges

Criterion: Which means of exchange for the settlement of the transactions? A CBDC (tokenized fiat) or a stable token?
1. Decentralized finance: key concepts
2. Decentralized finance: main use cases
3. Organizations and decentralization
4. Opportunities and risks
5. Questions
Lessons from “The DAO” case

The failure of “The DAO”, the first project of decentralized organization based on blockchain technology

- In 2016, an entity, “The DAO”, has been presented to the public as a new kind of organization, described in its white paper as the “first implementation of decentralized autonomous organization code to automate organizational governance and decision making”.

- 17 June 2016: “The DAO” raised more than $ 150 million to raise venture capital financing by going around the table via an ICO. In a few seconds the organization was robbed 3.6 million ethers, or about 50 million dollars.

- 25 July 2017: “The DAO” decision by the US regulator SEC.

Consequences of “The DAO” failure

- The legal uncertainty as to the definition of ICOs and crypto-assets.

- As computer code will progressively complete – and potentially sometimes replace – written legal codification, the key issue is to analyze if it would be feasible and advisable to govern an organization, e.g. a company, in a decentralized and distributed way.
The future of DAOs

What is a decentralized autonomous organization (or “DAO”)?

- Vitalik Buterin, 2014: a DAO is “a virtual entity that has a certain set of members or shareholders which, perhaps with a 67% majority, have the right to spend the entity’s funds and modify its code”. It is a “long-term form of smart contract that contain the assets and encode the bylaws of an entire organization.”

- DAOs vs ‘traditional’ companies.

Regulatory issues related to DAOs

- DAOs, a nexus of computer code contracts? (Jensen/Meckling)

- The jurisdiction issue: If a DAO is not incorporated in a country, what is the governing law and what is the competent jurisdiction? Could a digital jurisdiction be created?

- The liability issue.

- The ‘democracy’ issue: Would it be truly democratic? Is this model scalable? Algorithmic governance: could companies be entirely run by computer programs/code?
1. Decentralized finance: key concepts
2. Decentralized finance: main use cases
3. Organizations and decentralization
4. Opportunities and Risks
5. Questions
Opportunities related to DeFi use cases

- **Services liberalization and peer-to-peer philosophy**
  - Decentralization
  - Potentially no central control authority (less shutdowns or censorships)
  - Increased access to financial services
  - Lessen arbitration and dispute resolution costs, and prevent fraudulent/illegal activities

- **Reduced time-to-market**
  - Borderless
  - Open source / permissionless access to the services
  - Cost effective and time saving

- **Direct management over assets**
  - Full and direct control over assets
  - New potential services (staking, market making...)
Market risk / High volatility on crypto-asset markets

- Trading on crypto-asset platforms (notably DeFi ones)
  - Risks of loss of value related to the high degree of volatility in valuation and pricing of crypto-assets, due to disjointed crypto-assets platforms and/or to market manipulation / inside trading on these new markets (impeding price discovery)
  - **Example 1**: corporate treasury management and crypto-assets as potential alternative reserve assets
  - **Example 2**: trading in crypto-assets by an individual

  ![Graph showing the price of Bitcoin from 2014 to 2020](source: Coindesk.com)

- Mitigation points: diversification (BTC, ETH...), use of trusted intermediaries or service providers, rise of standardized products (ETFs, trend towards security tokens...), overcollateralization
Market risk / High volatility on crypto-asset markets

- Trading on crypto-asset platforms

Source: Binance.com
Operational risks due to the use of DLT and DeFi

- Operational, reputational, legal risks related to:
  i. the use of a nascent technology as the registration method (bitcoin, anonymized crypto-assets, reliance on technological third-parties…),
  ii. specific risks depending on the DLT used (reliance on blockchain governance/soundness…),
  iii. legal and regulatory uncertainties (recharacterization risk, no legal recognition of DeFi/DAO, KYC-AML, mismatches of IT/legal terms, lack of regulatory or contractual responsibility…),
  iv. RSE/CSR (corporate social responsibility) issues (e.g. the energy spent for the mining),
  v. IT and cybersecurity issues: potential cryptographical key thefts and/or to potential crypto-currencies (51% attack…), software-smart contract errors/bugs

- Legal mitigations:
  i. Identification of the crypto-asset holders (directly or indirectly)
  ii. Put in place a continuity plan (i.e. a backup plan in order to have access of the data outside the DLT) for financial instruments issued on a DLT

- Operational / regulatory mitigations: KYC, clients on-boarding & monitoring, whitelisting/operating model, technological audit of the smart contracts
Operational risks due to the use of DLT and DeFi

In addition to the need of contractual and regulatory certainty, operational considerations are key to the development of crypto-assets’ issuance and trading projects by companies:

The operating model of the issuance and trading of crypto-assets, between decentralised and centralised governance:

- How to issue and manage the crypto-assets in a compliant way (KYC / AML / Embargos & Sanctions)? Whitelisting, oracles…
- How to settle the tokens? Commercial money in token form, CBDC, stablecoins…

The choice of service providers related to crypto-assets and DeFi:

- Which role for the custodian acting on behalf of the investors?
- How to enhance liquidity on the secondary market of the crypto-assets?
Counterparty risk related to the use of blockchain

- Contract automation by smart contracts, DeFi infrastructures and the use of a native “delivery-versus-payment” could be ways to diminish counterparty risk.

- Nevertheless, it is a nascent technology with mature processes to be enhanced in the future.

- Counterparty risks related to crypto-assets:
  
  i. Practices by new crypto-asset service providers: e.g. crypto-asset platforms like Coinbase which hold the assets on behalf of their clients (vs traditional markets where clients are holding their assets).
  
  ii. Lack of professional service providers to assess counterparty risk (e.g. brokers).
  
  iii. Delivery-versus-payment: cash leg and title leg not yet on the same technology.
  
  iv. Use of a stable coin: advantages of a stable coin are its execution rapidity, its native onchain nature. But there are some collateralization issue for some stablecoins, and therefore an increase of the counterparty risk. Potential mitigation: overcollateralization.
Liquidity risk related to the use of DLT and DeFi

- **Liquidity issues related to crypto-assets and DeFi platforms**: Possibility of not being able to sell crypto-assets at little or no loss of value (e.g. in times of stress)
  
  i. Trading volume (low asset liquidity on many DeFi platforms),
  
  ii. Lack of regulated DeFi crypto-asset exchanges,
  
  iii. Acceptance by the public (e.g. stores, companies, ATMs...),
  
  iv. Legal/compliance frameworks (e.g. bans or restrictions in some countries on crypto-assets, on ICOs...),
  
  v. Lack of eligibility of crypto-assets as HQLA (High Quality Liquid Asset) to date
1. Decentralized finance: key concepts
2. Decentralized finance: main use cases
3. Organizations and decentralization
4. Opportunities and Risks
5. Questions