Risks, crypto-assets and blockchains

DOMINIQUE GUEGAN

Paris 1 Panthéon – Sorbonne

LabEx ReFI

Blockchain Technology

- Securized technology
  - Peer-to-peer technology
  - Consensus protocol
  - Cryptography
- All blockchains are not equivalent
  - What is the objective for using the blockchain technology?
  - Creation of crypto-assets
  - Payments
  - Transfers of goods
- Risks associated to the blockchains

RISKS ASSOCIATED TO THE BLOCKCHAINS ENVIRONMENT

- 51% attack
- Errors in codes (smart contracts)
- Hacking of the platforms (not directly link to the technology blockchain)
- Lost of private keys
- Theft of private keys

FRAUDS LINK TO THE FINANCIAL SYSTEM

- Payments
  - Fraudulous exchange payments
  - The money laundering (ML), terrorist financing (TF) : 0,4% of statements of suspicion in 2017, (TracFin , December 2018). On Coinhouse: 50 cases of money laundering have been identified during the less 18 months.
  - Evasion sanctions (circumventing exchanges and capital controls)
  - Erroneous transactions and transactions never executed
- Economics
  - Impact on the monetary policy and financial system
  - Stability on the financial system
  - High risk investment opportunities (pump and dump)

SCAM TO CRYPTO EXCHANGES

- Main fraud in 2018: between 500 M to 1B.
- sellers show off juicy returns to private investors
- They propose to you to give a good return on a small amount, then you receive it.
- Then, you send more money, and you receive again a good return
- When finally you send a very high amount of money, the sellers disappear: they close their account and you cannot find them.
- To get back the money is impossible: persons have to file a complaint

INITIAL COINS OFFERING
or INITIAL TOKENS OFFERING

- Since early 2016, a new way of raising funds has rapidly emerged as a major issue for FinTech founders and financial regulators
- A new method
  - to raise funds through the offer and sale by a group of developers or a company to a crowd (i.e. investors or contributors) of ad hoc crypto-assets (also coined as “tokens”) specifically created and issued on a distributed ledger,
  - sometimes preceded by an early sale of the crypto-assets called “pre-sale”,
  - for the purpose of launching a business or of developing ad hoc governance of projects based,
  - in exchange for pre-existing ‘mainstream’ crypto-assets, such as Bitcoin and Ether among others, or even fiat currencies. Perceived by several entrepreneurs as a less burdensome way of fundraising, at least 25 billion dollars have been raised between March 2016 and August 2018 through ICOs only.
- Perceived by several entrepreneurs as a less burdensome way of fundraising, at least 25 billion dollars have been raised between March 2016 and August 2018 through ICOs only (coinschedule.com).

FRAUDS and ICOS

- Importance of white paper
- New regulation (France, US, ASIA)
- Frauds concern the ICO which have no valuable project
- In 2016 – 2017 specific behavior
- In 2018 and in the future, due to the regulations which arise, frauds will diminish.
- Investigation on the ICOs which work, identifying the empty shells.
- New phenomena: DAICO

RISKS AND REGULATION

- Crypto-assets cannot be regulated
- Regulation of the payments platforms
- Information on the ICO: in France possibility to have a Label by AMF (optional)
- Information on the frauds link to the use of cryptocurrencies
- Banks and account in cryptocurrencies
- Uniform regulation between the different countries
- New fiscal legislation in France for tokens emitters and tokens acquirers.

CASE STUDIES
FOR RISK MANAGEMENT

- Open blockchains
  - Security of blockchains to avoid frauds: study of 51% attack investigating the protocols: definition of an economic indicator – ranking.
  - For ML/TF (whose volume is negligible in crypto-assets compare to the whole financial system), study of the volume exchanges considering the dynamic sequence of the cryptographic keys.
  - Speculative phenomena: studies of the bubbles, pump and dump events, strategies of investment based on crypto assets which are largely risky.
  - Importance of the second market: future of the tokens issued by ICOs.
  - Frauds on ICOs: the empty shells
- Close blockchains
  - Creation of commodities back digital assets
  - Central banks and monopolistic new market
- Creation and sharing of Database
- Development of new approaches for measuring the risks associated to the crypto-assets link with the blockchain technology.

D

REFERENCES

- D. Guégan, A. Sotiroopoulou (2017) Bitcoin and the challenge for financial regulation, Capital Markets law Journal, Issue 4
- D. Guégan (2017) Blockchain publique versus blockchain privée: limites et enjeux, Revue Banque, N° 810., Sept 2017
- Guégan D., (2017) Blockchain publique et contrats intelligents (Smart Contrats) :) Les possibilités ouvertes par Ethéreum… et ses limites, Revue Banque, N° 814, Dec. 2017.
- Blemus S. (2018) Law and Blockchain: a legal perspective on current regulatory trends worldwide, RTDF
- Guégan D. (2018) ICO: La nouvelle façon de lever des fonds sans contrainte?, Revue Banque N° 817, Février 2018.
- Guégan D. (2018) The digital world: I Bitcoin: from history to real life, Bankers, Markets and Investors, 151.
- Guégan D. (2018) The digital world: II Alternatives to the Bitcoin blockchain., Bankers, Markets and Investors, 152
- Frunza M., D. guégan (2018) Is the Bitcoin rush over ? Chapter in Handbook on Cypto-currencies and mechanism of exchange, eds S. Goutte, K. Guesmi, S. Daadi, Springer Verlag.
- Guégan D., Hénot C. (2019) A Fair Value for Authentication Use Case Blockchain, in revision for Digital Finance
- Blemus S., Guégan D. (2019) Initial Crypto-asset Offerings (ICOs), tokenization and corporate governance, , WP, University Paris1 Panthéon –Sorbonne.
- Cales L. D. Guégan (2019) The future of tokens\\ Regulatory stakes and a new prospective commodity-backed digital asset, the CommodCoin, WP, University Paris1 Panthéon –Sorbonne.

Measuring risks in blockchain payments

Paola Cerchiello[1]

[1]University of Pavia

1 February 2019

Case study I: Fraud detection in ICOs

- Initial Coin offerings are a new yet uncovered mean to raise funds through tokens: a conjunction of **crowdfunding** and **blockchain**.
- ICOs are a relatively new phenomenon but have quickly become a dominant topic of discussion within the fintech community.
- Few numbers (based on Coinschedule.com)
  - around **6** bi USD raised in 2017 by **456** ICOs
  - around **21.7** bi USD raised till the end of 2018 by **1076** ICOs
- The risky counter part is the presence of criminal activity.
- Financial market authorities are very prudent and some countries ban straightaway all ICOs from their jurisdiction.

Methodology - Response Variable

The analyzed status of an ICO is made up of 3 classes, intended as follows:

- **Success**: the ICO collects the predefined cap within the time horizon of the campaign;
- **Failure**: the ICO does not collect the predefined cap within the time horizon of the campaign;
- **Scam**: the ICO is discovered to be a fraudulent activity during the campaign and described as such by all the platforms we use for data gathering (namely ICObench and Telegram).

Methodology - Explanatory variables

Table: Employed Covariates

class0	f=failed, sc=scam su=success
class1	0=success, 1=scam
class2	0=failed, 1= success
w_site	Website (dummy)
tm	Telegram (dummy)
w_paper	White paper (dummy)
usd	presale price in USD
tw	Twitter (dummy)
fb	Facebook (dummy)
ln	Linkedin (dummy)
yt	Youtube (dummy)
gith	Github (dummy)
slack	Slack (dummy)
reddit	Reddit (dummy)
btalk	Bitcointalk (dummy)
mm	Medium (dummy)
nr_team	Number of Team members
adv	Existence of advisors (dummy)
nr_adv	Number of advisors
project	Official name of the ICO
nr_tm	Number of users in Telegram
tot_token	Number of Total Tokens
Pos_Bing	Standardized number of positive words for BL list
Neg_Bing	Standardized number of negative words for BL list
Sent_Bing	Standardized sentiment for BL list
Pos_NRC	Standardized number of positive words for NRC list
Neg_NRC	Standardized number of negative words for NRC list
Sent_NRC	Standardized sentiment for NRC list

Results - I

Table: Results from Logistic regression on Success/Failure

	Dependent variable:
	class2
tw	2.63$^{\cdot}$
	(1.49)
w_paper	1.51*
	(0.65)
Sent_NRC	2.36***
	(0.61)
Nr_adv	0.53***
	(0.15)
Nr_team	0.30**
	(0.10)
Constant	-4.40
	(1.64)
Observations	196
Residual Deviance	71.14
Akaike Inf. Crit.	83.14
Note:	*p<0.1; **p<0.05; ***p<0.01

Results – II

Table: Results from multilogit regression: failure and scam compared to success

	Dependent variable:	
	f	sc
	(1)	(2)
Oweb_dum	0.363	-1.731^{*}
	(0.859)	(1.042)
tw	-3.046^{**}	-2.768^{**}
	(1.310)	(1.350)
adv_dum	-1.679^{***}	-0.943
	(0.607)	(0.855)
Paper_du	-2.060^{***}	-0.737
	(0.722)	(0.954)
Sent_NRC_sc	-2.934^{***}	-1.585^{**}
	(0.785)	(0.790)
Constant	1.732	1.685
	(1.365)	(1.459)
Akaike Inf. Crit.	161.230	161.230
Note:	*p<0.1; **p<0.05; ***p<0.01	

Case study II: Cyber risk prioritisation

- Cyber risks can be defined as: operational risks emerging from the use of ICT, that compromises the confidentiality, availability, or the integrity of data or services (IMF, 2018).
- Data on cyber risk is scarce: there is no common standard to record them, and companies have no incentives to report them For example, among around 4,000 annual reports for U.S. firms published in 2017, only 7 percent included a reference to cyber-risk.
- There have been very few quantitative analyses of cyber risk. We extend IMF (2018) in two main directions: i) modelling data available only at an ordinal scale; ii) capturing interdependence between event types by means of contagion models, to improve predictive performance.

Preliminary Results - criticality index (Facchinetti et al. (2018))

Attack technique	$\hat{I}$ (SE) Cybercrime	Hacktivism	Espion./Sab.	Inf.Warfare
0-day	0.600 (0.126)	1.000 (0.000)	1.000 (0.000)	1.000 (0.000)
Account Cracking	0.188 (0.061)	0.281 (0.088)	1.000 (0.000)	-
DDoS	0.370 (0.078)	0.188 (0.121)	-	1.000 (0.000)
Malware	0.291 (0.024)	0.600 (0.126)	0.971 (0.023)	0.938 (0.058)
Multiple Thr./APT	0.409 (0.082)	0.500 (0.000)	0.952 (0.038)	0.950 (0.047)
Phishing/Soc.Eng.	0.096 (0.035)	-	1.000 (0.000)	0.875 (0.108)
Phone Hacking	-	-	1.000 (0.000)	1.000 (0.000)
SQLi	0.500 (0.000)	0.500 (0.000)	-	-
Unknown	0.162 (0.026)	0.352 (0.081)	0.969 (0.043)	1.000 (0.000)
Vulnerabilities	0.280 (0.051)	0.325 (0.075)	1.000 (0.000)	1.000 (0.000)
Geometric mean	**0.239**	**0.342**	**0.973**	**0.952**