BIS 2019 conference
BSCT 19 workshop

Contagion in Bitcoin networks

27th of June 2019, Universidad de Sevilla, Sevilla, Spain

***Coquidé Célestin*[1], *Lages José*[1] *and Shepelyansky Dima L.*[2]**

[1]Institut UTINAM, university of Bourgogne Franche-Comté, Besançon , France

[2]Laboratoire de physique théorique, University of Paul Sabatier, Toulouse, France.

http://perso.utinam.cnrs.fr/~lages/apex/

Outline

1) Bitcoin network
2) Google matrix (GM) theory and PageRank algorithm
3) Ranking of users
4) Crisis propagation
5) Reduced google matrix method (REGOMAX)
6) Conclusion

1) Bitcoin network

The Bitcoin *is a* ***crypto-currency*** *created by* ***Satoshi Nakamoto*** *in* ***2009***

- This digital currency is **independent** and very **secured**
- **Every transactions** are **stored** as a chain = **blockchain**
- Usable for everyone who get a Bitcoin **wallet**
- Used for **shopping** and **trading**

Its ***value*** *has known* ***skyrocketing*** *periods*

today (07:38 UTC) 1 BTC = 10,825.88 €

1) Bitcoin network

- About **35 M** of **‘users’** by the first quarter (Q1) of **2019**
- Anonymized **transactions** are **accessible** at www.blockchain.com/explorer
- Network construction :

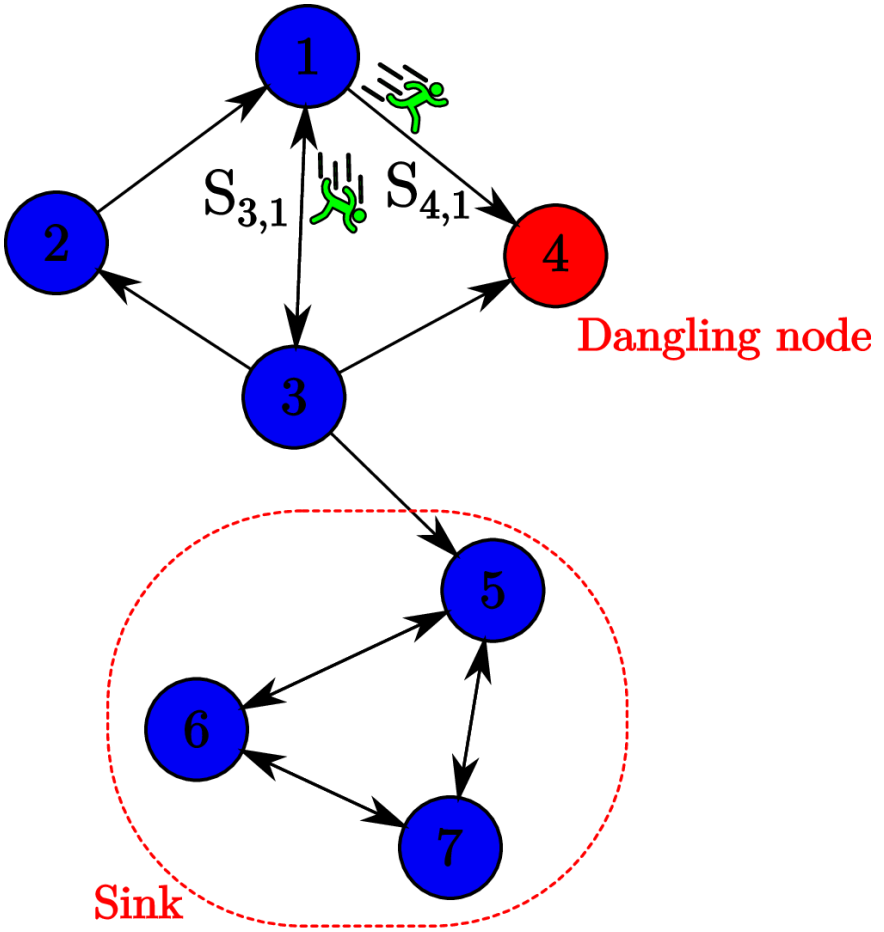
  Node = **Wallet**

  Link = **Transaction** (directed)
- We use data from **2009 Q3** (142 users, 117 Transactions) to **2013 Q2** (6 M, 16 M)

*How can we **analyze efficiently** such a **big** (directed) **network** ?*

2) Google matrix and PageRank

- **Modeling** a **random walk** through a **directed network**
- **Stochastic** matrix (**S**)
  - Transition **probabilities**
  - **Dangling node** fixed
- **Google** matrix (**G**) (Brin and Page 1998)
  - **Sink** effect **avoiding**
  - **Leading eigenvalue** degeneracy = 1



2) Google matrix and PageRank

- **PageRank** (P) = **leading eigenvector** such that (***GP=P***)

  => **Steady-state**

  => The **highest component** for the **most reachable node**

  => **Efficiency** of **ingoing** link = **Importance**

- **Inverting** links **direction** => *G** => **CheiRank**

  => **Efficiency** of **outgoing** link = **communicability**

- We can **rank** nodes by **PageRank/CheiRank** order

3) Ranking of users

- For each time slice we have ***G*** , ***G****, **P** and **P***
- **PageRank** (**P**) encodes **information** on Bitcoin **import effectiveness**
- **CheiRank** (**P***) encodes **information** on Bitcoin **export effectiveness**
- **2DRank** brings **informations** contained in **both PR and CR**

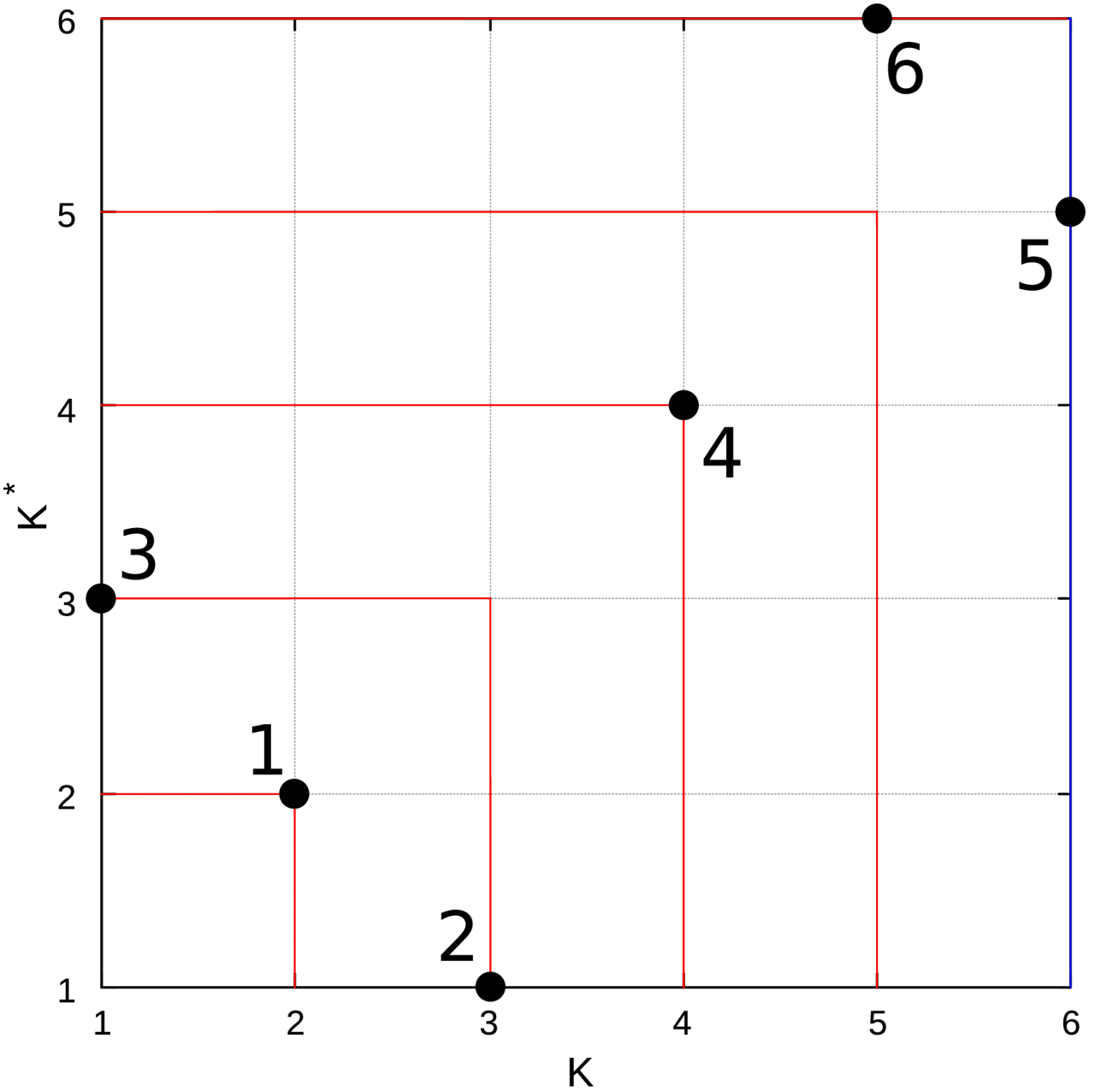
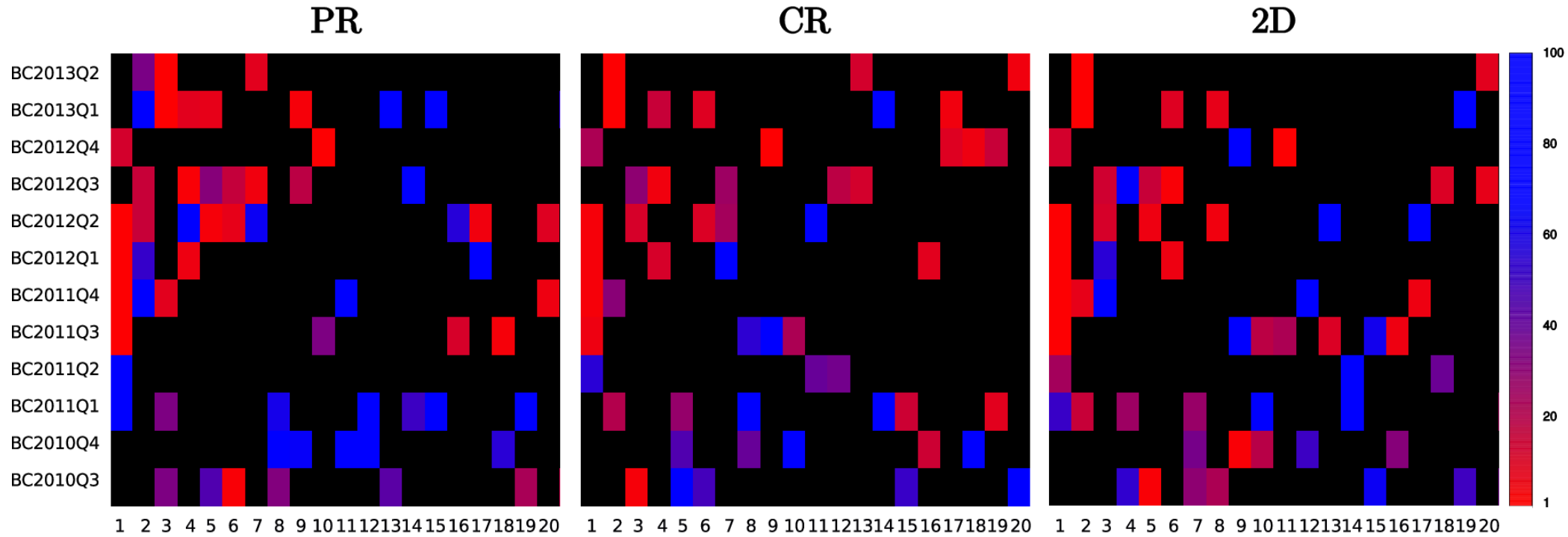


Fig1. Construction of the **2DRank**. **K** is for **PageRank** list, **K*** for **CheiRank** list.



Rank	Node	Occurance
1	6	7
2	4	6
3	11	5
4	24	4
5	18	4
6	26	3
7	15	3
8	2	3
9	20	3
10	30	2
11	443	2
12	220	2
13	23	2
14	515	2
15	89	2
16	49	2
17	1469	2
18	103	2
19	9	2
20	1136	2

Rank	Node	Occurance
1	6	6
2	11	4
3	89	3
4	15	3
5	24	3
6	18	3
7	4	3
8	2	3
9	30	2
10	220	2
11	1469	2
12	23	2
13	239	2
14	857	2
15	213	2
16	19618	2
17	159	2
18	3553	2
19	10	2
20	2149	2

Rank	Node	Occurance
1	6	7
2	11	4
3	4	4
4	115	3
5	15	3
6	18	3
7	2	3
8	24	3
9	30	3
10	89	3
11	10	2
12	103	2
13	12	2
14	1	2
15	1302	2
16	1469	2
17	16	2
18	19618	2
19	199	2
20	20	2

Tab.1 List of the **20 most present users** among **12 top 100s**. From **PageRank** algorithm (left), **CheiRank** (center) and **2DRank** (right).

4) Crisis propagation

- Crisis model :

  1) $\mathbf{B_u}$ is the CheiRank/PageRank **balance** for a given **user**

$$B_u = \frac{P_u^* - P_u}{P_u^* + P_u}$$

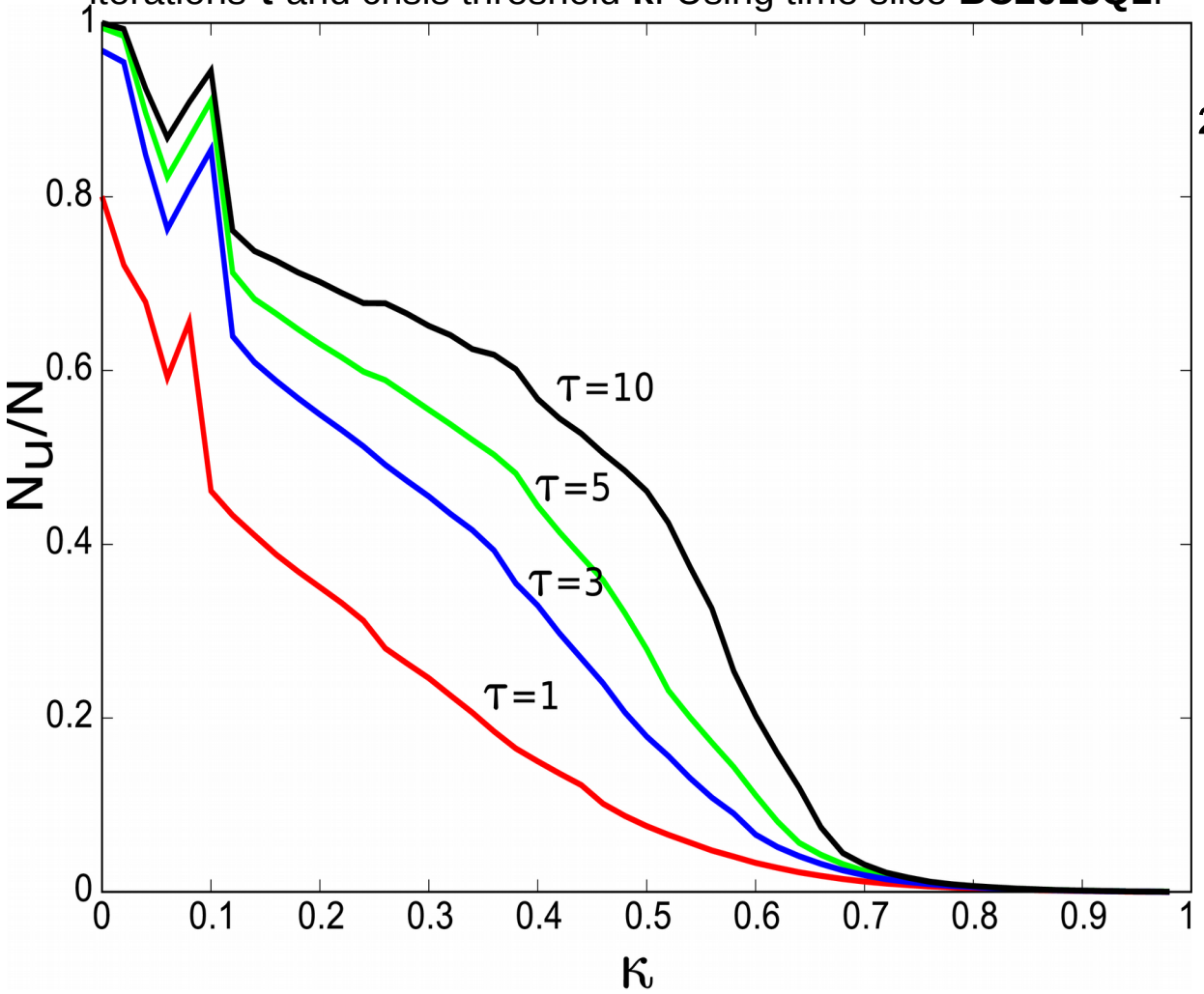
  2) If $\mathbf{B_u \leq -\kappa}$ (**crisis threshold**) then we consider a **bankrupt event** for the user ‘u’

  3) ‘u’ needs to **close all** its Bitcoin **import** transactions

  Do it for all nodes => **new network**

- We do it for different step **τ**

Fig2a. **Probability** to find a **bankrupt user** at 4 different iterations **τ** and crisis threshold **κ**. Using time slice **BC2013Q1**.



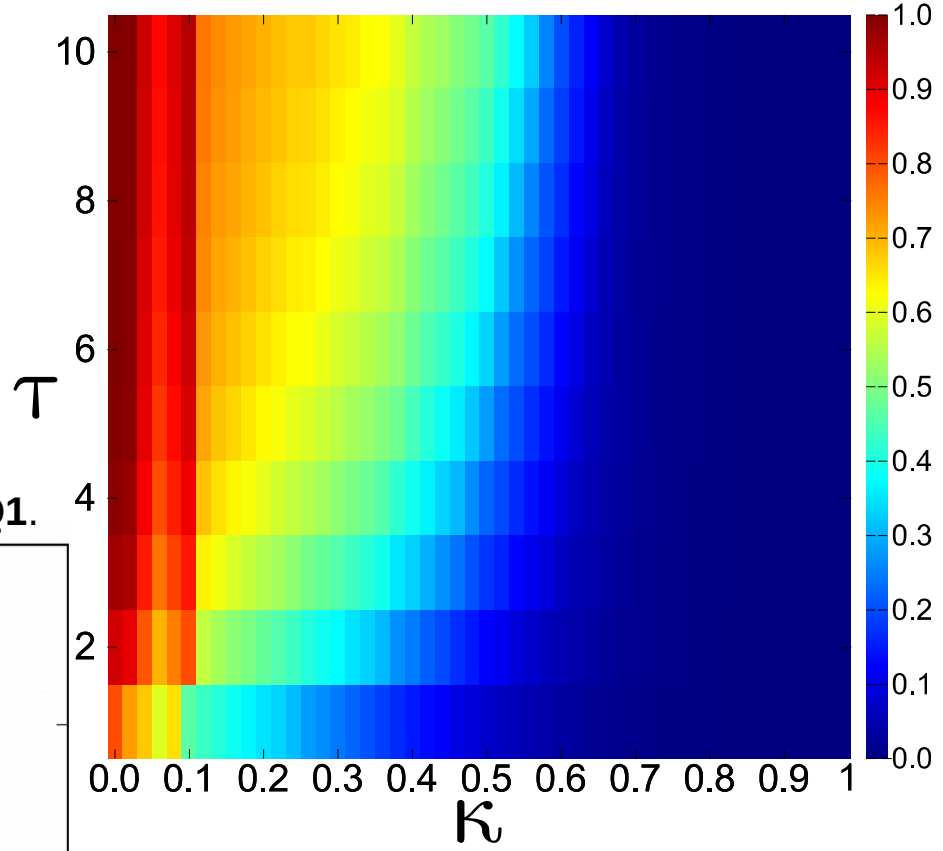


Fig2b. **Probability** to find a **bankrupt user** at several iterations **τ** and crisis threshold **κ**. Using the time slice **BC2013Q1**.

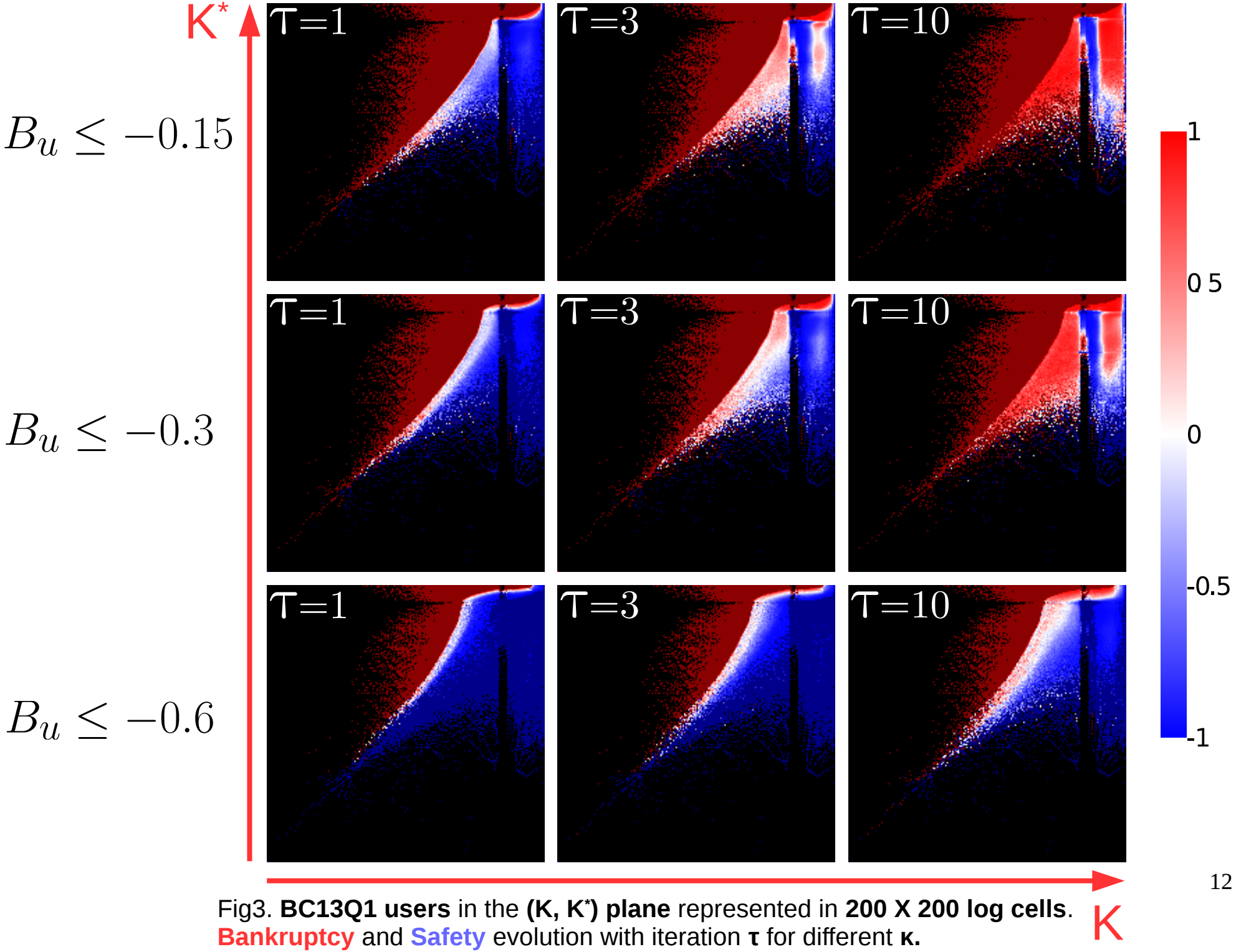


Fig3. **BC13Q1 users** in the **(K, K*) plane** represented in **200 X 200 log cells**. **Bankruptcy** and **Safety** evolution with iteration **τ** for different **κ.**

5) Reduced google matrix method (REGOMAX)

- **REGOMAX** allows us to **point out hidden links** between nodes of interest (Frahm and Shepelyansky 2016, Frahm et al. 2016)

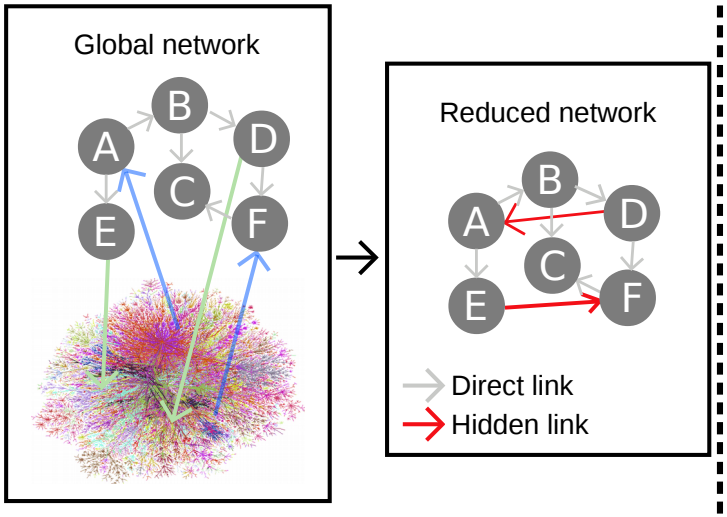
Transition between the N_r nodes

Transitions from the other N-N_r nodes toward the N_r nodes

$$G = \begin{pmatrix} G_{rr} & G_{rs} \\ G_{sr} & G_{ss} \end{pmatrix}$$

Transitions from the N_r nodes toward the other N-N_r nodes

Transitions between the other N-N_r nodes



$$G_R = G_{rr} + G_{pr} + G_{qr}$$

Direct links Contribution from **Hidden** links **«PageRank »**

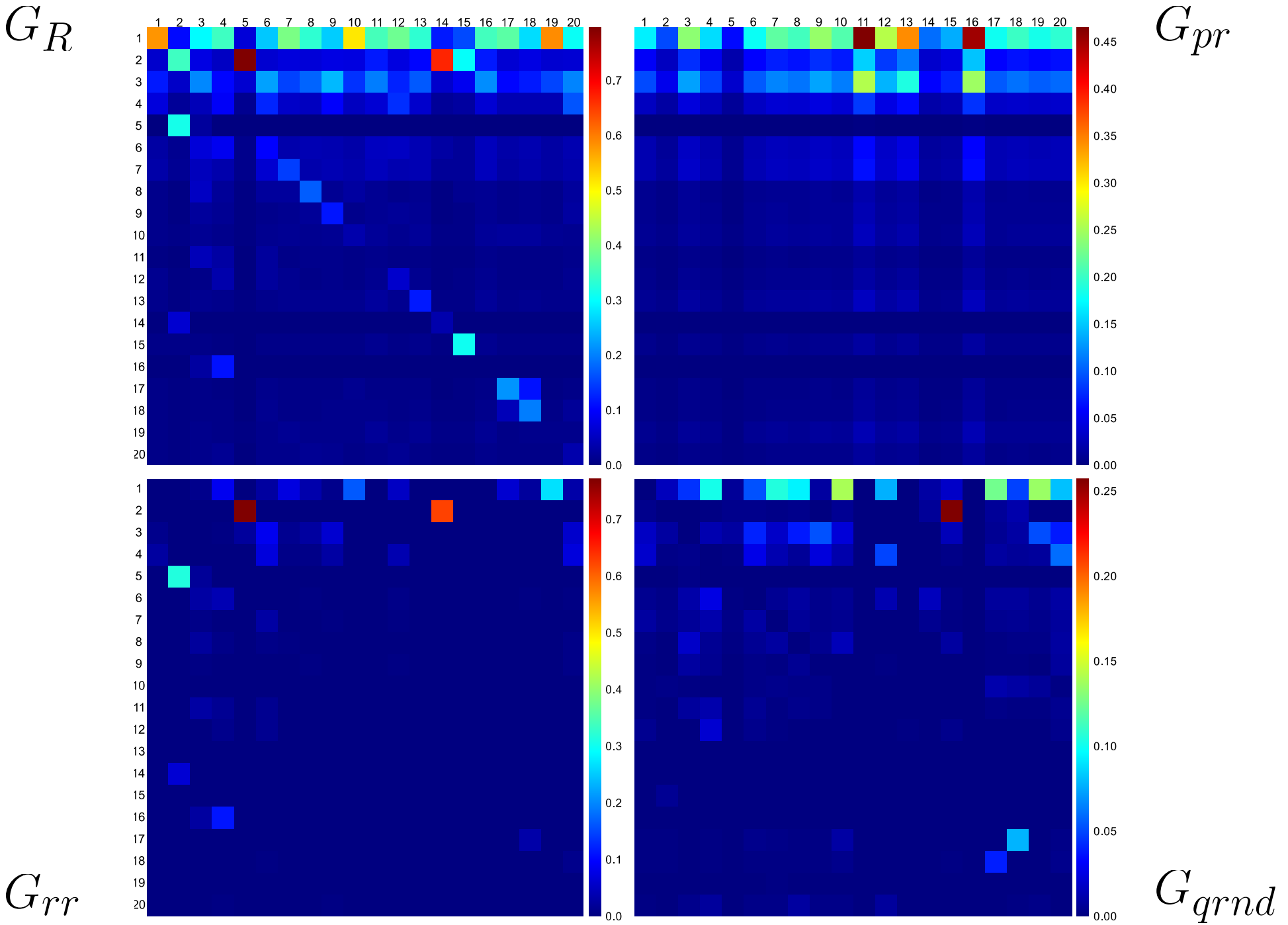


Fig4. **Reduced google matrix** for the **top 20 PageRank** users of **BC13Q1**.

6) Conclusion

- **Blockchain** can be **used** for **Bitcoin transactions network analysis**
- With such a complex network **GM** and **PageRank/CheiRank** algorithms are **useful**
- With our simple **crisis contagion model** we can have access to **different scenario** of crisis **propagation** of the **Bitcoin network**
- **Top users** seem to get **bankruptcy rapidly**
- By using **REGOMAX** for inferring **hidden** (indirect) **relationships** we showed that top users have strong hidden + direct transactions and partnerships

6) Conclusion

- We don’t have **metadata** about the **nature** of the **transactions**
  - Services, shopping, internal exchange (**same person** but **multiple accounts**)
- We want to **compare** contagion **robustness** of **bitcoin** network with **other net** like **WTN**, **banking exchange** network

6) Conclusion

- **Wikipedia network :**
  - Hidden relationship between political leaders (Frahm et al. 2016)
  - Terrorist groups (El Zant et al. 2018)
  - Application to biomedical topic such as infectious diseases (Rollin et al. 2019)
  - World influence and Interactions of Universities (Coquidé et al. 2019)
- **Trade network :**
  - Influence of petroleum and gas trade on EU economies (Coquidé et al. 2019)
  - Economic activities with WTO (Coquidé et al. 2019)
  - Crypto-currency
- **Game network** :
  - Game of go (Coquidé et al. 2017)


Thank you