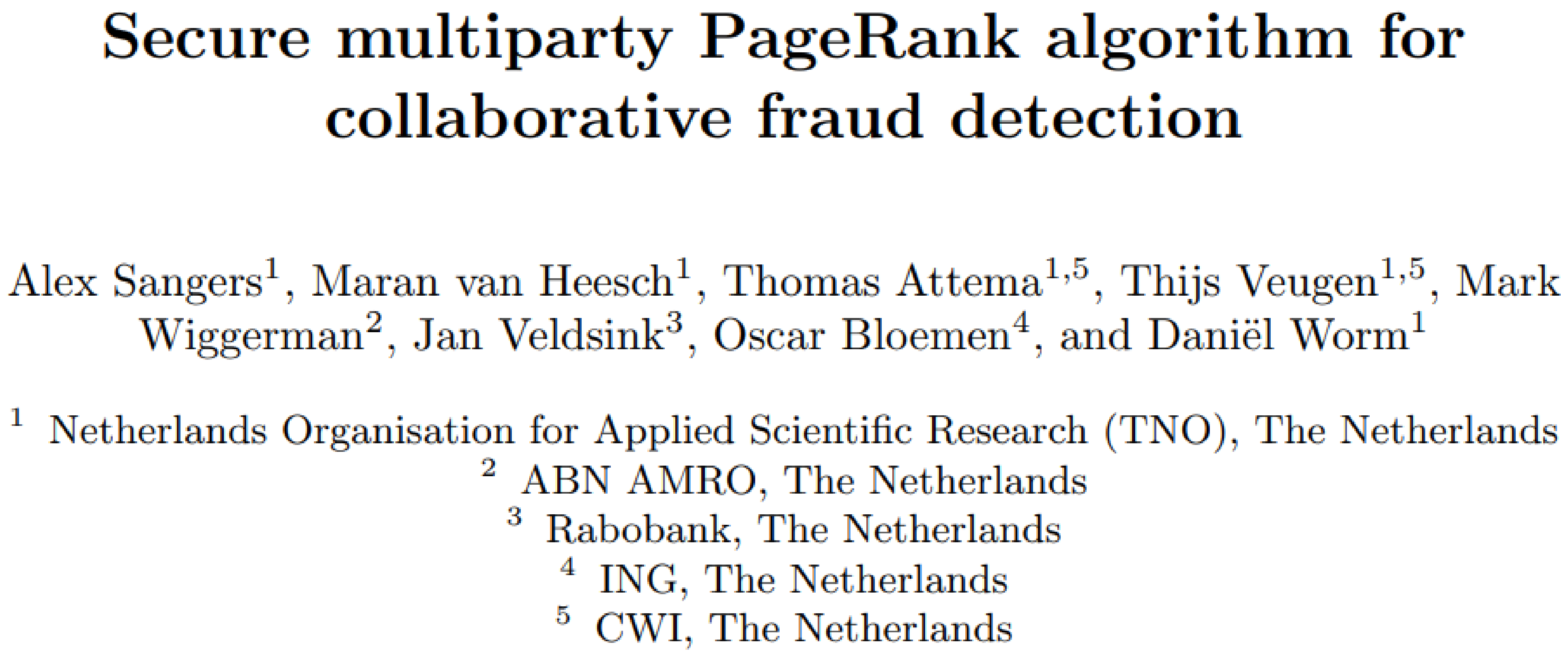
TNO innovation for life

DETECTING TRANSACTION FRAUD WITH MULTI-PARTY COMPUTATION

THOMAS ATTEMA - THOMAS.ATTEMA@TNO.NL

12 March 2020

JOINT WORK



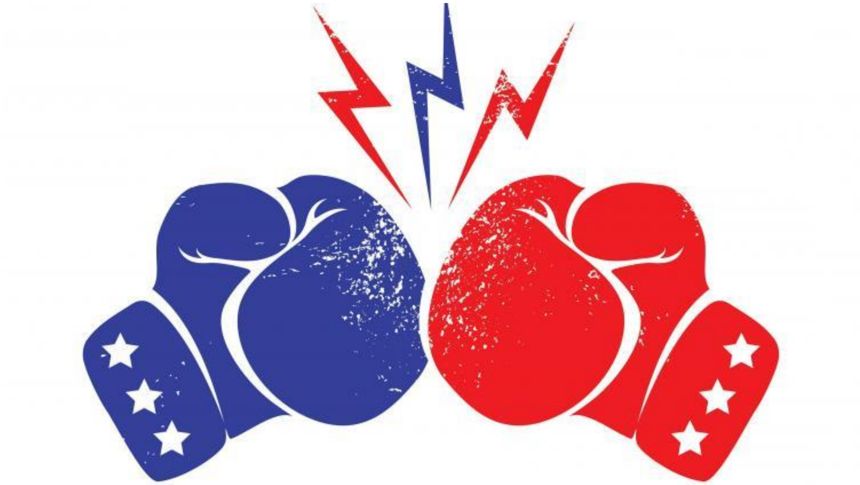
Secure multiparty PageRank algorithm for collaborative fraud detection

Alex Sangers[1], Maran van Heesch[1], Thomas Attema[1,5], Thijs Veugen[1,5], Mark Wiggerman[2], Jan Veldsink[3], Oscar Bloemen[4], and Daniël Worm[1]

[1] Netherlands Organisation for Applied Scientific Research (TNO), The Netherlands
[2] ABN AMRO, The Netherlands
[3] Rabobank, The Netherlands
[4] ING, The Netherlands
[5] CWI, The Netherlands

THE MULTIPARTY COMPUTATION PARADOX

Information Sharing
Collaboration

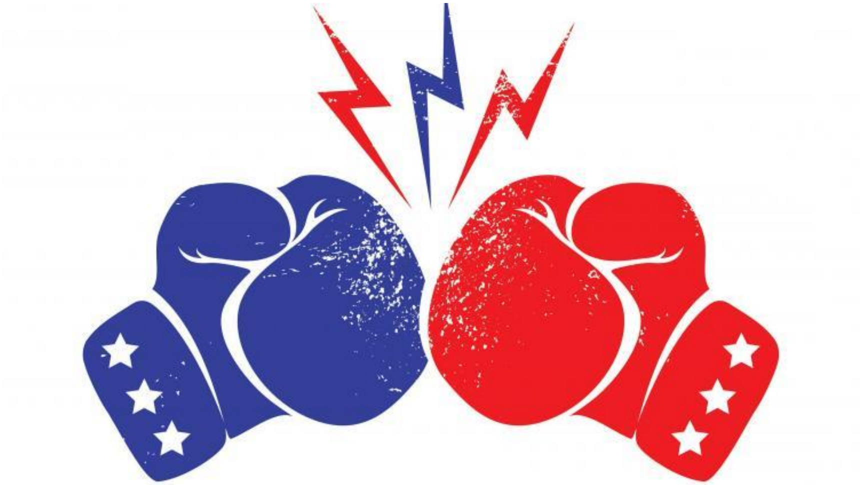


Privacy
Confidentiality

TOY EXAMPLE DATING

THE MULTIPARTY COMPUTATION PARADOX

Second date??

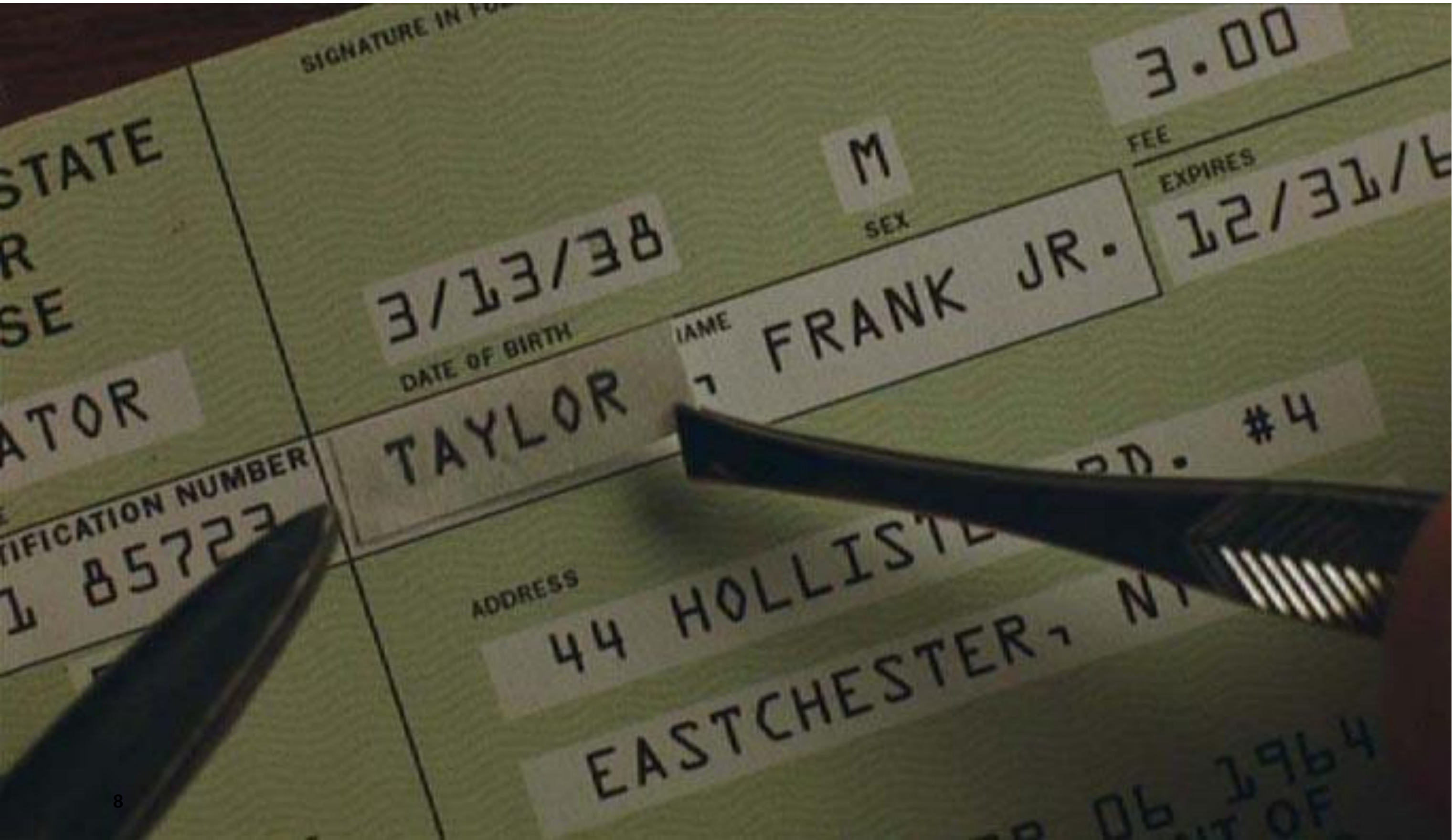


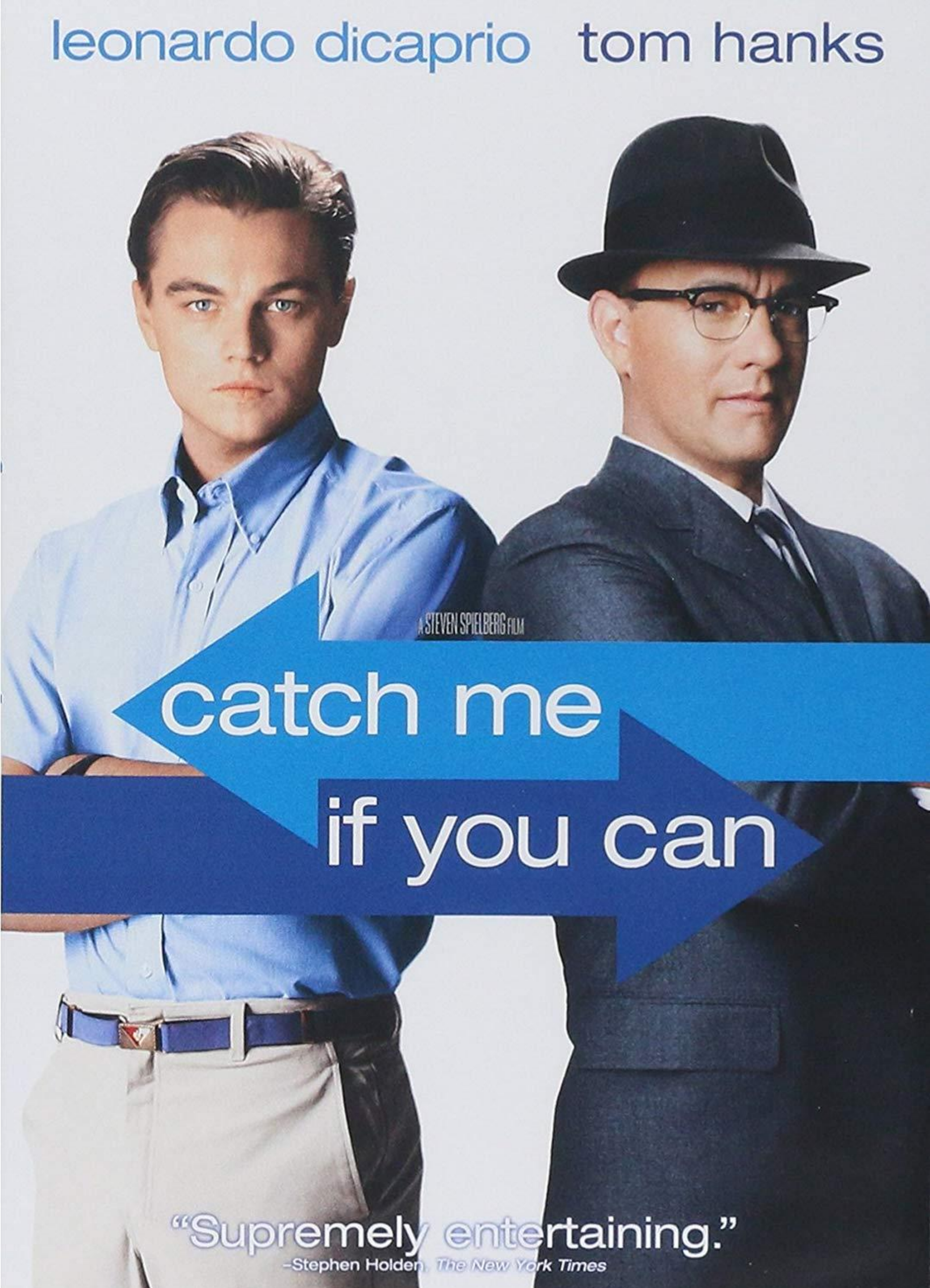
Rejection??

https://www.youtube.com/watch?v=JnmESTrsQbg

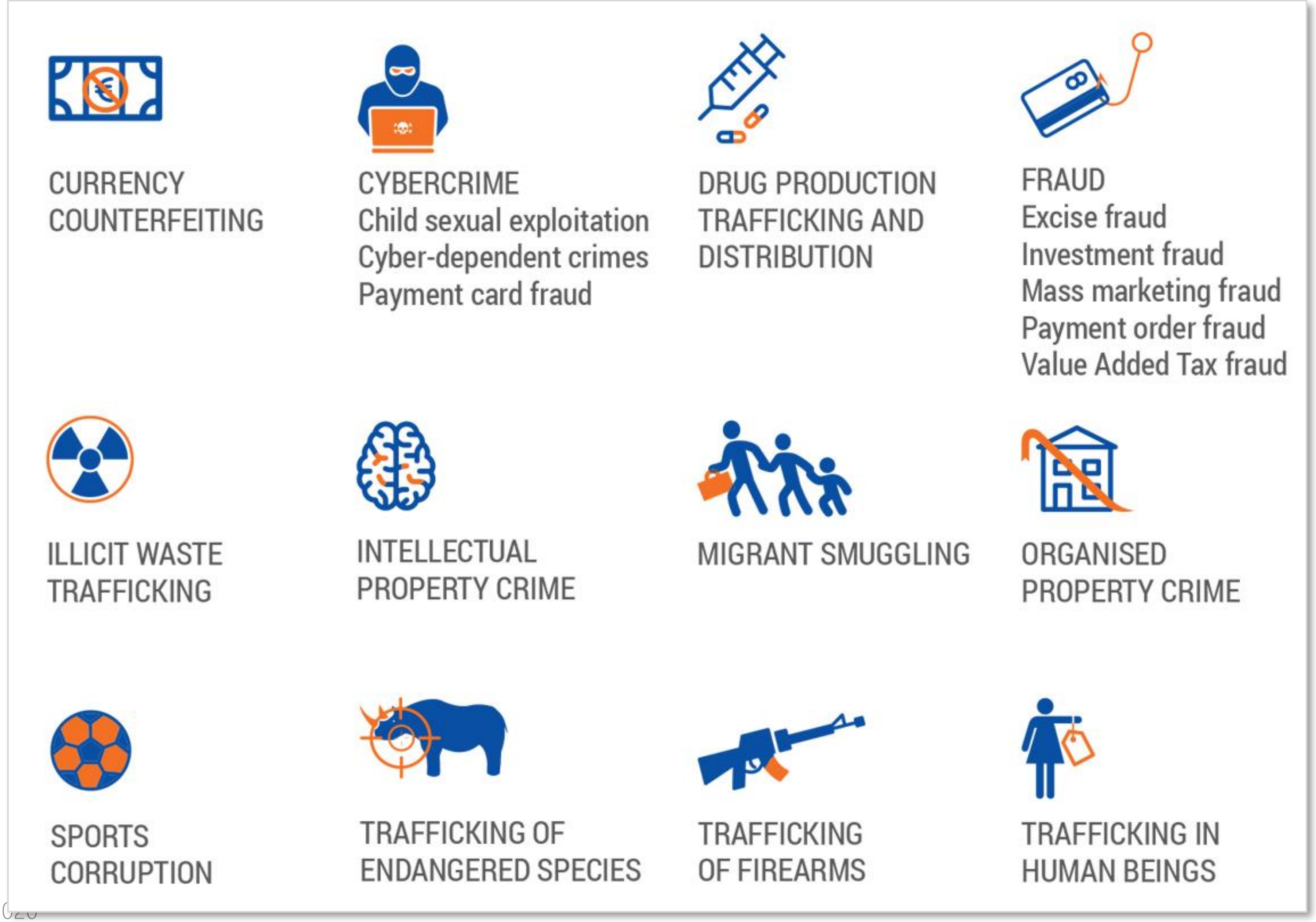
FRAUD DETECTION

FRAUD WAS INDIVIDUAL





FRAUD HAS BECOME ORGANIZED



CURRENCY COUNTERFEITING

CYBERCRIME
Child sexual exploitation
Cyber-dependent crimes
Payment card fraud

DRUG PRODUCTION TRAFFICKING AND DISTRIBUTION

FRAUD
Excise fraud
Investment fraud
Mass marketing fraud
Payment order fraud
Value Added Tax fraud

ILLICIT WASTE TRAFFICKING

INTELLECTUAL PROPERTY CRIME

MIGRANT SMUGGLING

ORGANISED PROPERTY CRIME

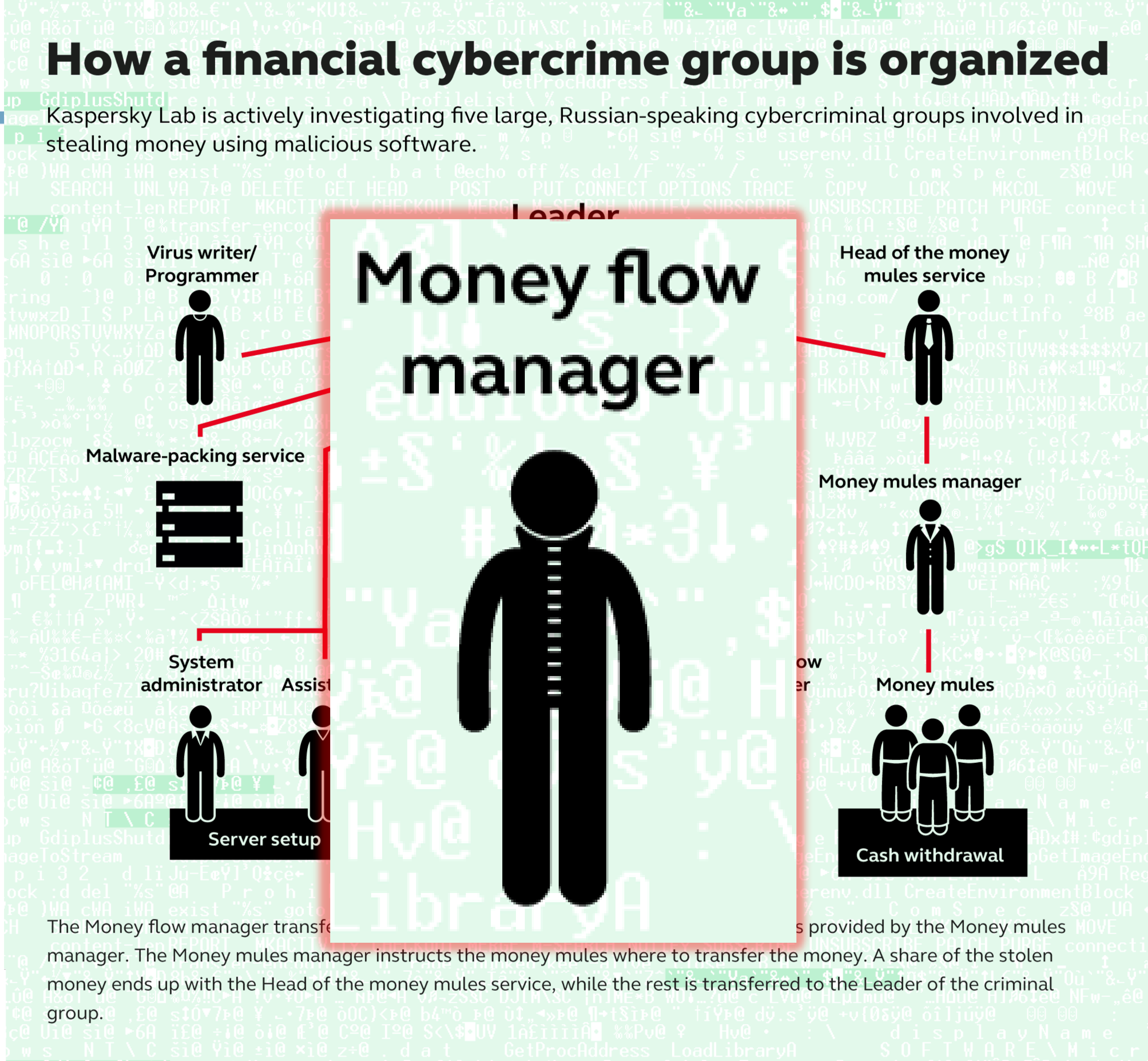
SPORTS CORRUPTION

TRAFFICKING OF ENDANGERED SPECIES

TRAFFICKING OF FIREARMS

TRAFFICKING IN HUMAN BEINGS

- Europol: “*Organized crime is more connected and internationally active than ever before.*”

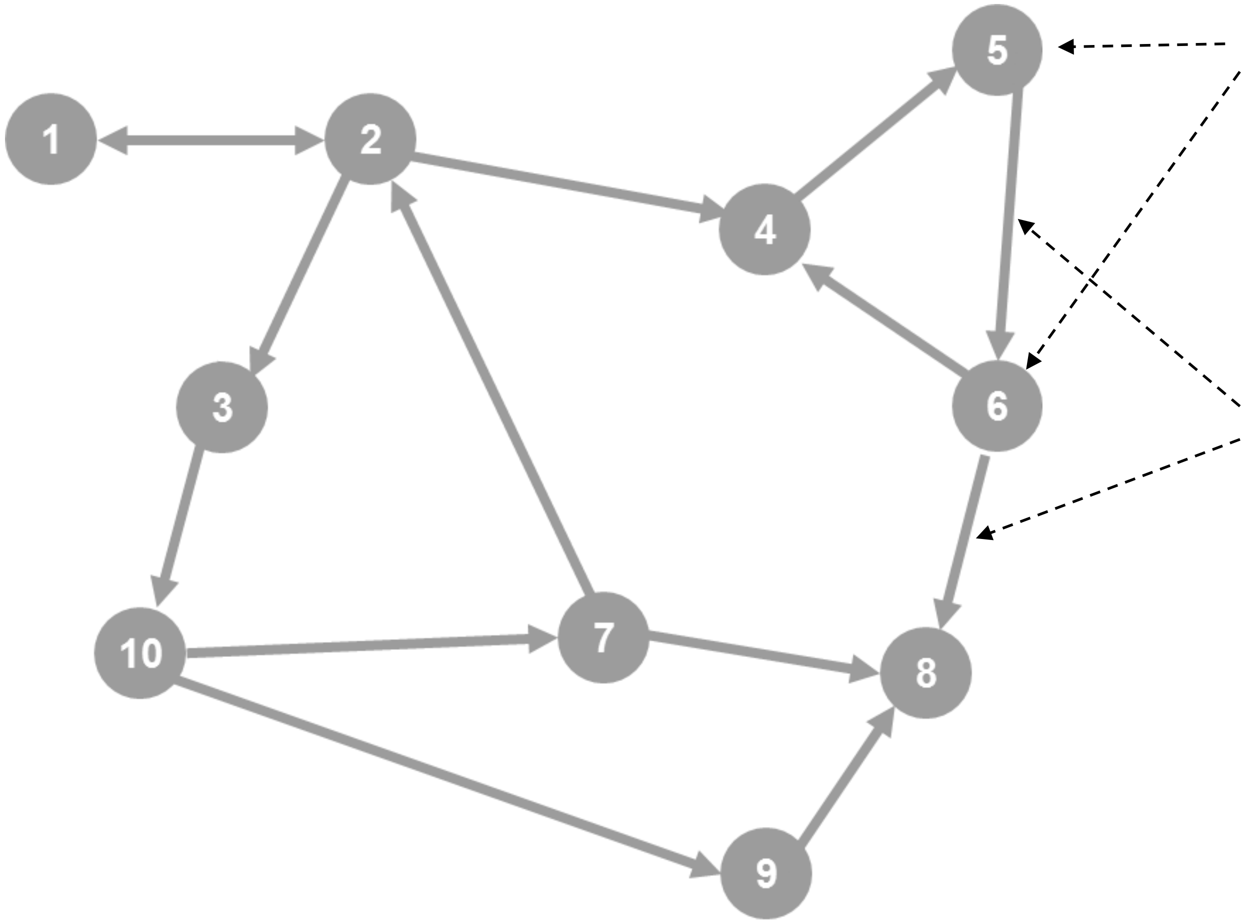


How a financial cybercrime group is organized

Kaspersky Lab is actively investigating five large, Russian-speaking cybercriminal groups involved in stealing money using malicious software.

The Money flow manager transfe
s provided by the Money mules
manager. The Money mules manager instructs the money mules where to transfer the money. A share of the stolen money ends up with the Head of the money mules service, while the rest is transferred to the Leader of the criminal group.

DETECTING FRAUD BY IDENTIFYING SUSPICIOUS MONEY FLOWS



Nodes: Bank accounts

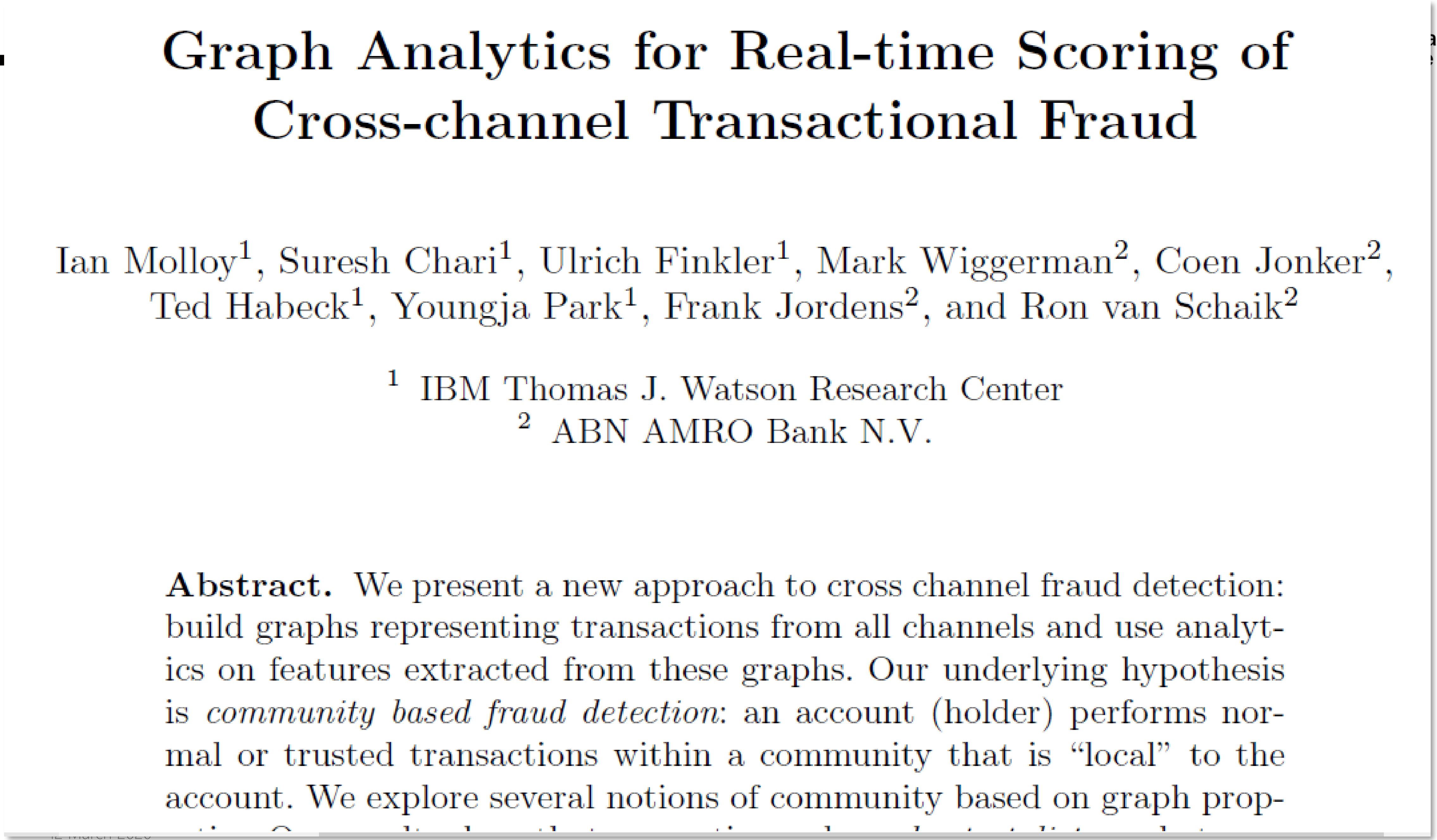
Links: Transactions

Additional properties per link:

- Number of transactions
- Total amount of money transferred
- …

For a given time interval

ation



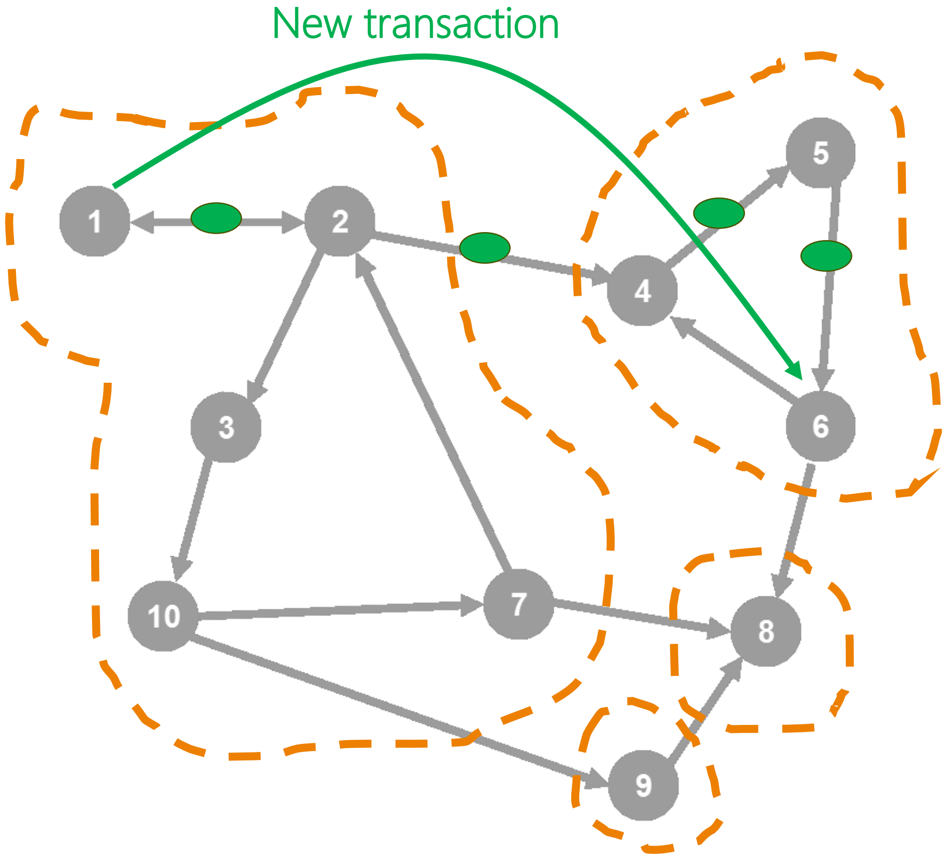
Graph Analytics for Real-time Scoring of Cross-channel Transactional Fraud

Ian Molloy[1], Suresh Chari[1], Ulrich Finkler[1], Mark Wiggerman[2], Coen Jonker[2], Ted Habeck[1], Youngja Park[1], Frank Jordens[2], and Ron van Schaik[2]

[1] IBM Thomas J. Watson Research Center
[2] ABN AMRO Bank N.V.

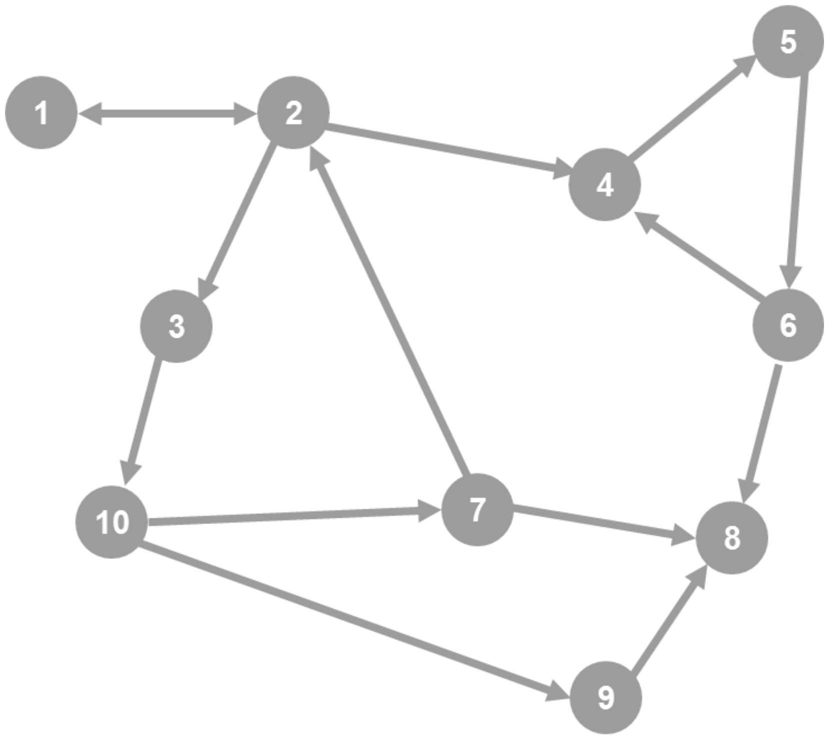
Abstract. We present a new approach to cross channel fraud detection: build graphs representing transactions from all channels and use analytics on features extracted from these graphs. Our underlying hypothesis is *community based fraud detection*: an account (holder) performs normal or trusted transactions within a community that is “local” to the account. We explore several notions of community based on graph prop-

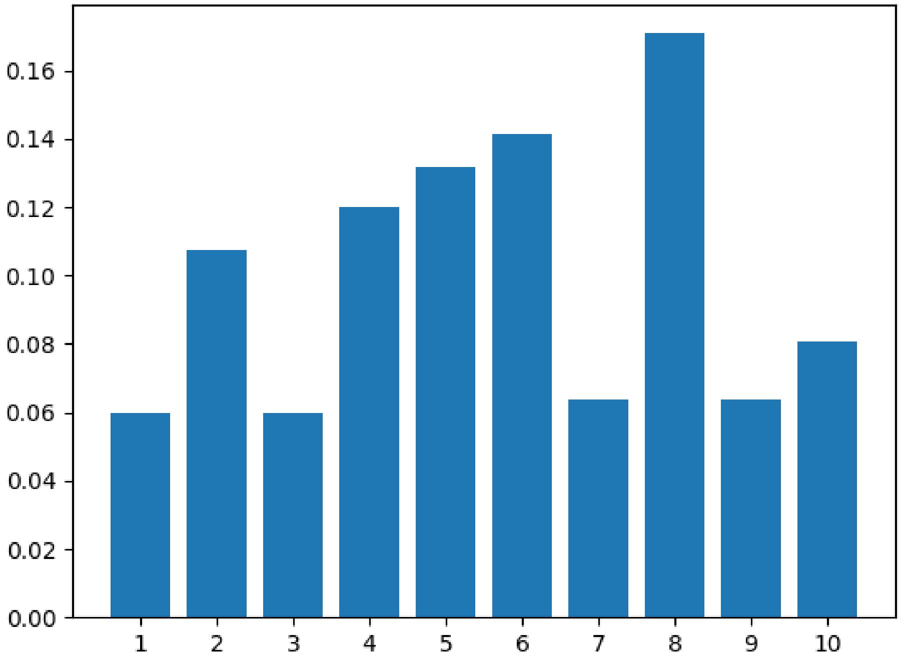
FEATURES INVESTIGATED



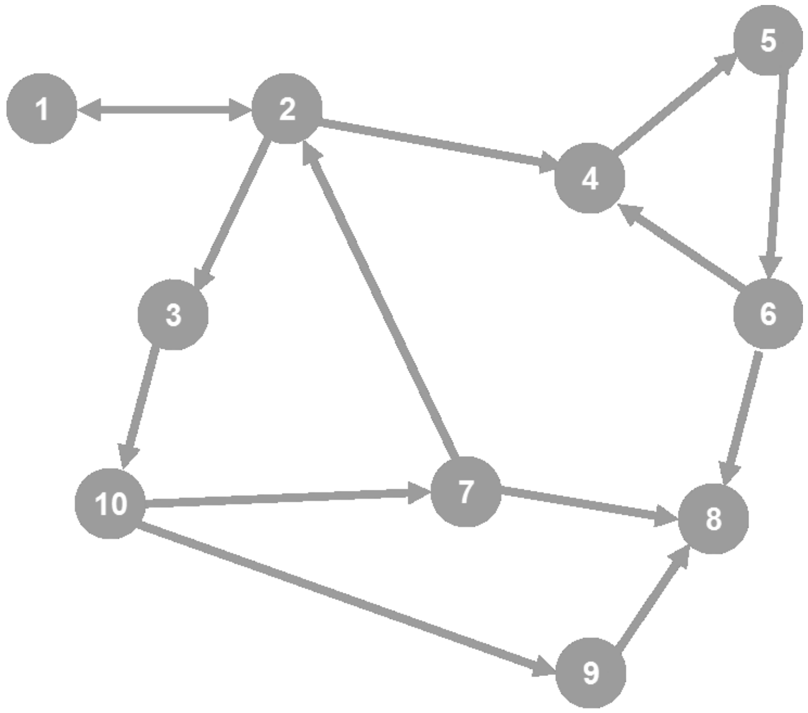
- **Shortest Path**
  distance between debit and credit
- **Strongly connected components**
  financial 'communities'
- **PageRank**
  Trust score for an account…
  used by Google to rank search results.

PAGERANK IS A CENTRALITY MEASURE

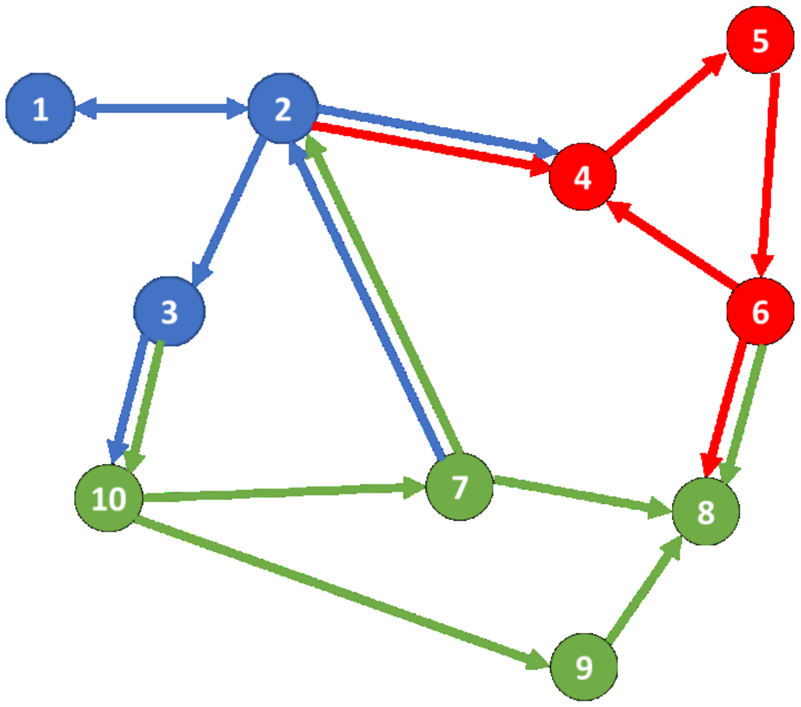




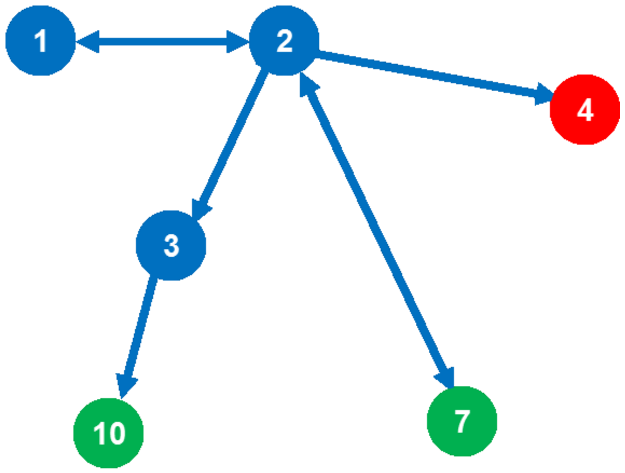
MONEY FLOW INFORMATION IS DISPERSED OVER MULTIPLE BANKS



Total network



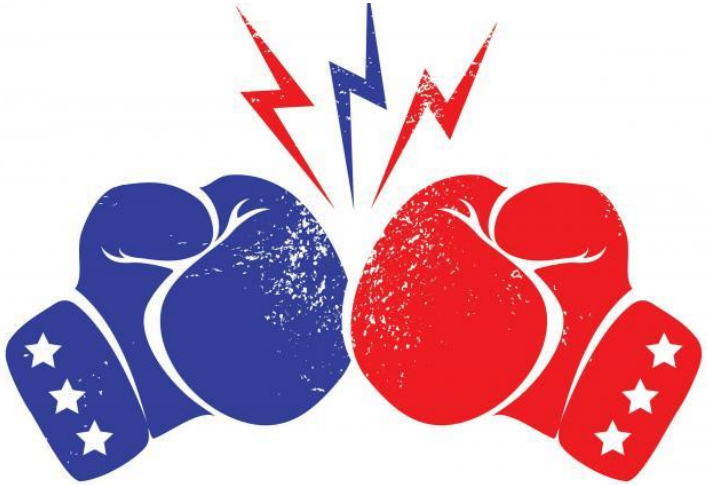
Network per bank



Network seen by blue bank

THE MULTIPARTY COMPUTATION PARADOX

Information Sharing
Collaboration



Privacy
Confidentiality

THE MPC PARADOX – RESOLVED

Information Sharing
Collaboration

Conclusion

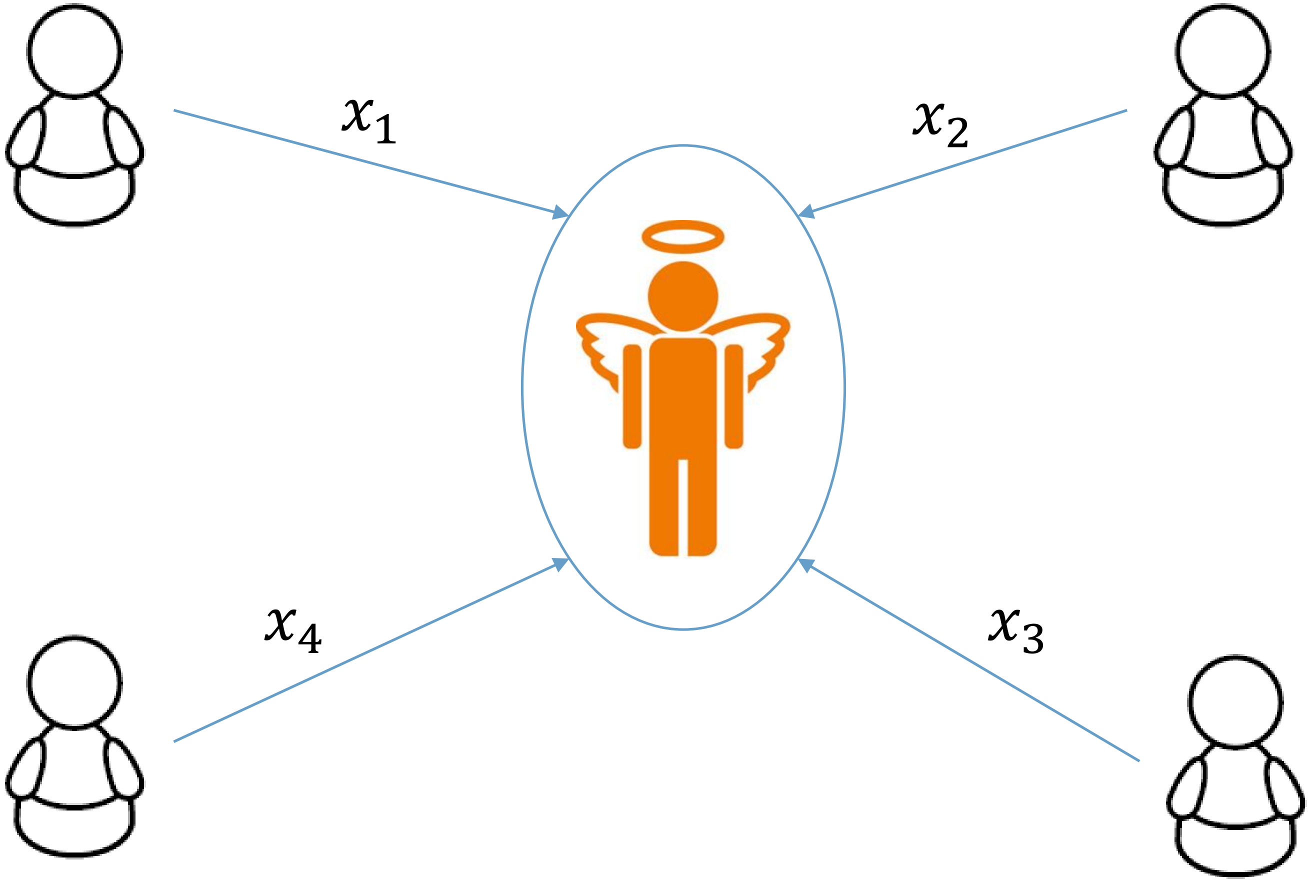
MPC

Privacy
Confidentiality

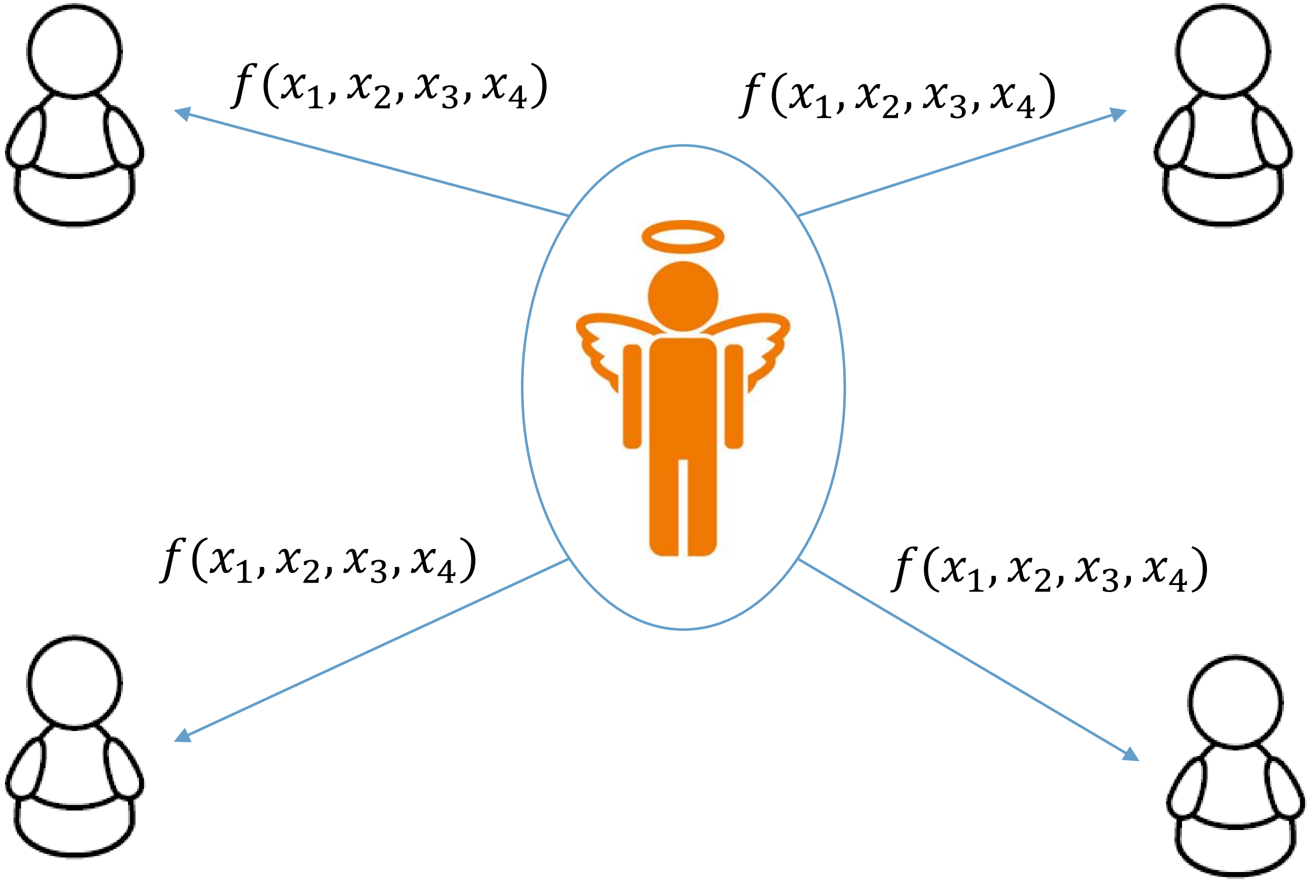
MULTI-PARTY COMPUTATION

A CRYPTOGRAPHIC SOLUTION

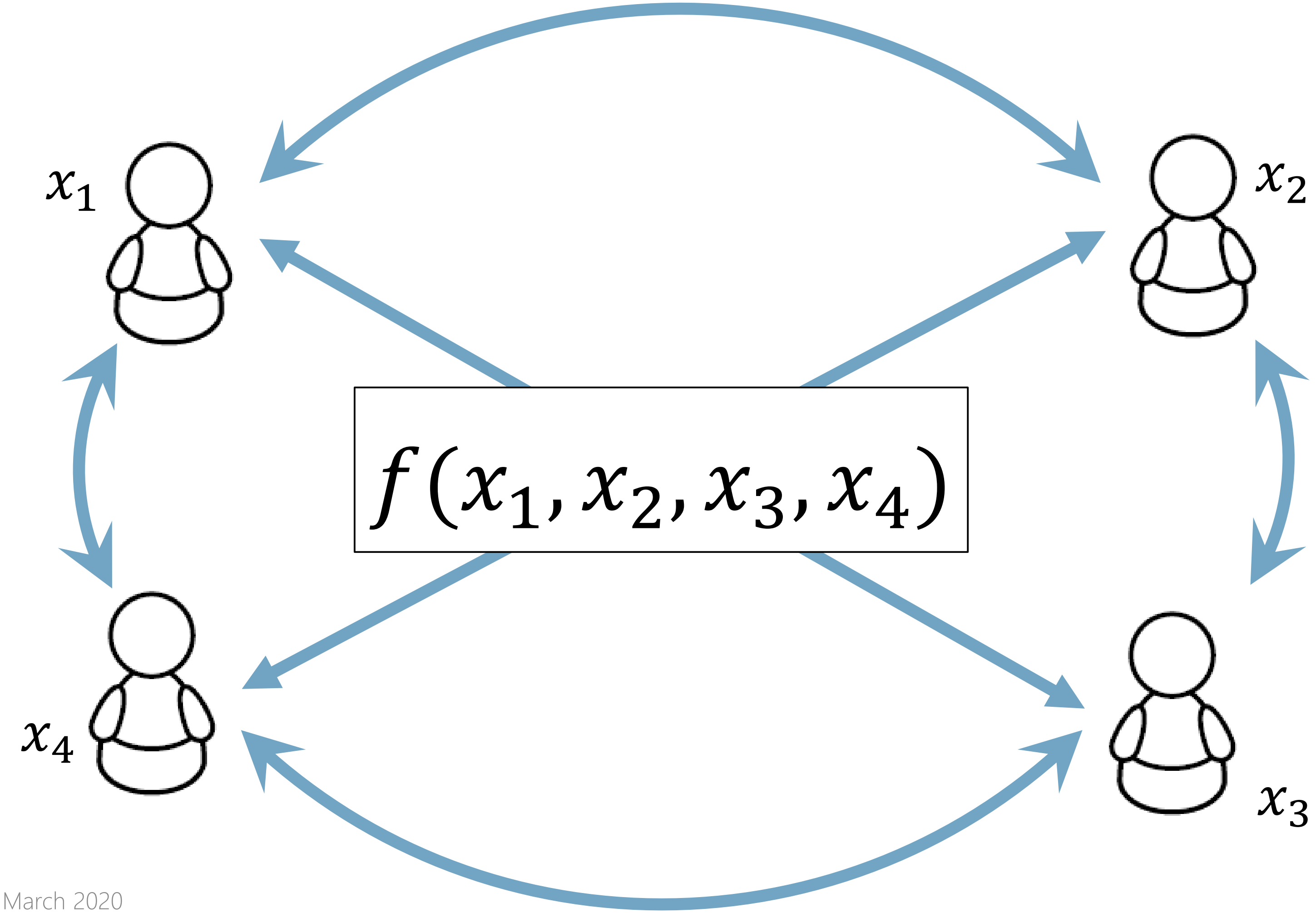
JOINT COMPUTATION WITH A TRUSTED PARTY



JOINT COMPUTATION WITH A TRUSTED PARTY



SECURE MULTI-PARTY COMPUTATION

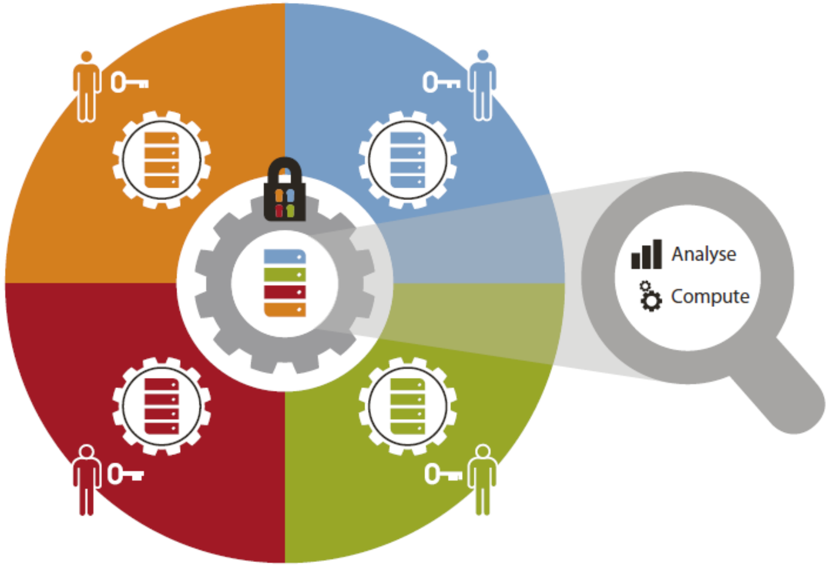


- *Privacy*
  - Private inputs remain private
- *Correctness*
  - Output is guaranteed to be correct

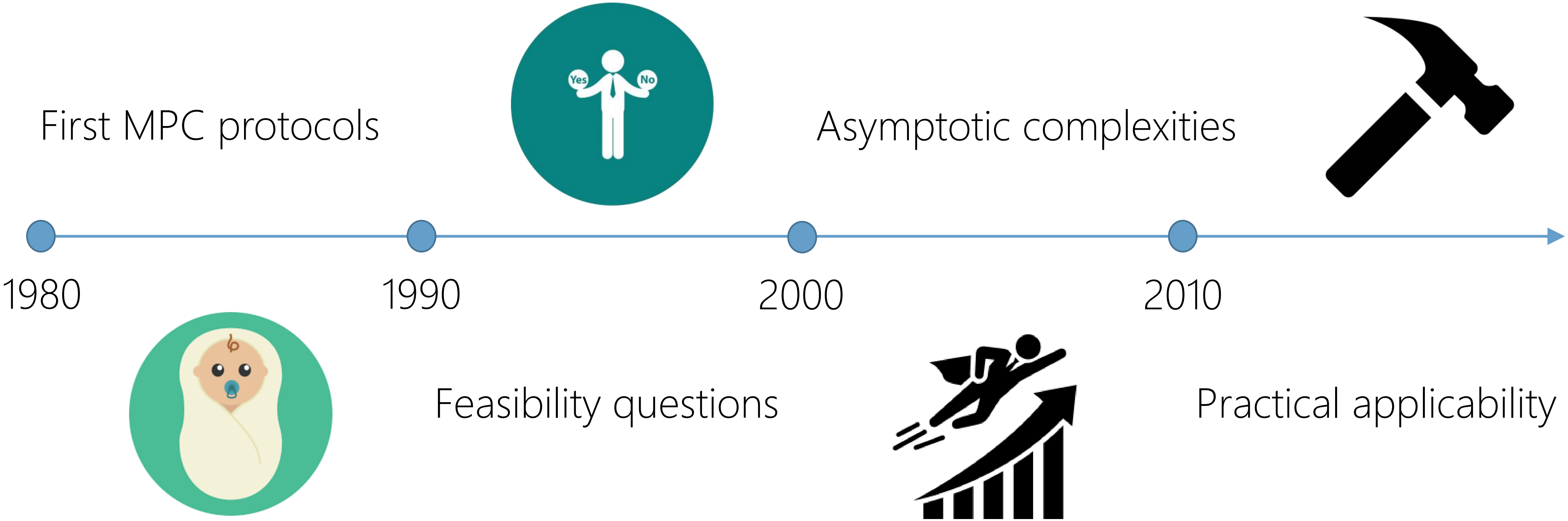
12 March 2020

MPC AND BLOCKCHAIN
TWO CRYPTOGRAPHIC TECHNOLOGIES TO DECENTRALIZE

- Both alternatives for ***trusted third parties (TTP)***
- MPC focusses on disintermediation and establishes ***confidentiality***
- Blockchain focusses on disintermediation and establishes ***data integrity*** and ***non-repudiation***



HISTORY OF MPC



First MPC protocols

Asymptotic complexities

1980

1990

2000

2010

Feasibility questions

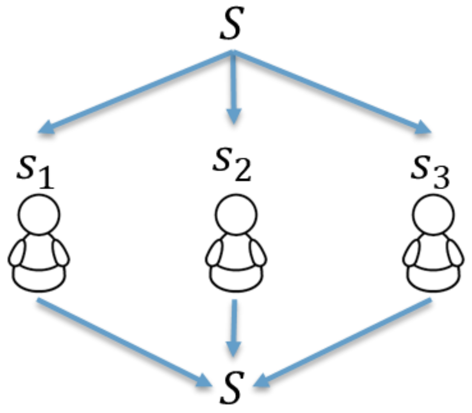
Practical applicability

MANY DIFFERENT MPC TECHNIQUES

- (Fully) homomorphic encryption
  - *Computation on encrypted data*

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, "Enc"'] & f(m) \\
Enc(m) \arrow[r, "f'"] & Enc(f(m)) \arrow[u, "Dec"']
\end{tikzcd}$$

- Garbled circuits
  - *Encrypted Boolean Circuits*
- Secret sharing
  - *Dividing a secret S into various shares*

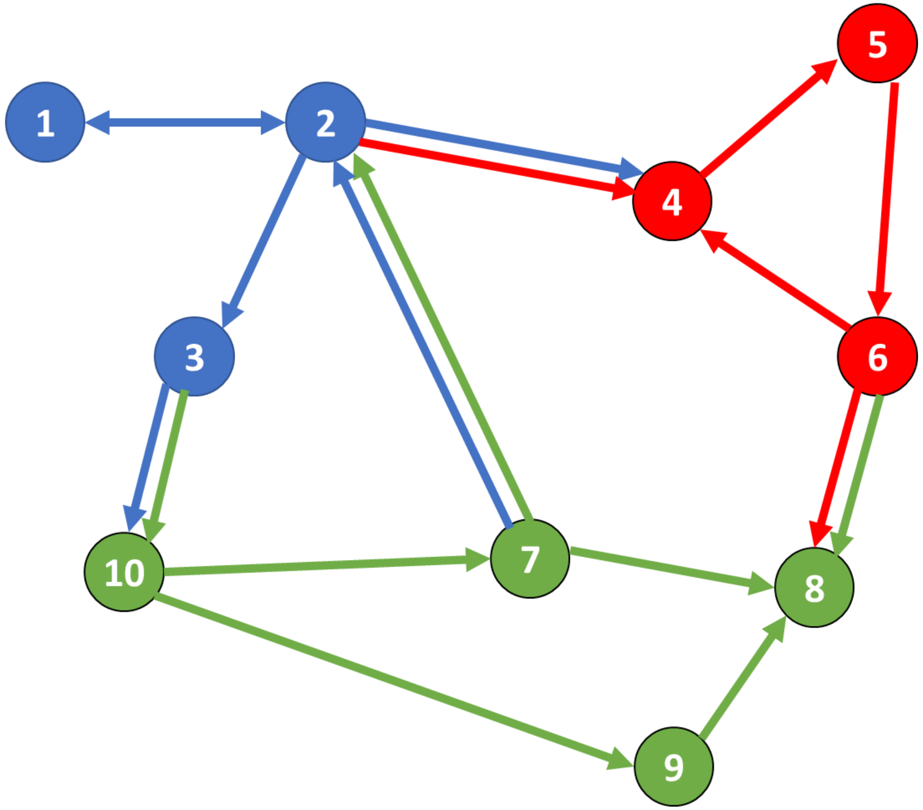


A ‘toolbox’ of cryptographic techniques, but no one-size-fits-all solution

THE CHALLENGES OF APPLYING MPC

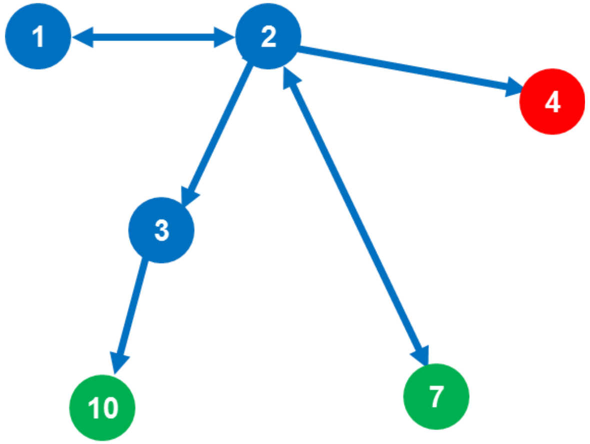
- Technological
  - *What are the theoretical limitations of MPC?*
  - *What is the optimal MPC protocol for this specific solution?*
  - *What ad-hoc efficiency improvements can we make?*
- Legal
  - *Does MPC comply with privacy legislation?*
- Ethical
  - *Do we want to create this functionality in all cases?*

COLLABORATION IS REQUIRED TO ANALYSE THE COMBINED TRANSACTION NETWORK



- Three different parties: A, B, C

- Party A only sees the blue transactions:



- Challenge: how can we compute the PageRank of each node?
- Solution:
  - ~~Trusted third party~~
  - Secure multi-party computation

CRYPTOGRAPHIC BUILDING BLOCK
HOMOMORPHIC ENCRYPTION

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, "Enc"'] & f(m) \\
Enc(m) \arrow[r, "f'"] & Enc(f(m)) \arrow[u, "Dec"']
\end{tikzcd}$$

PROTOCOL ARCHITECTURE

Key generation:

- Centralized. Provide a public key and partial private keys.

Initialization:

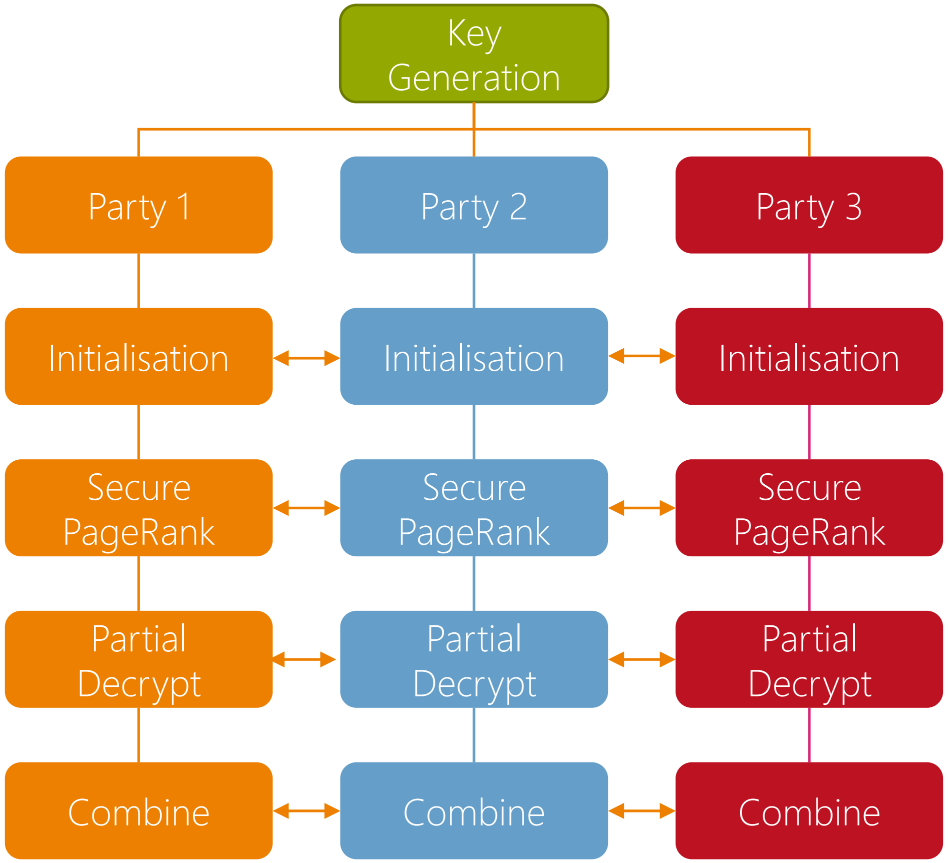
- Collaboratively compute n (total number of nodes).

Secure PageRank:

- Only share encrypted PageRank contributions and values at each PageRank iteration.

Partial Decrypt & Combine:

- Collaboratively decrypt the PageRank values with partial decryptions.



CONCLUSION

- MPC allows banks to
  - Collaboratively analyse transaction networks
  - Without sharing private data
- Only the output of the computation is revealed by the protocol
- The protocol eliminates the need for a trusted-third party
- An implementation is readily available

THANK YOU FOR YOUR TIME

TNO innovation for life