簡単で軽い話。

インターネットおよびデータ保険、ブロックチェーン

パート1：サイバー保険の証券化

GREGORY FENN :: グレゴリー・フェン　(グレグ)

ロンドン大学

ROYAL HOLLOWAY UNIVERSITY OF LONDON

EPSRC
Engineering and Physical Sciences Research Council

CYBERINSURANCE AND BLOCKCHAINS. (AN EASY AND LIGHT TALK.)

PART 1: THE SECURITISATION OF CYBERINSURANCE

GREGORY FENN :: グレゴリー・フェン　(グレグ)

INFORMATION SECURITY GROUP
ROYAL HOLLOWAY UNIVERSITY OF LONDON

パート1の概要

- サイバー・インナブル … データ保険
- 背景: 債券の証券化への導入
- 保険関連証券（ILS）
- 大惨事債券（ネコ債）の概念
- 関連する総リスク
- サイバー保険リスクのモデリングフレームワーク
- 一般的な結論
- オープンな質問と今後の作業

OVERVIEW OF THIS PART 1

- Background: brief introduction to cyberinsurance & securitisation of debt

- Insurance-linked Securities (ILS)

- Notion of catastrophe bonds (cat bonds)

- A modelling framework for cyberinsurance risk

  - general conclusions

- Open questions and further work

サイバー保険は何をカバーしていますか?

企業はサイバー愛好家!!

- インターネットがオフになります
- サイバー恐喝
  - ランソムウイルス
    （CryptoLocker、WannaCry）
  - ウイルスや恥ずかしいメディアをアップロードすることに脅威を与えます。
- 会社（または愚かな従業員）は著作権法を偶然破ります。 または、会社がプライバシー法を偶然破ります。
- 彼らは、ハッカーのサイバー犯罪者のために攻撃されます。 だから彼らは仕事をすることができないので、彼らはお金を失い、罰金を科され、顧客を失う。

“On the limits of cyber-insurance”. Böhme and Gaurav. 2006.

CYBER AND DATA INSURANCE

BUSINESSES NEED ALL THE CYBER

- Network downtime
- Cyber-extortion
  - Ransoms
  - Reputational harm
- Critical infrastructure attacks from terrorist groups or warfare
- Cyber-esponiage leading to market harm

"On the limits of cyber-insurance". Böhme and Gaurav. 2006.

「アセット」とは、価値または富を生み出す所有するオブジェクトを意味します

「リスク」：資産によって生み出される価値の不確実性

"ASSETS": VALUE-GENERATING PROPERTY

"RISK": UNCERTAINTY IN THE VALUE TO BE GENERATED BY AN ASSETT

ガウスリスクアセットの例

本当にガウスではない

- イギリスでは**140000000**円の封筒（**E**）があります
- 為替レートは

  ¥140 000 000 = £1 000 000

- それが私が知っているものであれば、**1**年後の**E**の値はガウス分布です

  $E \xleftarrow{£} N(1\ 000\ 000,\ 114\ 286^{**})$

  平均は**£1000000**で、標準偏差は**114286**です

*実際には、これは貧弱なモデルになります。変更は乗法であり、加算ではありません

EXAMPLE OF A NORMAL RISK ASSET

NORMAL THINGS ARE ABNORMAL

- Suppose I have an envelope E containing ¥140 000 000
- Currently, the exchange rate is such that

  ¥140 000 000 = £1 000 000
- Assuming we don't know more about global market dynamics and Japanese fiscal policy than anyone else, we might* model the value of E after one year using a Gaussian distribution

$$E \xleftarrow{f} N(1\,000\,000,\ 114\,286^{**})$$

*ACTUALLY THIS WOULD BE POOR MODEL, AS CHANGES ARE MULTIPLICATIVE, NOT ADDITIVE

**BASED ON AN EMPIRICAL ST.DEV OF 16 JPY:: (1/140)*16*1000000 = 114286

この男はさすけと呼ばれています

彼は、ローンや金融デリバティブなど、多くの高付加価値資産を所有しています

彼は彼らが大きな利益を得ると信じている。 だからソースケはこれらの資産をさらに買うためにもっとお金を借りる。

しかし、ソスケは落ちるかもしれないと分かっていて、彼が彼のお金を失うことを心配している。

したがって、リスク資産全体を他の誰かに売却する必要があります。 それから、他の人たちがリスクを抱えています。

すすけは豊かです。
あなたはすすけのようでなければなりません。

SECURITISATION IS FOR RISK-HUNGRY INVESTORS WHO OVEREAT

THIS IS BILL

BILL OWNS LOANS, BANKRUPTCIES, MORTGAGES AND FUTURE DERIVATIVES.

BILL EXPECTS THESE TO MAKE MONEY FOR HIM, SO BILL INVESTS THE MONEY HE HASN'T MADE YET TO MAKE EVEN MORE.

BUT BILL DOESN'T WANT TO ACCEPT THE RISK THAT THE ORIGINAL ASSETS WON'T PAY-OFF AFTER ALL.

SO BILL WRAPS-UP THESE ASSETS INTO A PACKAGE AND SELLS IT ON IN CHUNKS.

BILL IS RICH.
BE LIKE BILL.

私たちが望むなら、これは100万ポンドでできる危険な資産です。

0.3

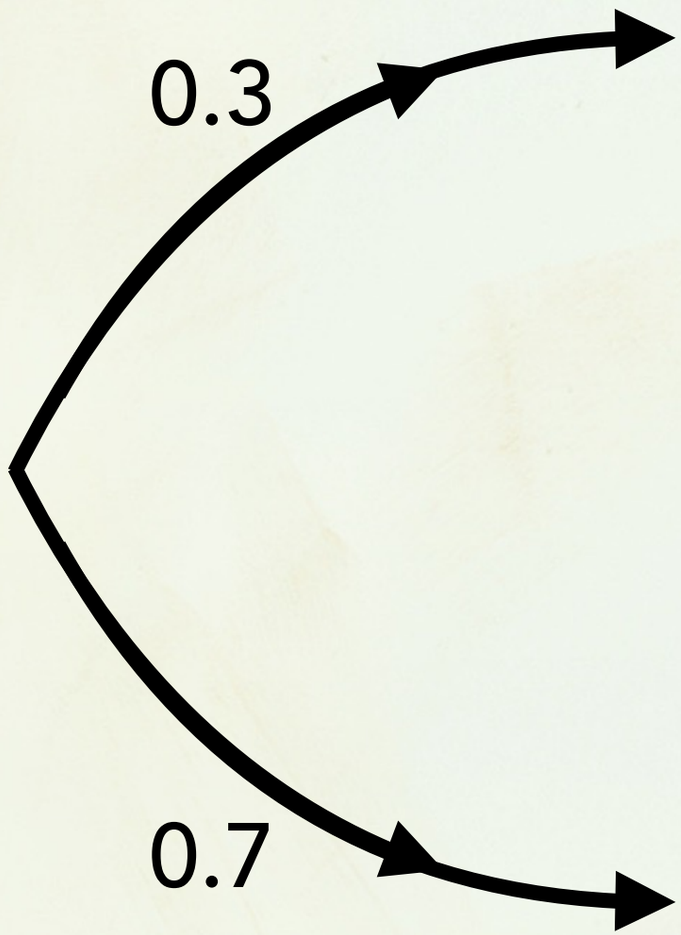
500万ウォン獲得

0.7

ゼロに勝つ。 何もない。

この商品を購入すれば、平均利益は50万ドルになります。 これは大きな平均利益です。 しかし、それは危険です。

A VERY RISKY ASSET: WE CAN BUY IT FOR £1M



Get £5M!!

Lose it all…

Expected return £1.5M

Expected profit £0.5M

このリスクをどのように証券化していますか?

- 資産を購入し、それを大銀行に0.35百万株で売却することに同意することができます。

- 我々はリスクなしで良い利益を上げる。 銀行はまた、良い利益を上げる。

- 銀行には多くのリスク資産があり、リスクのないポートフォリオ（資産の集合）に平均しています。

- リスクの高い資産をより大きなグループに販売するこの方法は、「証券化」です。

"SECURITISING" THIS RISK

- The long-term investment produces a good expected profit per unit (0.5), but the risk of ruin is huge (0.7), too high for us.

- Suppose we come to a deal with HSBC and agree to the following simplified contract:

- We sell the risky asset to HSBC for a price = 1.5 - p (where p = expected profit to HSBC.)

- HSBC then accept all the stochastic losses and gains on the asset, while we simply keep a fixed return of r = 1.5 - p

- If p < 0.5, then we still make an overall profit from buying the risky assett and then immediately selling it to HSBC.

- E.g. if p = 0.35, both us and HSBC do rather well

- —> HSBC can diversify-away their own risk by coming to similar deals with 1000s of other people.

災害債券。 非常にありそうもなく、非常に悪い出来事のための金融デリバティブ。

保険会社の証券化の一種。

- 保険会社は投資家に似ています。 保険会社は何かが良い状態（高価値）で長時間賭けることを（ギャンブルで）賭けている。さもなければ彼らは賭けを失い、お金を失わなければならない。

- 保険会社は、すべてのお金を失う大惨事が心配です。

- 例えば、フロリダの住宅保険会社は、被保険者全住宅を破壊するハリケーンが心配です。

- 「災害債券」は、他の投資家がこの災害イベントが起こらないようにする賭けです。 それが起これば、彼らは保険会社にたくさんのお金を送ります。

“Modeling Fundamentals: So You Want to Issue a Cat Bond?”. AIR (report). 2016.

CATASTROPHE BONDS

A SPECIAL KIND OF SECURITISATION FOR INSURANCE FIRMS

- An insurer can be understood as an investor who takes a "long position" against a client's business, or some asset of their's, or even their life.

- The insurer will want to diversify (smooth-out) their long positions so their their aggregate portfolio is Gaussian, with a negligible standard deviation.

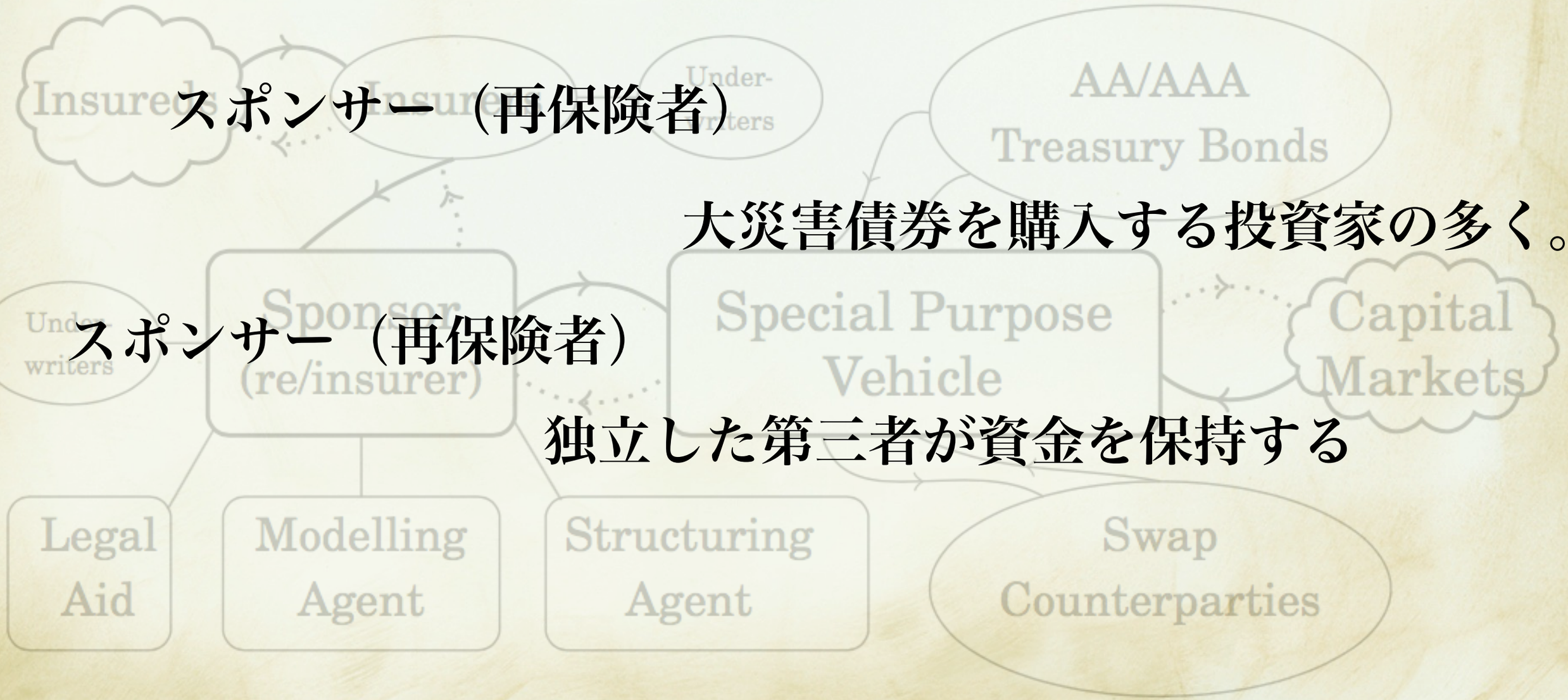
- But consider a property insurer who covers homes in Florida. Should a hurricane directly hit Orlando the chance of ruin becomes very high. These catastrophes create correlated risk, making the insurer's loss distribution very un-Gaussian.

- By packaging up these extreme risks and selling to banks and capital markets, the insurer can effectively "reinsure" themselves against catastrophes.

"Modeling Fundamentals: So You Want to Issue a Cat Bond?". AIR (report). 2016.

災害債券

これは、これらの債券が通常どのように構成されているかです。



スポンサー（再保険者）

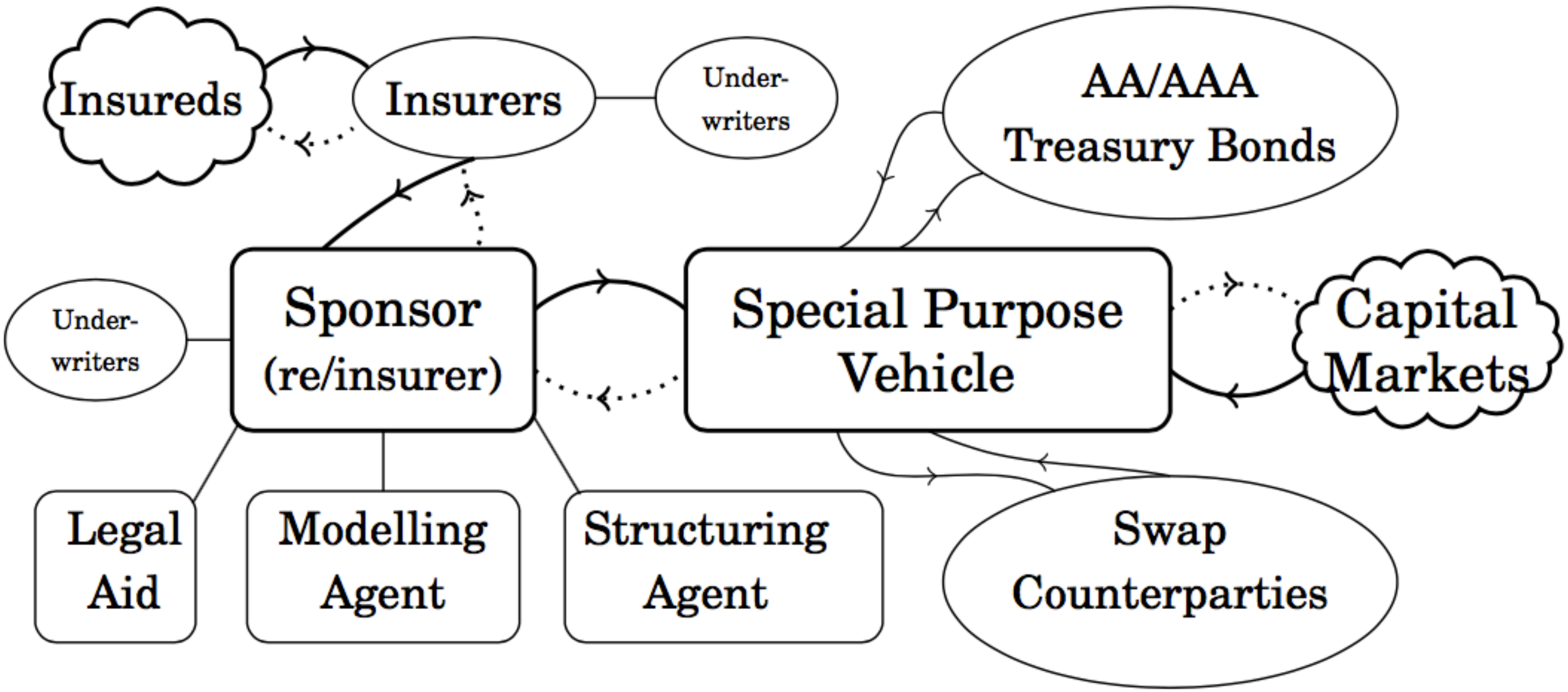
大災害債券を購入する投資家の多く。

スポンサー（再保険者）

独立した第三者が資金を保持する

Cat Bonds

Traditional insurance firms will have used this kind of model for the last couple of decades (since Hurricane Andrew)

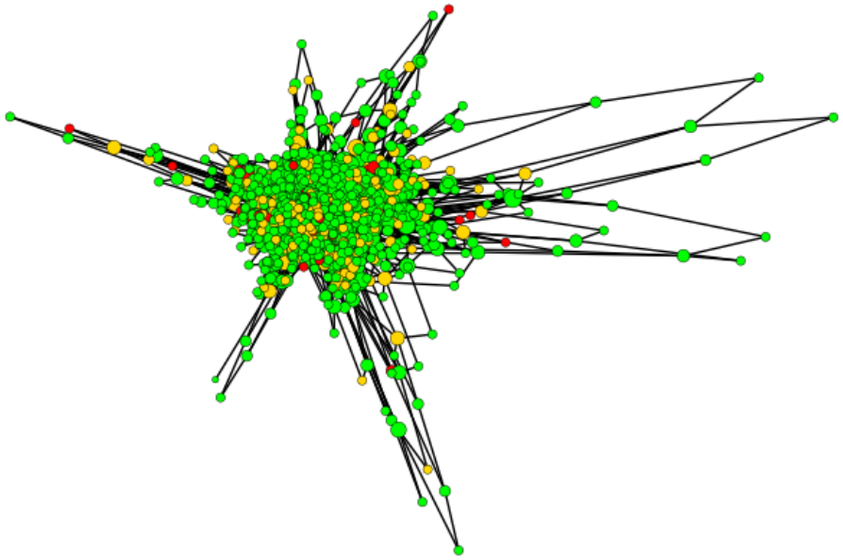


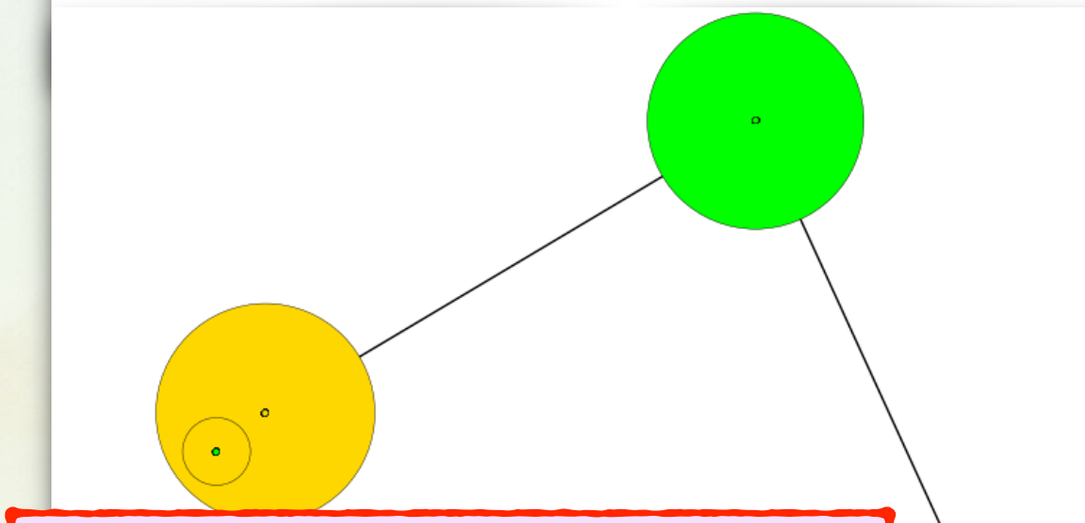
サイバーセキュリティとサイバー保険のリスクをモデル化する方法はたくさんあります。

これらのすべてが悪いです。 現実の生活では、サイバー保険会社はサイバーリスクを理解していません。

- 1つのモデルは、数学的グラフと「ネットワーク」を使用します。
- ノード（ドット）は事業と被保険者です。
- エッジ（線）は、データ接続またはビジネス関係です。
    - これは、サイバー脅威の接続性を記述することができます。 接続をモデル化します。
    - あるノードが犯罪者によって攻撃された場合、またはウイルスを取得した場合 接続された企業も危険にさらされています。
- これらの写真は私がいくつかの仕事で使ったネットワークの2つでした。 大きなノードには多くの友達がいます。 色は、同じコンピュータを使用するか、同じ国で同じようなプロパティをモデル化するために使用されます。

“The complexity of estimating systematic risk in networks”. Johnson, Laszka and Grossklags. 2014



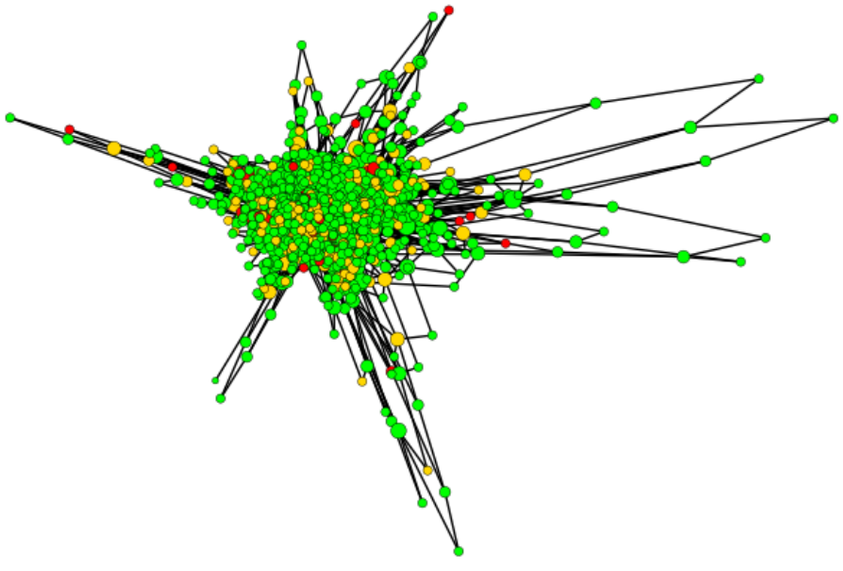


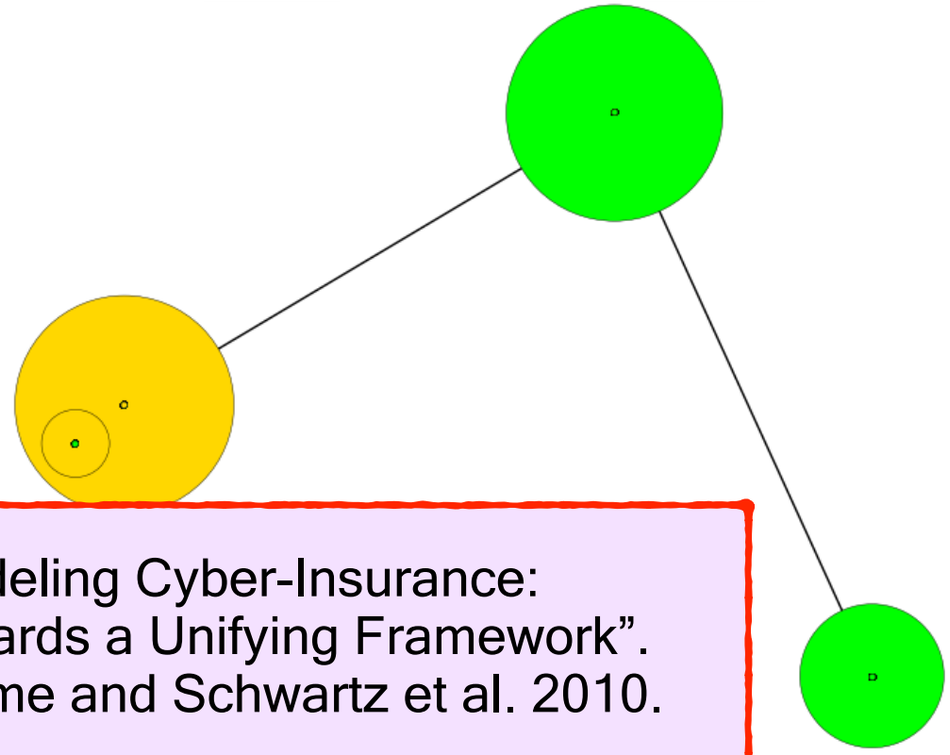
“Modeling Cyber-Insurance: Towards a Unifying Framework”. Böhme and Schwartz et al. 2010.

MODELLING CYBER-RISK

- Traditional cyber-risk models (especially for insurance) use the mathematical concept of a simple connected graph
  - A simple model for interdependency
    - positive externality of security
- These pictures were two of the networks I used in some work. The large nodes have many friends. The colours are used to model similar properties, such as using the same computers or in the same country.

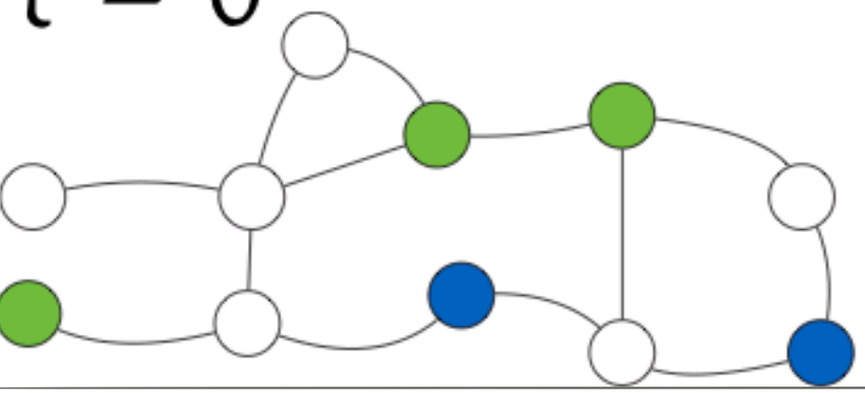
"The complexity of estimating systematic risk in networks". Johnson, Laszka and Grossklags. 2014





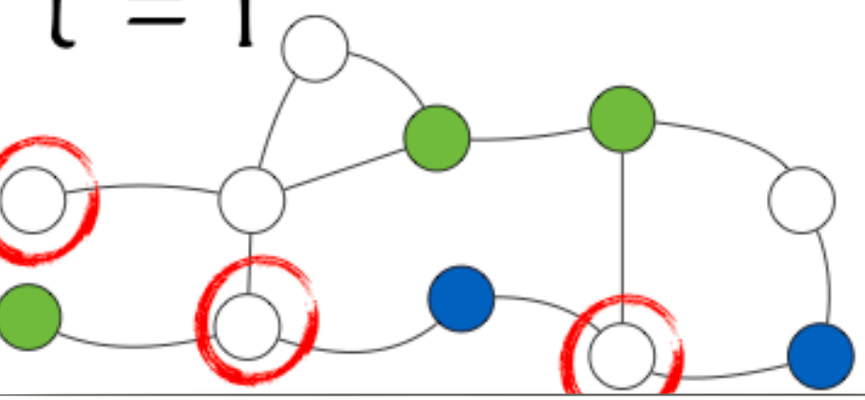
"Modeling Cyber-Insurance: Towards a Unifying Framework". Böhme and Schwartz et al. 2010.

τ = 0



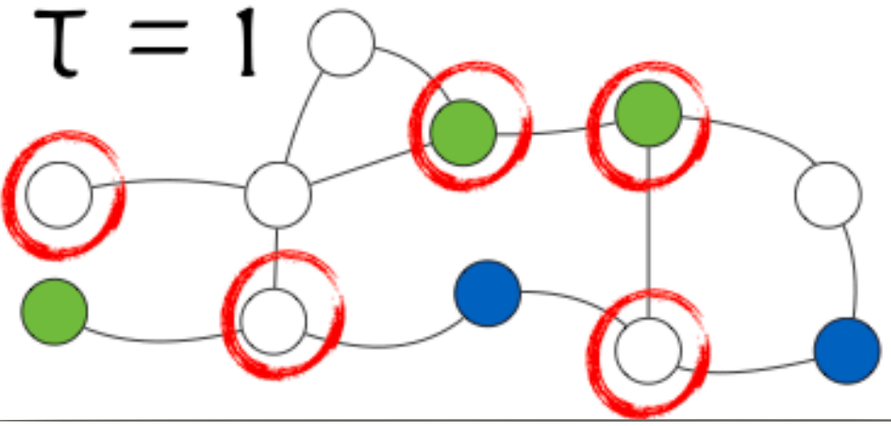
メキシコにいるため、いくつかのノードは緑色です。 一部のノードは**Microsoft Windows XP**を使用しているため青色です。

τ = 1



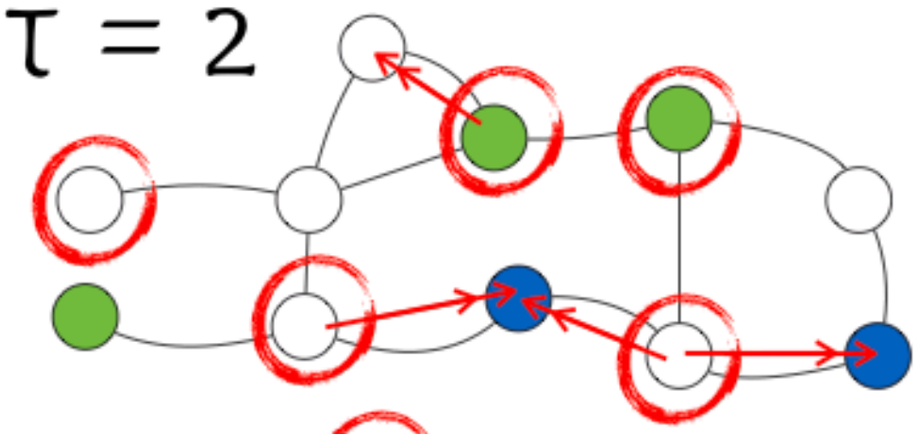
任意のノードは、犯罪者またはウイルスによってランダムに攻撃される可能性があります。

τ = 1



メキシコの悪い知らせ、電気が動いていない。 メキシコのほとんどの企業が影響を受けています。

τ = 2



被害は近隣住民にも感染する可能性があります。

τ = 3

感染しているほとんどの企業が問題を解決するか、隔離します。

τ = 4

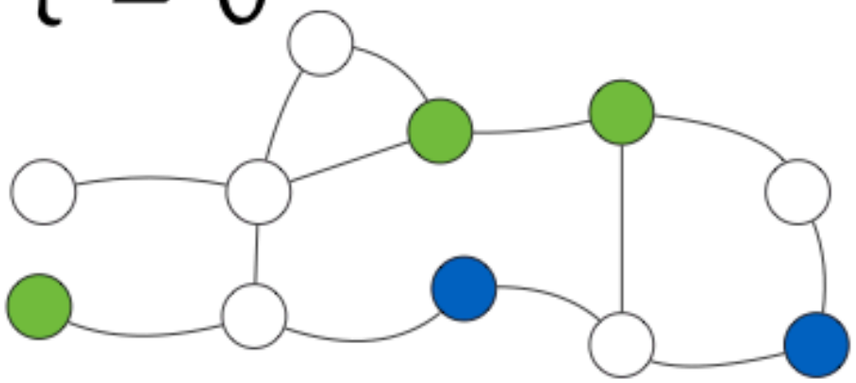
他の企業も依然として友人にとって脅威になる可能性があります。

τ > 4

我々のモデルでは、この感染は生存するウイルスがなくなるまで続きます。

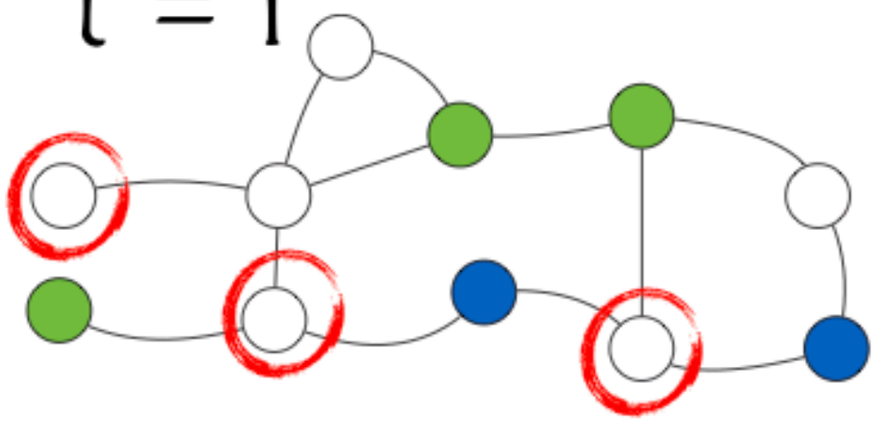
“A modified epidemiological model for computer viruses”. Piqueria and Araujo. 2009.

$\tau = 0$



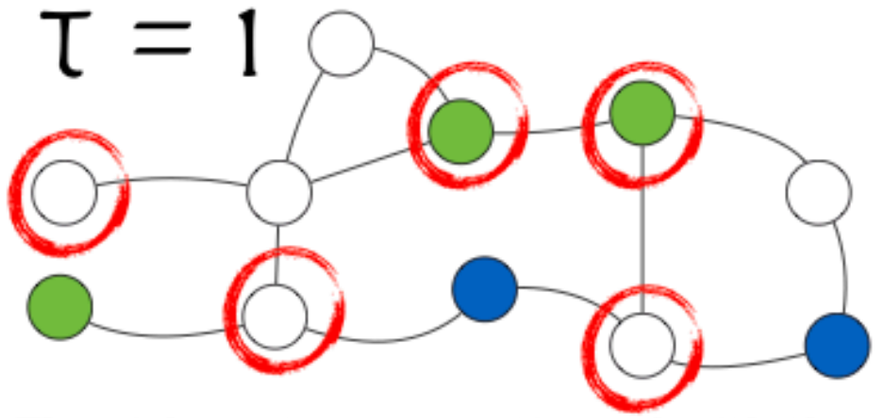
First we have a graph with some nodes associated with a given risk-feature (here represented with green or blue colours).

$\tau = 1$



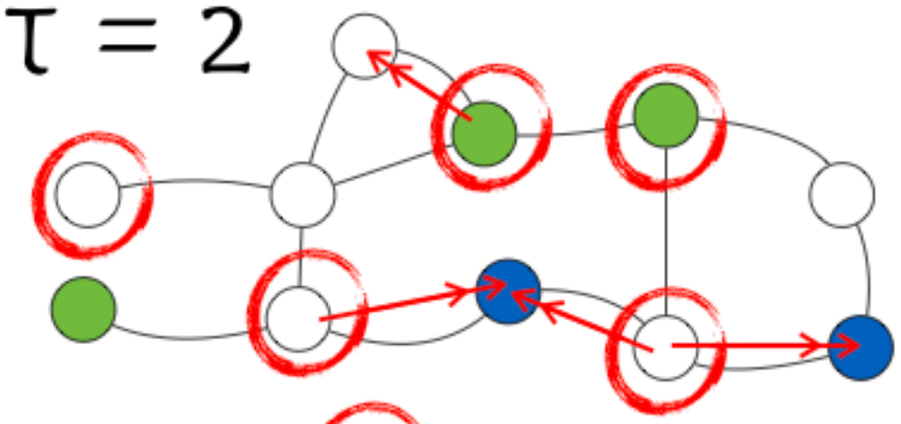
Then each node is randomly infected with an independent probability P: circled in red.

$\tau = 1$



The risk-vectors are activated with there own probabilities. Here "green" nodes turn out to be at risk, and so many green nodes that would otherwise be healthy are infected.

$\tau = 2$



With probability Q, infected nodes propagate damage to any neighbour.

$\tau = 3$

After each time–period, there is a high chance of infected nodes being "quarantined".

$\tau = 4$

But a small proportion of nodes may stay infected and continue propagating the risk.

$\tau > 4$

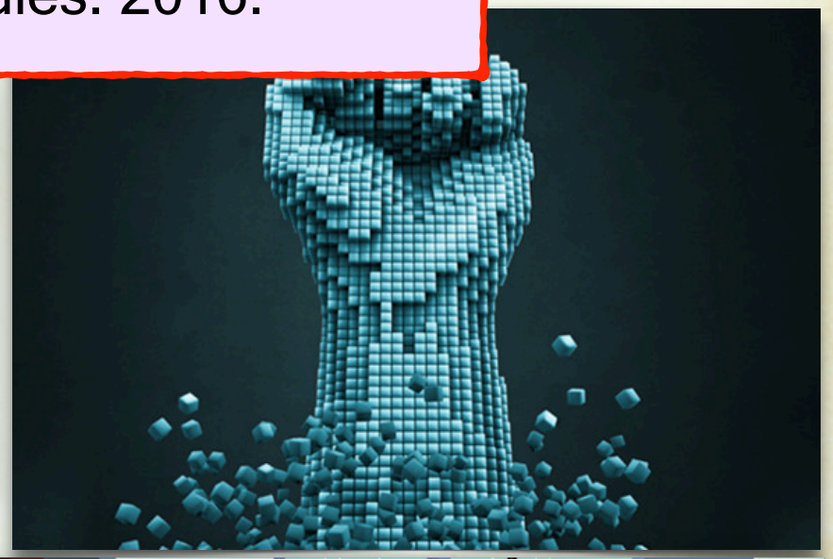
The process terminates when all infected nodes are quarantined.

"A modified epidemiological model for computer viruses". Piqueria and Araujo. 2009.

ケンブリッジ・リスク研究所に基づくサイバー破局債券の例

“Managing Cyber Insurance Accumulation Risk”. Cambridge Centre for Risk Studies. 2016.

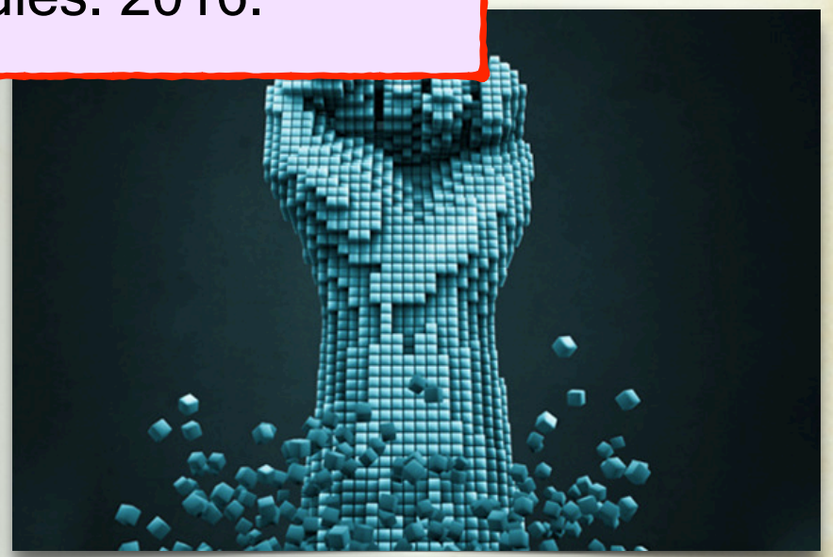
- サービス拒否攻撃がたくさんあります。
- 犯罪者は共謀して、強要と身代金のウイルスを送る。
- クラウドサービスプロバイダ（**iCloud、Amazon Web Services**）が攻撃されます。
- 大企業の正当なデータが公開されています。
- クレジットカードマシンやデジタルマネーマシンがハッキングされています。



CYBER CAT BONDS

"Managing Cyber Insurance Accumulation Risk". Cambridge Centre for Risk Studies. 2016.

- Mass DDoS
- Extortion Spree
- Cloud Compromise
- Leakomania
- Financial Transactional Interference



私たちの仕事で大惨事の絆を引き起こします。
サイバー保険の災害の定義のための提案。

相関リスク。 集約リスク。

✤ 例えば、テロリスト集団によるメキシコへの攻撃。
Microsoft Windows 10の重大な致命的なソフトウェアのバグの脆弱性

✤彼らは起こることはまれであるが、そうであれば同時に多くの同様の事業に影響を与えるだろう。

接続とリンクからのリスク。

✤ 多くの重要なノードが感染しています。 例えば、インターネットサービスプロバイダ、またはドメインネームサービスが提供する。

✤他の多くのビジネスに不可欠なビジネス。 彼らが侵害された場合、これは非常に悪いです。

TRIGGERS FOR CYBER RISK

'CYBER' IS STILL A VAGUE TERM

Correlational Risk

- Identify a subset of risk-features of firms such that, if a threat affects only firms with those features, that event acts as a trigger.

- Can use conjunctive or disjunctive forms to get more precise parametrics, and to keep the probability of trigger at around 1%

Interdependent Risk

- Identify some notion of "exogenous risk"

- Define a metric on the portfolio of clients that captures this exogenous risk

  - e.g. the sum of the degrees of the firms that are directly affected by random attacks

- Then define a trigger based on the output of that metric

CYBERINSURANCE AND BLOCKCHAINS.

PART 2: THE POTENTIAL OF BLOCKCHAINS

サイバー保険とブロックチェーン。

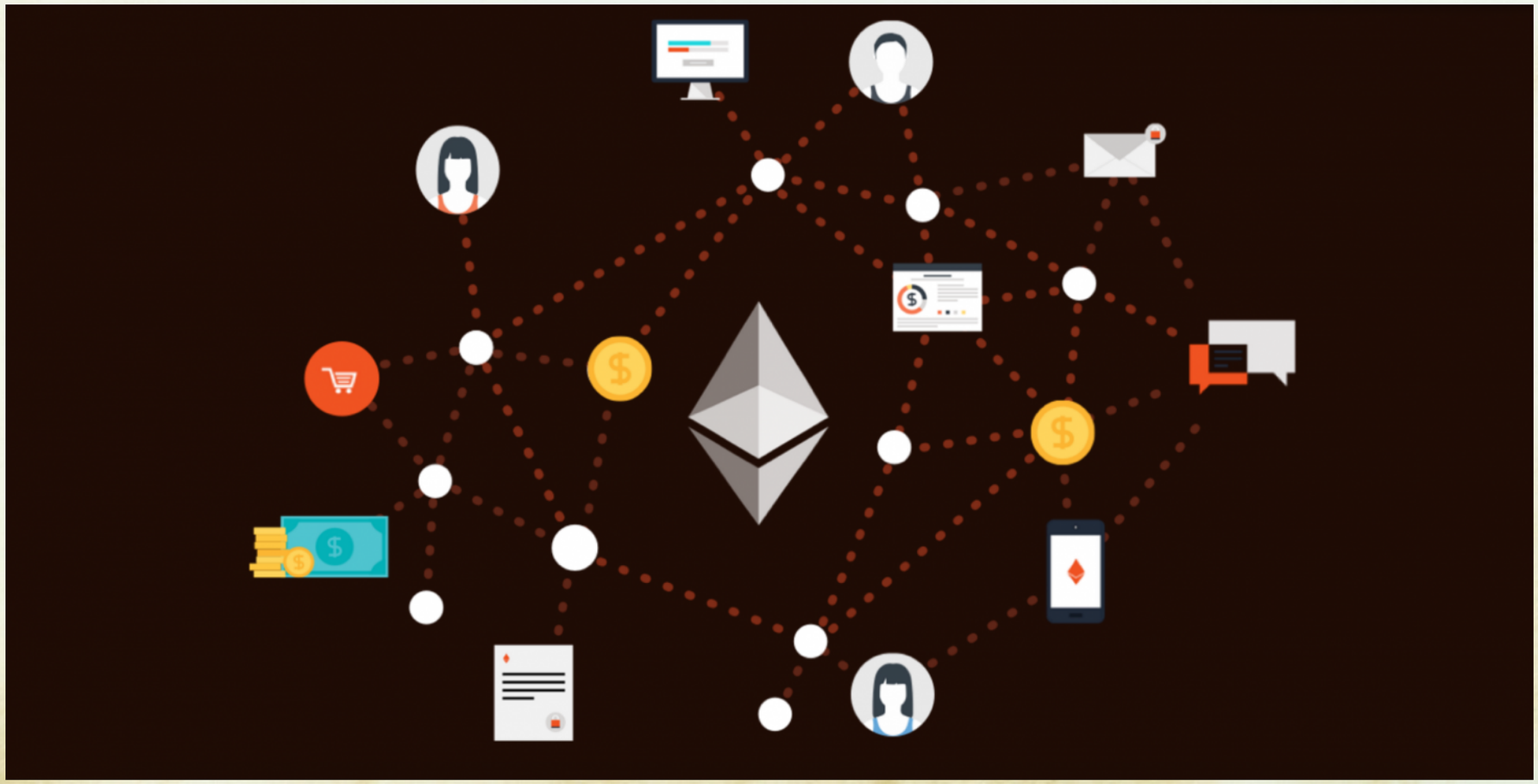
第2部: ブロックチェーンの可能性。 いくつかのアイデア。

本旨

* **Ethereum**に似た公開ブロックチェーンで分散コンピュータアプリケーションを使用する。

* 企業はパブリックアドレスを使用して、サイバー攻撃やデータの消失または悪いイベントを報告します。 誰もがそれを読むことができますが、誰がメッセージを送ったのかは分かりません。

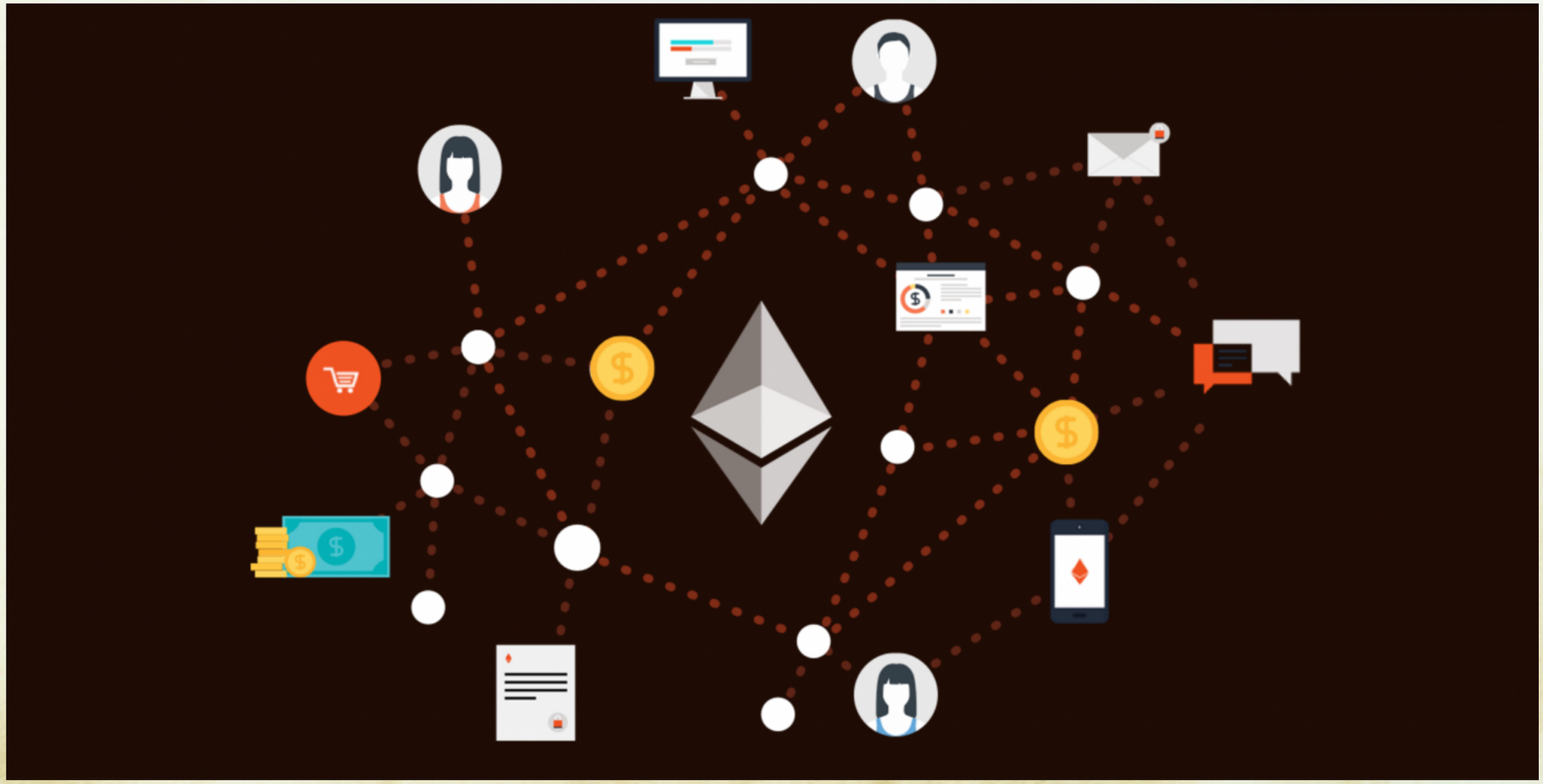
* その後、ビジネスはスマートな契約で自動的に報酬を受け取ることができ、デジタル契約は公的なブロックチェーン上で実施されます。



GENERAL IDEA

* Use DAPPs on a public blockchain such as Ethereum to enforce and define cyberinsurance (CI) policies, products, event definitions, payouts and fraud history in the form of smart contracts.

* All cyber-incidents to be publicly reported, as well as all policies offered/accepted.



“Cyber Insurance [is] ’held back’ by lack of data”. Ralph (Financial Times). 2017.

良いと悪い理由。

“Insurers tap cyber security ratings to limit liabilities”. Kuchler (Financial Times). 2017.

* 過去の取引および支払いは、公に観察され、監視されています。 正直な信用履歴

* 契約は明確に定義されており、常に尊重され強制されます。

* 多くのデータが利用可能となり、保険会社はリスクをよりよく理解することができます。

* 警察はサイバー犯罪者を捕まえるのが悪い。 国はインターネット上の不正行為を阻止するのに悪いです。

* 人や保険会社にとって信頼できる評判とフィードバックが必要です。

* 弁護士や弁護士、引受人はコンピュータプログラミングのコードがよくない。

"Cyber Insurance [is] 'held back' by lack of data". Ralph (Financial Times). 2017.

"Insurers tap cyber security ratings to limit liabilities". Kuchler (Financial Times). 2017.

ADVANTAGES VS DISADVANTAGES

- Credit history immediately available
- Contracts publicly enforced -> good faith
- Large-scale incident data available for risk-modelling
- Efficent competition between insurance products (as consumers compare for cheap)
- Unambigious contract defintions as given by the code executed.
- Trends of cyber threat easy to follow
- Data on insurance fraud publicly available

- Cedant anonymity depends on hiding the link between yourself (or your business) with the public key.
- Underlying currency (e.g. ether) highly volotile.
- For non-anonymous entities such as insurers, state law-makers, judges, some kind of Certificate Authority and Public Key Infrastructure will be needed, which may weaken trust in the technology
- Regulatory enforcement of frauds, bad-faith or credit failure historically poor in cyberspace
- Requires an intricate reputation and scoring system for honestly of clients.
- If client profile is not publicly known, insurers will need to conduct invasive checks before offering them a product (although this is the case anyway)
- Solicitors are not software designers or programmers

例。 クライアントまたは企業は、公開識別番号を持っています。 彼らの本名を知っている唯一の人々は、彼らが伝えたい人です。

* 会社に関する情報は、さまざまな事実の短いコードで提供することができます。

* 業種コード（"保健医療 - 私立 - 小"）

* この申請者が申請した以前の保険契約は、一般に公開されています。

* 国（「フランス」）

* 犯罪または詐欺の履歴は、保険会社または警察によって報告され、誰にでも伝えられます。

* 信用履歴と支払い履歴も公開されています。

* 会社の規模に関する情報、または他の情報を書くことができます。 より多くの情報があれば、より安い保険契約契約を購入することになります。

EXAMPLE: PUBLIC DATA ON A CLIENT. EACH PROPERTY CAN BE CODIFIED AND ASSOCIATED WITH A VARIABLE SCORE/CATEGORY

* Industry code for business (e.g. Healthcare-Dental-Private)
* Previous insurance policies applied-for: approved/denied
* Size of business (turnover, profit history, staff nubmers)
* Legal domestication (e.g. France)
* Criminal or fraud history
* Credit history
* Business model
* History of Mergers and Aquisitions
* .....

聞いてくれてありがとう

Many thanks!

~*Gregory Fenn*　グレゴリー・フェン

Gregory.Fenn.2014@rhul.ac.uk

REFERENCES :: 引用。 関連文献

- “Modeling Fundamentals: So You Want to Issue a Cat Bond?”. AIR (report). 2016.
- “On the limits of cyber-insurance”. Böhme and Gaurav. 2006.
- “Modeling Cyber-Insurance: Towards a Unifying Framework”. Böhme and Schwartz et al. 2010.
- “Cyber Insurance [is] ’held back’ by lack of data”. Ralph (Financial Times). 201.
- “The complexity of estimating systematic risk in networks”. Johnson, Laszka and Grossklags. 2014
- “Insurers tap cyber security ratings to limit liabilities”. Kuchler (Financial Times). 2017.
- “A modified epidemiological model for computer viruses”. Piqueria and Araujo. 2009.
- “Managing Cyber Insurance Accumulation Risk”. Cambridge Centre for Risk Studies. 2016.

SYSTEM COMPONENTS OF A BLOCKCHAIN CYBER-INSURANCE MARKET

Public :: Mixed :: Private