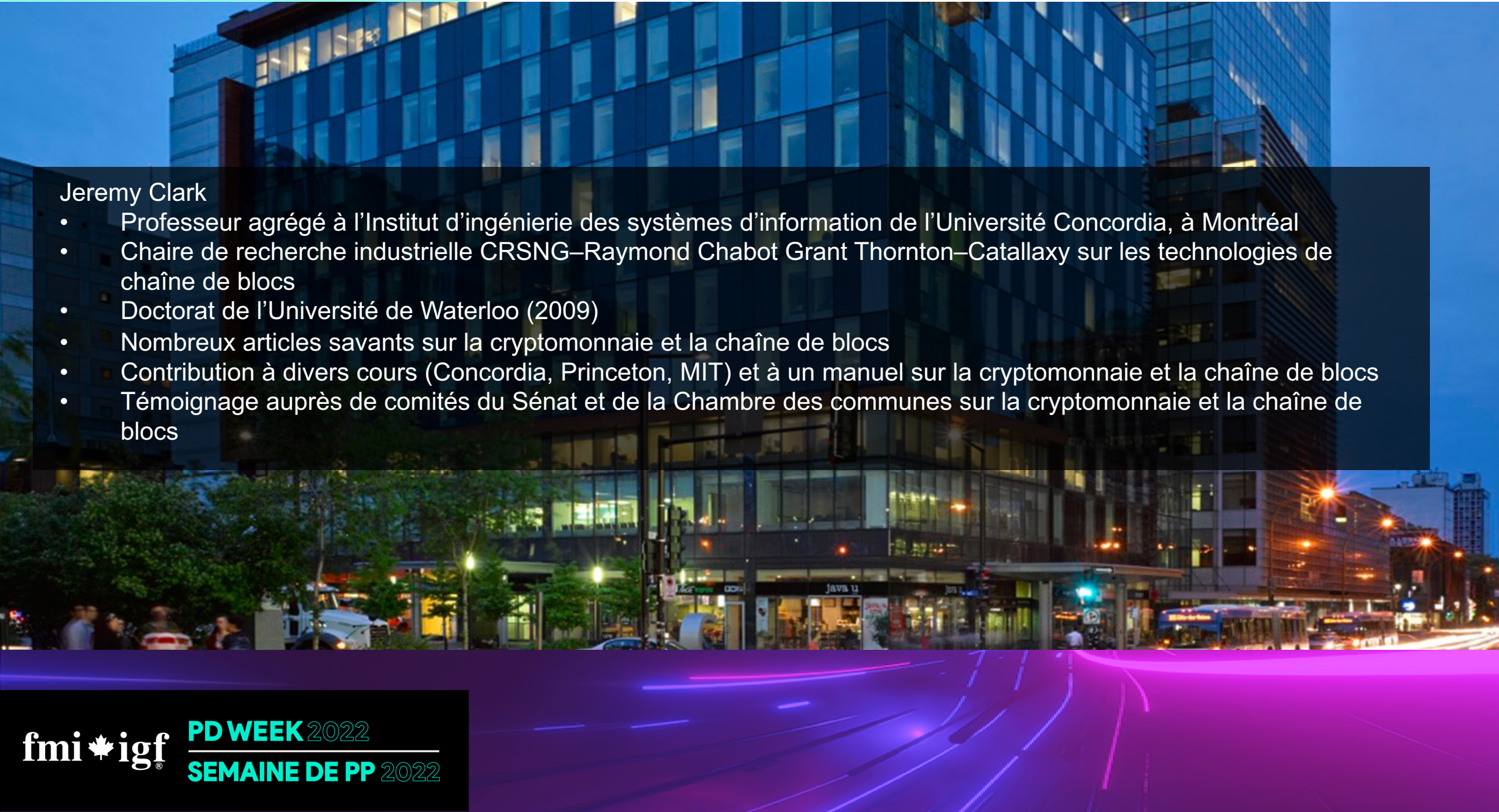
PD WEEK 2022

SEMAINE DE PP 2022

Chaîne de blocs et finance décentralisée

Paysage technologique et réglementaire



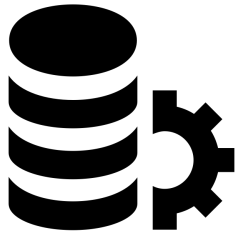
Jeremy Clark

- Professeur agrégé à l'Institut d'ingénierie des systèmes d'information de l'Université Concordia, à Montréal
- Chaire de recherche industrielle CRSNG–Raymond Chabot Grant Thornton–Catallaxy sur les technologies de chaîne de blocs
- Doctorat de l'Université de Waterloo (2009)
- Nombreux articles savants sur la cryptomonnaie et la chaîne de blocs
- Contribution à divers cours (Concordia, Princeton, MIT) et à un manuel sur la cryptomonnaie et la chaîne de blocs
- Témoignage auprès de comités du Sénat et de la Chambre des communes sur la cryptomonnaie et la chaîne de blocs

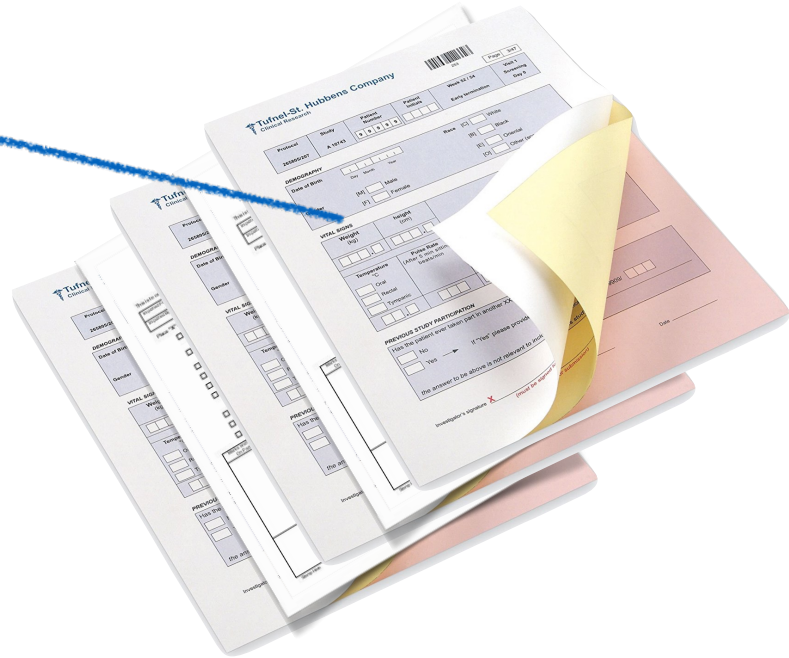
fmi igf

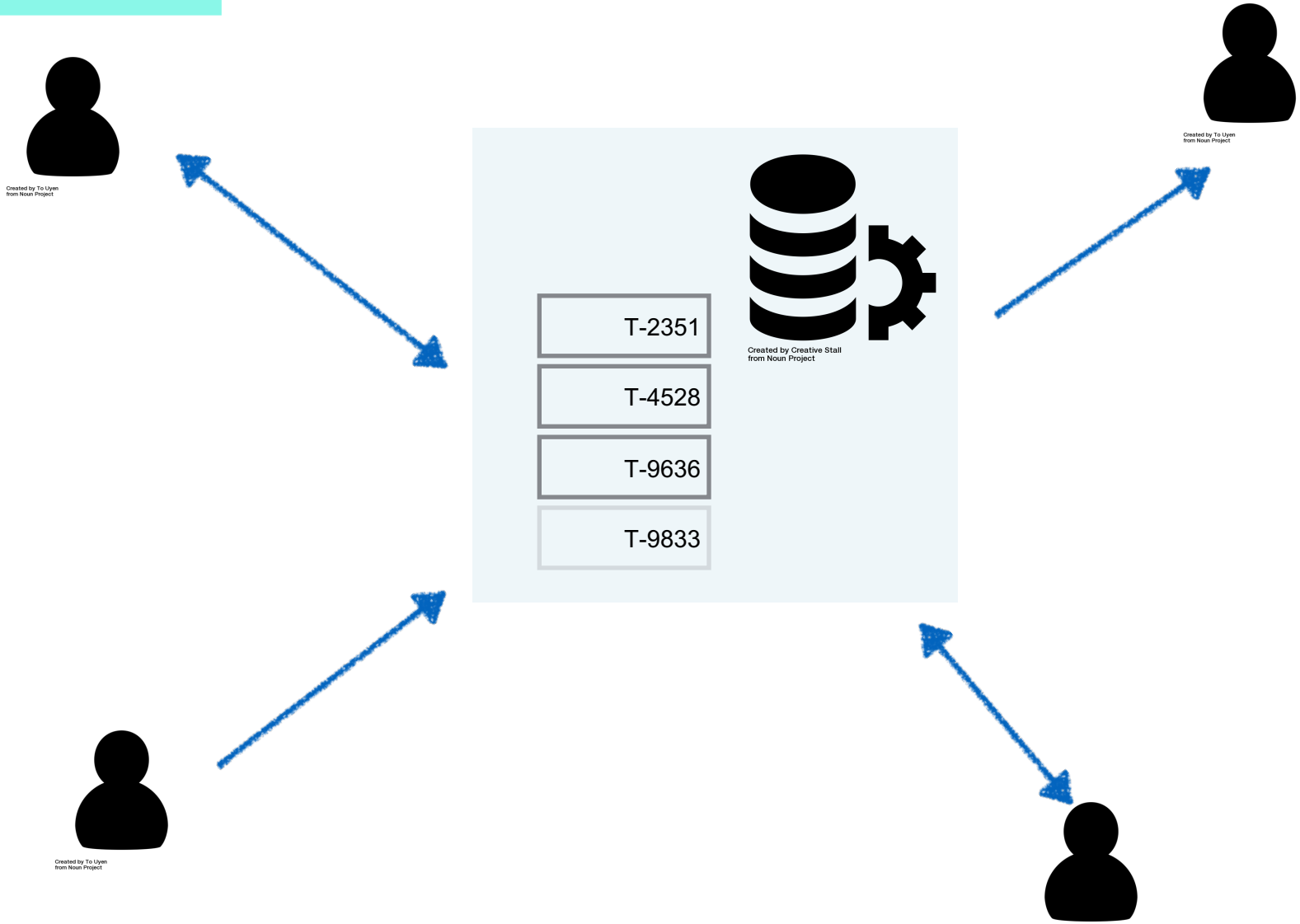
PD WEEK 2022

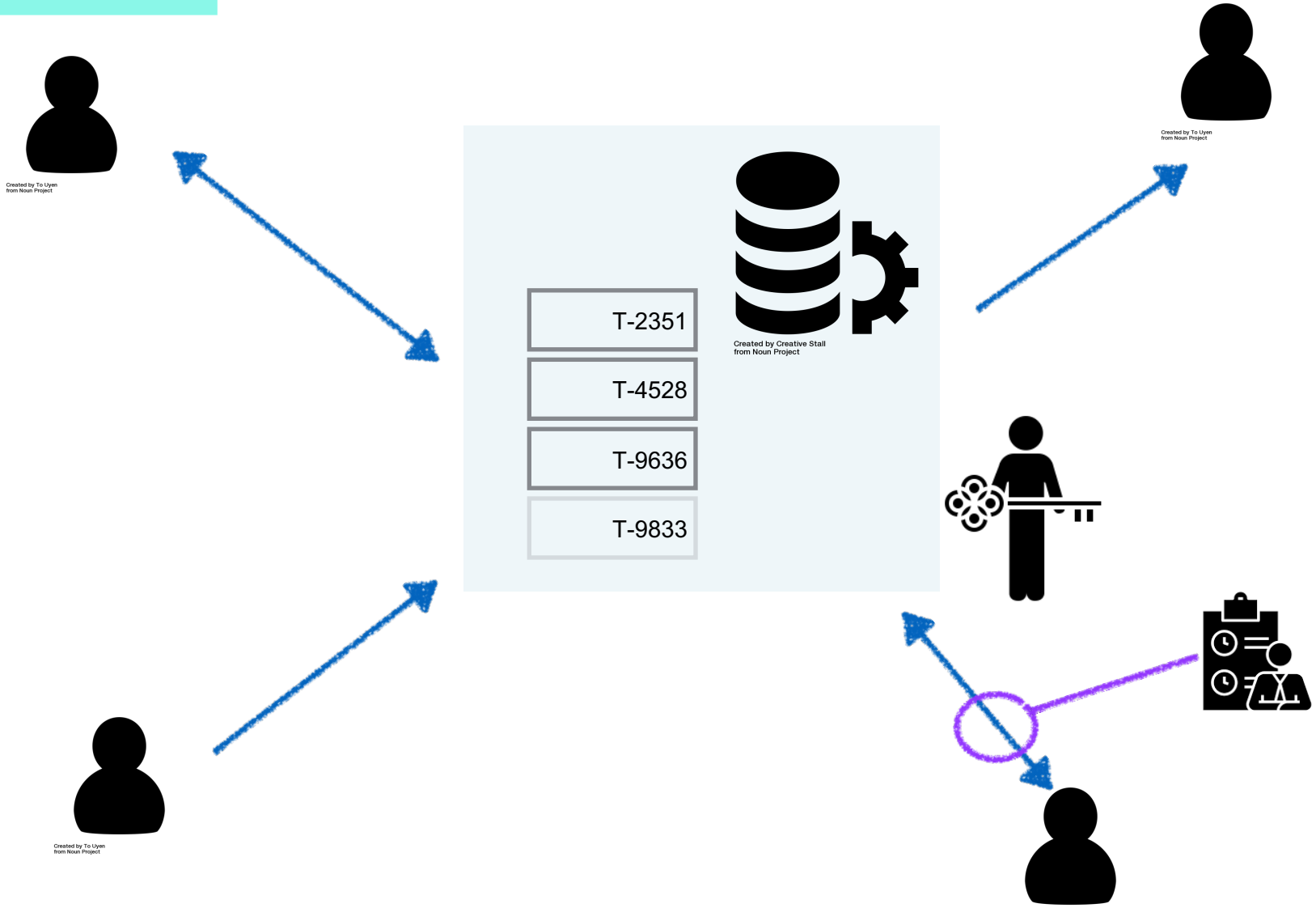
SEMAINE DE PP 2022



Created by Creative Stall
from Noun Project




Created by To Uyen
from Noun Project
Created by To Uyen
from Noun Project
T-2351
T-4528
T-9636
T-9833
Created by Creative Stall
from Noun Project
Created by To Uyen
from Noun Project
Created by To Uyen
from Noun Project
Created by To Uyen
from Noun Project


Created by To Uyen
from Noun Project
Created by To Uyen
from Noun Project
T-2351
T-4528
T-9636
T-9833
Created by Creative Stall
from Noun Project
Created by To Uyen
from Noun Project
Created by To Uyen
from Noun Project
Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

Created by Creative Stall
from Noun Project

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

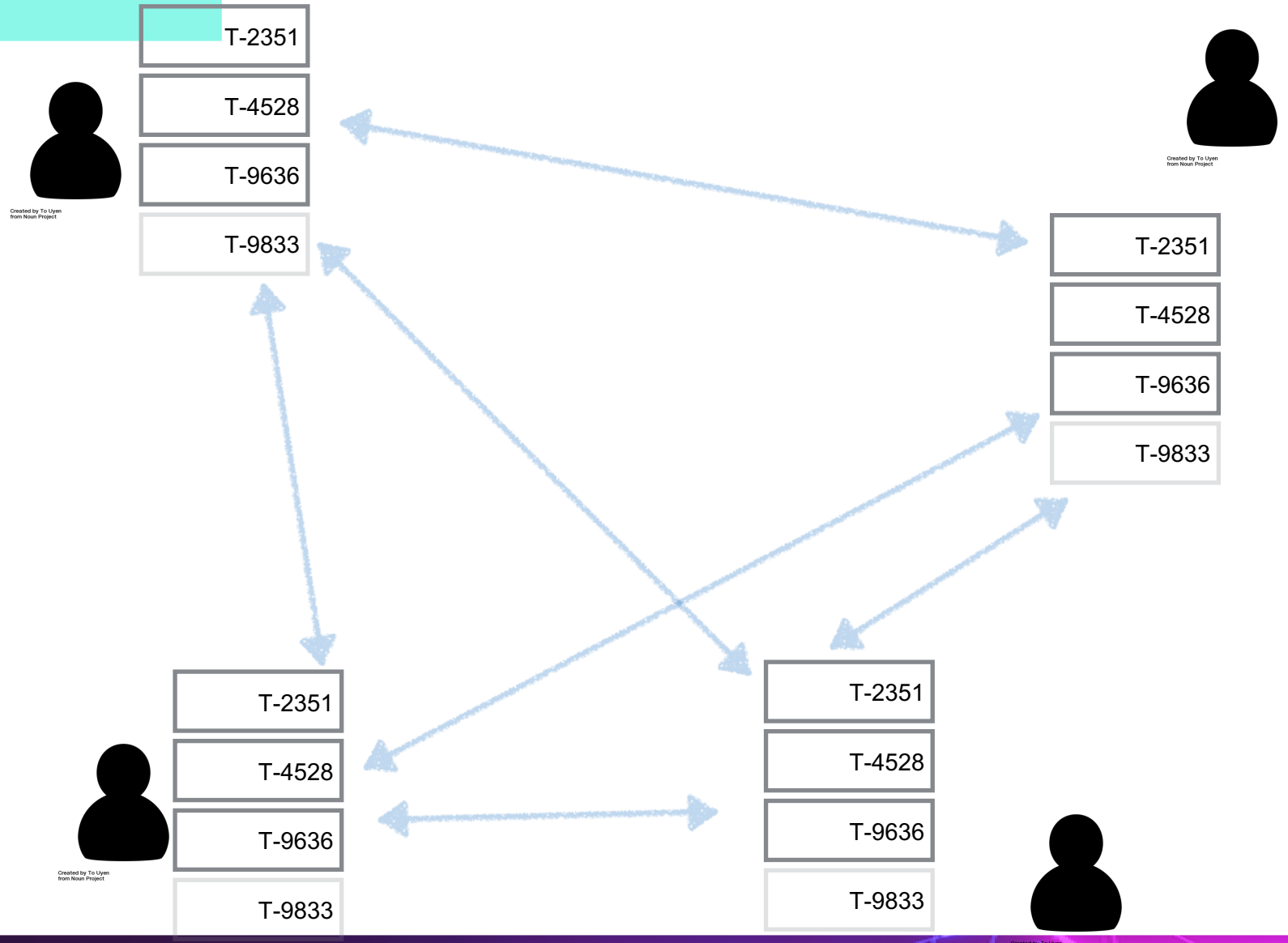
T-9833

Created by To Uyen
from Noun Project

fmi igf

PD WEEK 2022

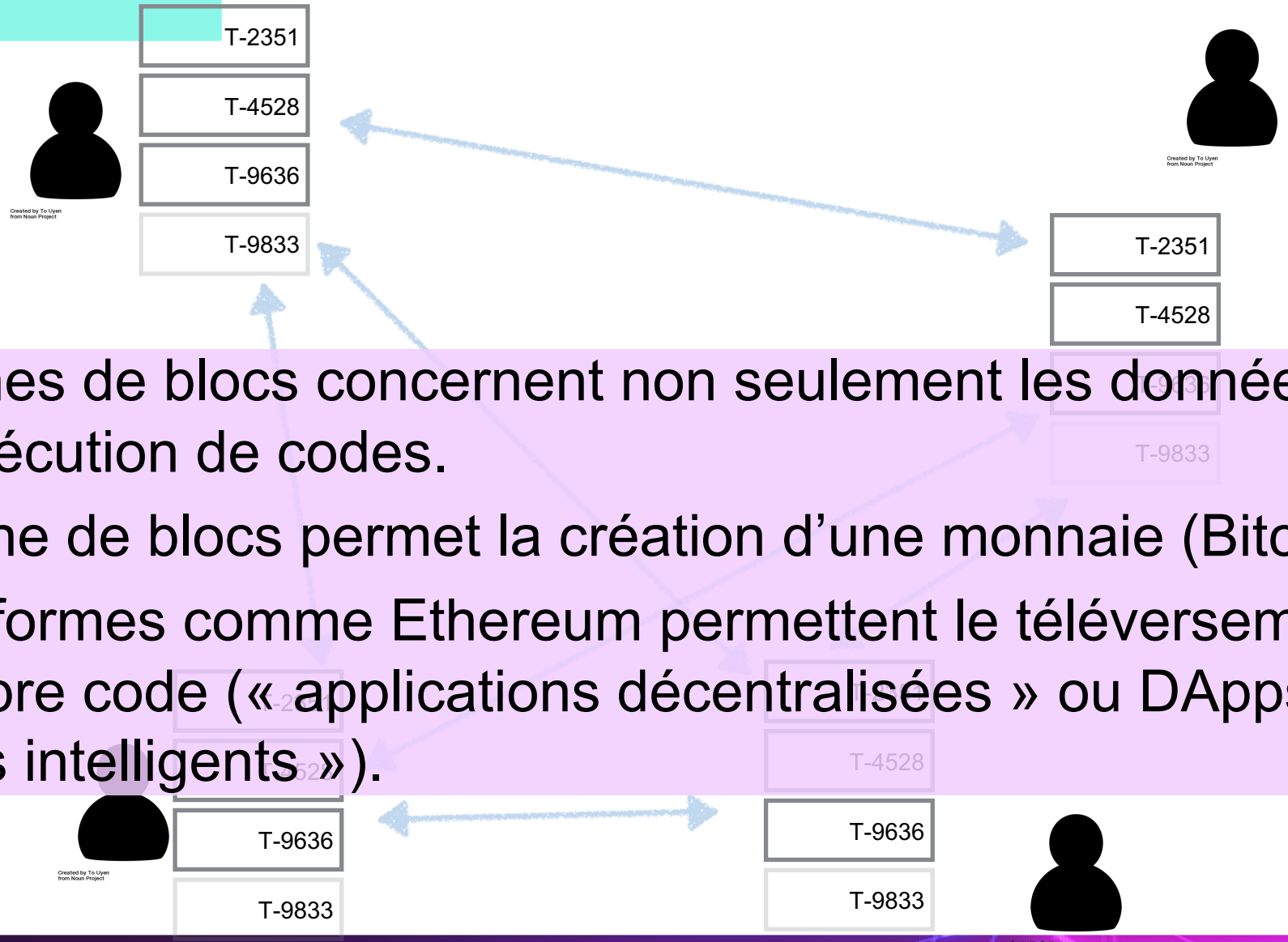
SEMAINE DE PP 2022



fmi igf

PD WEEK 2022

SEMAINE DE PP 2022



- Les chaînes de blocs concernent non seulement les données, mais aussi l'exécution de codes.
- Une chaîne de blocs permet la création d'une monnaie (Bitcoin).
- Les plateformes comme Ethereum permettent le téléversement de votre propre code (« applications décentralisées » ou DApps, ou « contrats intelligents »).

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

DealBook / Business & Policy

DEALBOOK NEWSLETTER

Why Bill Gates Is Worried About Bitcoin

It's all about the carbon footprint.

By Andrew Ross Sorkin, Jason Karaian, Michael J. de la Merced, Lauren Hirsch and Ephrat Livni

March 9, 2021

Sign Up

SIGN UP: *Want this in your inbox each morning?*

"Bitcoin uses more electricity per transaction than any other method known to mankind," Bill Gates noted. Yuri Gripas/Reuters

'It's not a great climate thing'

Bitcoin is continuing to climb — its price is now above $54,000, giving it a market cap of more than $1 trillion — and draw more fans in corporate America. But skeptics are increasingly asking

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

```
contract token {
       mapping  (addr
public coinBalanceOf;
       event CoinTran
sender, address rece:

function token (uint
       if supply (sup
10000;
       coinBalanceOf[
supply;
  }
}
```

signature 1
signature 2

```
contract token {
      mapping  (addr
public coinBalanceOf;
      event CoinTran
sender, address rece:

function token (uint
      if supply (sup
10000;
      coinBalanceOf[
supply;
  }
}
```

signature 1
signature 2

```
contract token {
      mapping  (addr
public coinBalanceOf;
      event CoinTran
sender, address rece:

function token (uint
      if supply (sup
10000;
      coinBalanceOf[
supply;
  }
}
```

signature 1
signature 2

```
contract token {
      mapping  (addr
public coinBalanceOf;
      event CoinTran
sender, address rece:

function token (uint
      if supply (sup
10000;
      coinBalanceOf[
supply;
  }
}
```

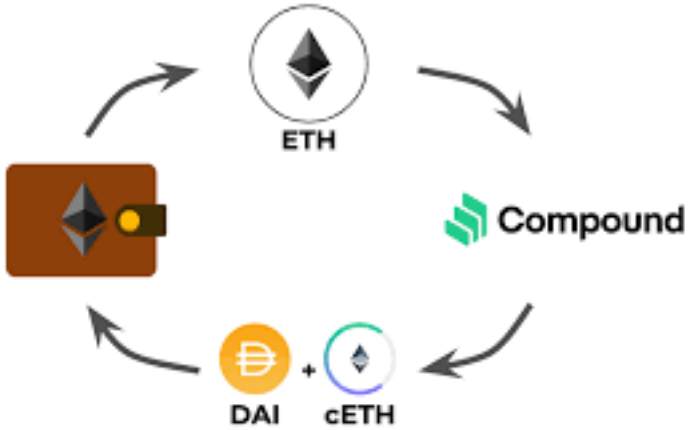
signature 1
signature 2

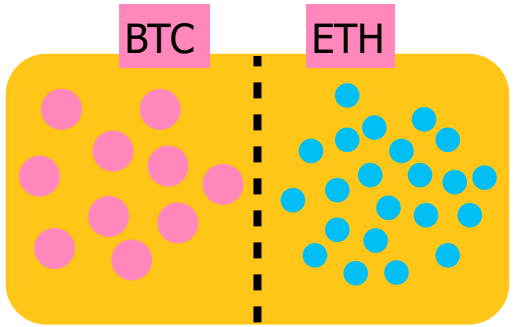
```
contract token {
      mapping  (addr
public coinBalanceOf;
      event CoinTran
sender, address rece:

function token (uint
      if supply (sup
10000;
      coinBalanceOf[
supply;
  }
}
```

signature 1
signature 2

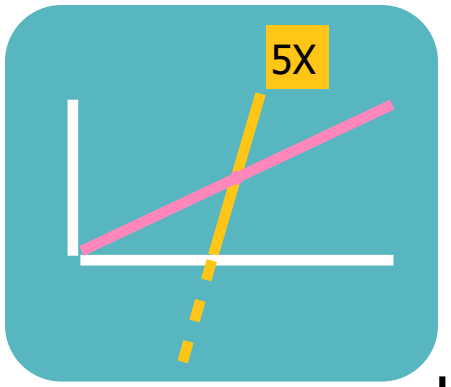
2022: $10B USD

Stablecoins





Uniswap



bZx

```
{

      TRANSACTION:

            RUN FUNCTION 1
            RUN FUNCTION 2
            RUN FUNCTION 3 => FAILS
            RUN FUNCTION 4

}
```

```
SKIP: 1, 2, 4
ABORT: 1, 2
REVERT: NONE
```

rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
5. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
6. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
7. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
8. **Wintermute - REKT 2** *N/A*
   $162,300,000 | 09/20/2022
9. **Compound - REKT** *Unaudited*
   $147,000,000 | 09/29/2021
10. **Vulcan Forged - REKT** *Unaudited*
    $140,000,000 | 12/13/2021
11. **Cream Finance - REKT 2** *Unaudited*
    $130,000,000 | 10/27/2021
12. **Badger - REKT** *Unaudited*
    $120,000,000 | 12/02/2021
13. **Mango Markets - REKT** *Out of Scope*
    $115,000,000 | 10/11/2022
14. **Harmony Bridge - REKT** *N/A*
    $100,000,000 | 06/23/2022
15. **Mirror Protocol - REKT** *Unaudited*
    $92,000,000 | 10/08/2021
16. **Fei Rari - REKT 2** *Unaudited*
    $80,000,000 | 05/01/2022
17. **Qubit Finance - REKT** *Unaudited*
    $80,000,000 | 01/28/2022
18. **Ascendex - REKT** *Unaudited*
    $77,700,000 | 12/12/2021
19. **EasyFi - REKT** *Unaudited*
    $59,000,000 | 04/19/2021
20. **Uranium Finance - REKT** *Unaudited*
    $57,200,000 | 04/28/2021
21. **bZx - REKT** *Unaudited*
    $55,000,000 | 11/05/2021
22. **Cashio - REKT** *Unaudited*
    $48,000,000 | 03/23/2022
23. **PancakeBunny - REKT** *Unaudited*
    $45,000,000 | 05/19/2021
24. **Kucoin - REKT** *Internal audit*
    $45,000,000 | 09/29/2020
25. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37,500,000 | 02/13/2021
26. **Vee Finance - REKT** *Slowmist, Certik*
    $34,000,000 | 09/21/2021
27. **Crypto.com - REKT** *Deloitte*
    $33,700,000 | 01/18/2022
28. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32,000,000 | 03/04/2021
29. **MonoX - REKT** *Halborn, Peckshield*
    $31,400,000 | 11/30/2021
30. **Spartan Protocol - REKT** *Certik*
    $30,500,000 | 05/02/2021

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

FINTRAC
CANAFE

fmi igf

PD WEEK 2022

SEMAINE DE PP 2022

FINTRAC
CANAFE

AUTORITÉ
DES MARCHÉS
FINANCIERS

fmi igf

PD WEEK 2022
SEMAINE DE PP 2022

FINTRAC
CANAFE

AUTORITÉ
DES MARCHÉS
FINANCIERS

Canada Revenue Agency
Agence du revenu du Canada

fmi igf

PD WEEK 2022
SEMAINE DE PP 2022

FINTRAC
CANAFE

AUTORITÉ
DES MARCHÉS
FINANCIERS

Canada Revenue Agency
Agence du revenu du Canada

cpab ccrc
Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes

fmi igf

PD WEEK 2022
SEMAINE DE PP 2022

Bitcoin & Blockchain Technology

INSE 6630: Recent Developments in Information Systems Security (Fall 2018)

Blended course with online lectures

Classroom for occasional meetings: Wednesdays, 14:45, FG B40

- Instructor: Jeremy Clark
- Office Hours: Drop in on Thursdays 13:00 - 15:00 in EV 9.177
- Marker: Shayan Eskandari

Course Outline

The offical course outline is available here.

Prerequisites

This course has no formal prerequisites. It will involve a little cryptography, which will be taught as if you have not taken 611 little programming of short smart contracts (10s of lines of code). Students from Quality or other departments welcome.

Textbook

The lectures are based, in part, on the following textbook. It is not required but may be useful for further reading. Exams and assignments will be based on what is presented during the lectures, with the textbooks providing additional detail and formaliza

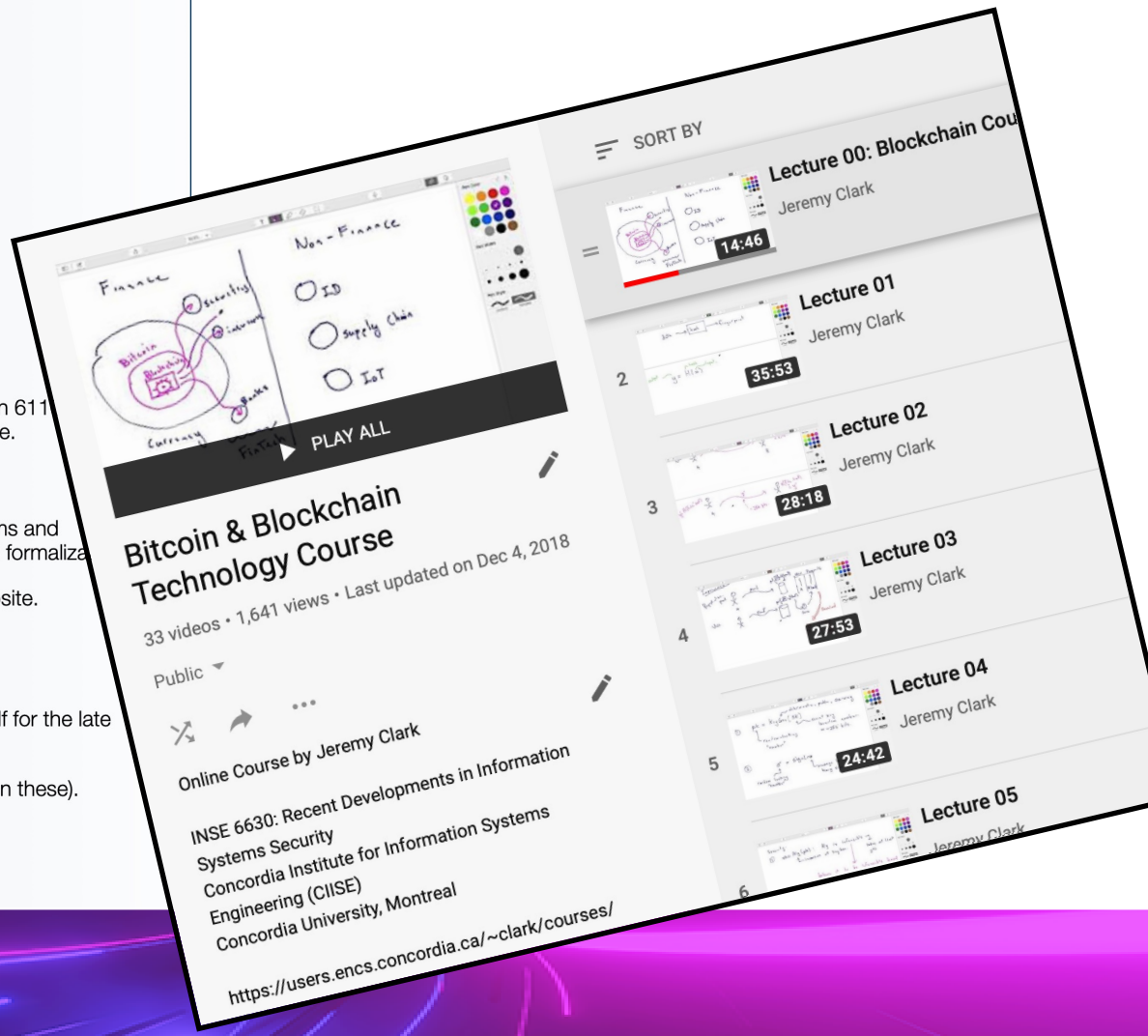
- Bitcoin and Cryptocurrency Technology (Narayanan et al): Free pre-print (as PDF) is available from the book website. Hardcopies are available in the Concordia bookstore or from Amazon

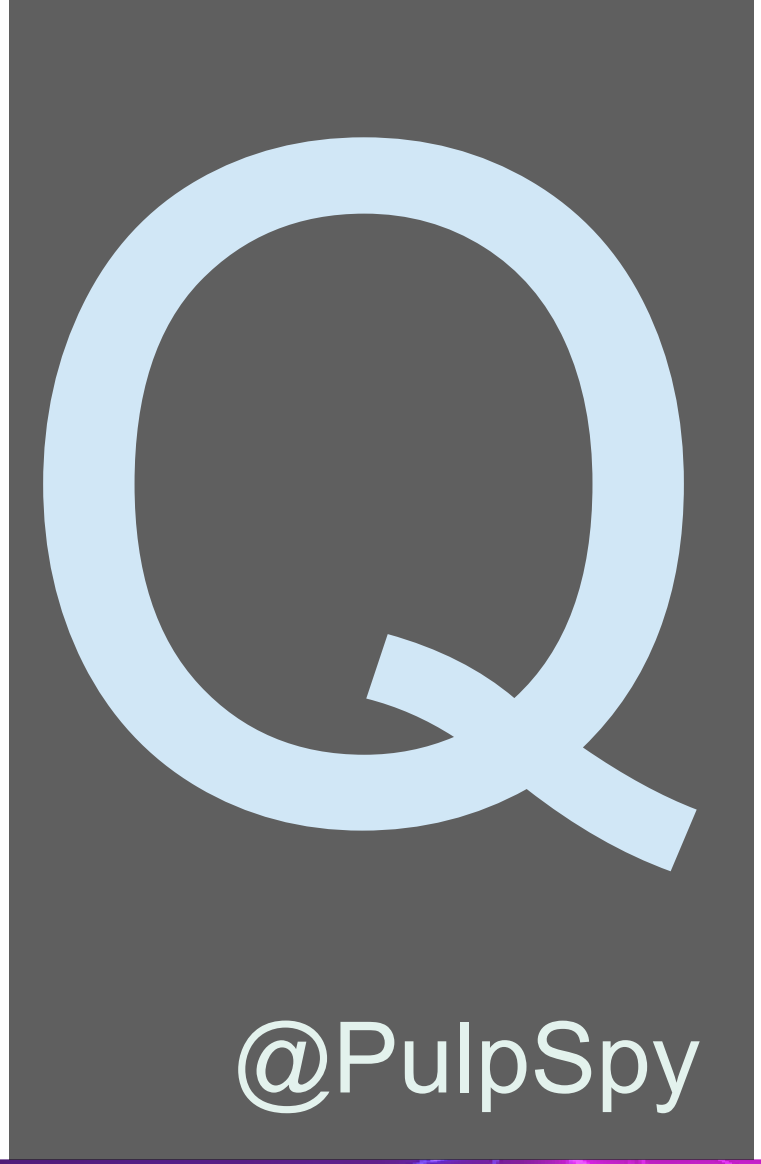
Assignments and Exams

Assignments are due by the end of class on the due date. They are to be submitted via EAS. See the assignment itself for the late policy.

A previous midterm exam and final exam are available. Note the questions will be completely different (not variations on these).

- **Midterm Test (15%):** Oct 24 (in class)
- **Assignment 1 (5%):** Due Oct 10 (by end of class) [A1]
- **Assignment 2 (5%):** Due ~~Nov 18~~ Nov 28 (by end of class) [A2, Tutorial]





fmi igf

PD WEEK 2022

SEMAINE DE PP 2022