

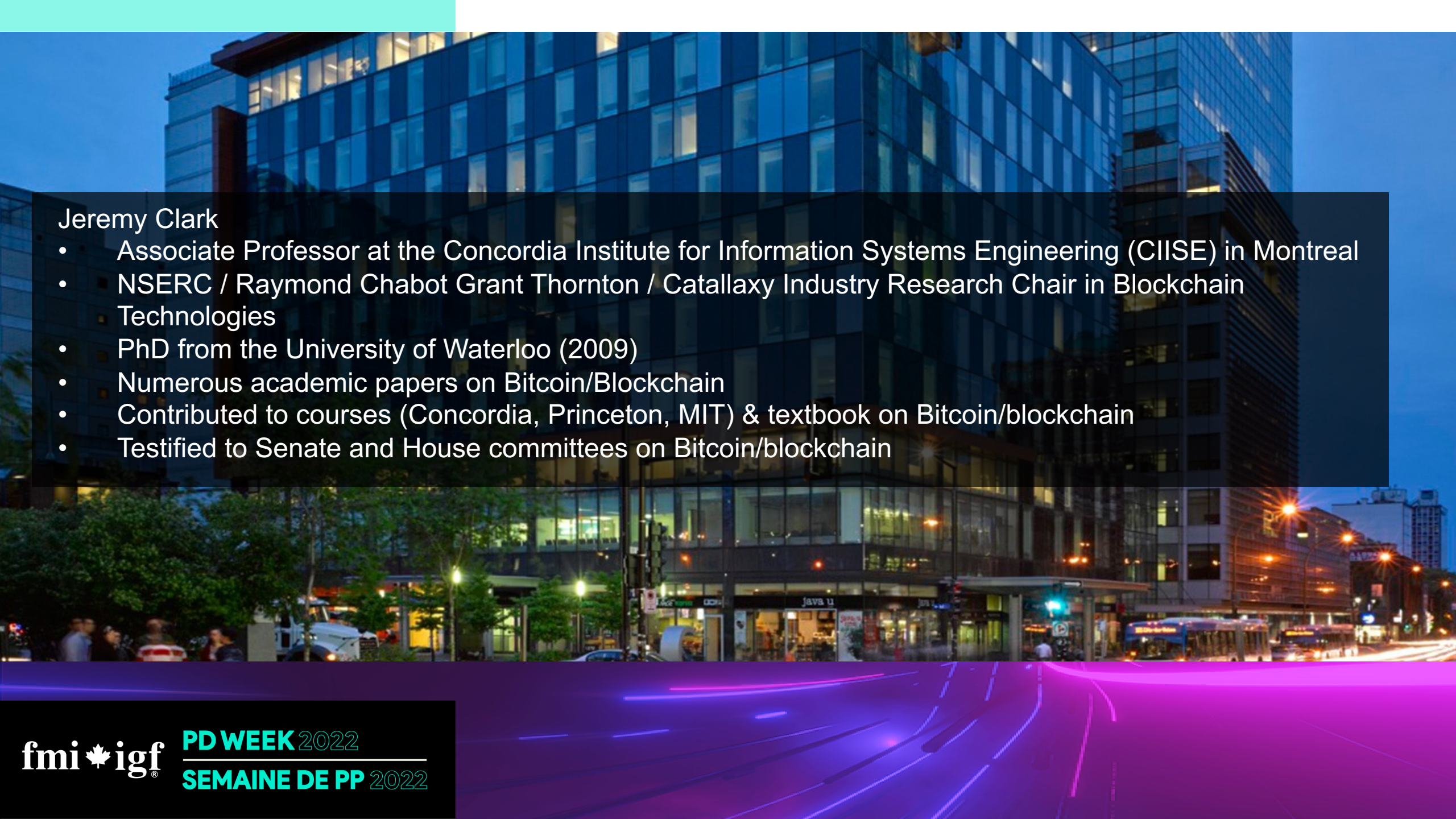


PD WEEK 2022

SEMAINE DE PP 2022

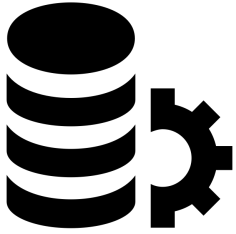
Blockchain and Decentralized Finance

Technological and Regulatory Landscape

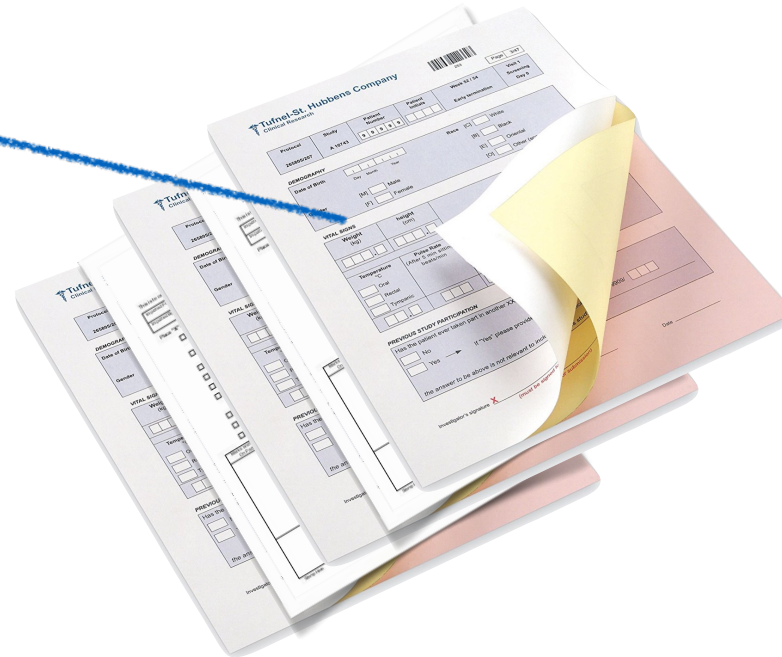


Jeremy Clark

- Associate Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- NSERC / Raymond Chabot Grant Thornton / Catallaxy Industry Research Chair in Blockchain Technologies
- PhD from the University of Waterloo (2009)
- Numerous academic papers on Bitcoin/Blockchain
- Contributed to courses (Concordia, Princeton, MIT) & textbook on Bitcoin/blockchain
- Testified to Senate and House committees on Bitcoin/blockchain

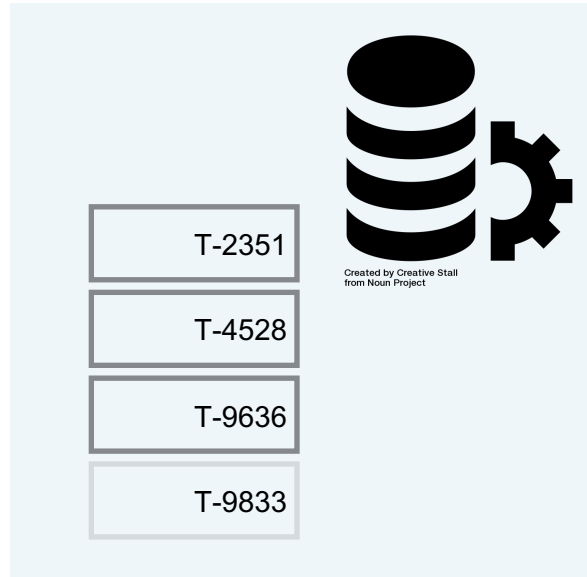
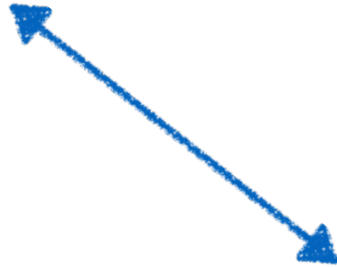


Created by Creative Stall
from Noun Project

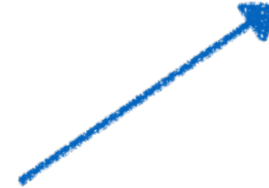




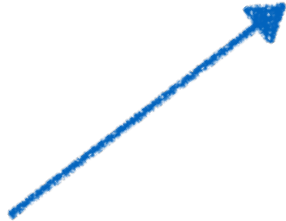
Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project



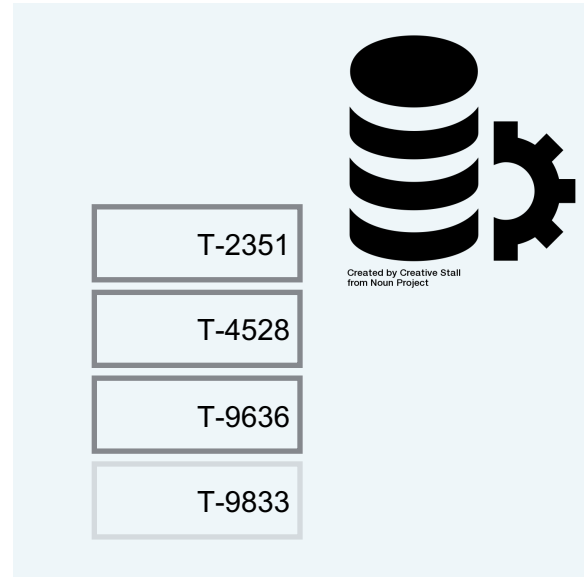
Created by To Uyen
from Noun Project



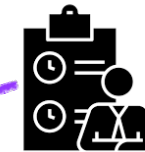
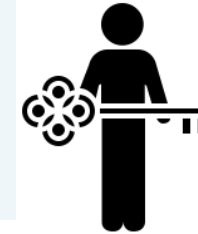
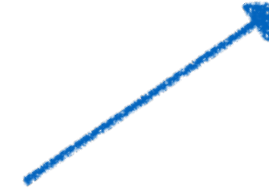
Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project



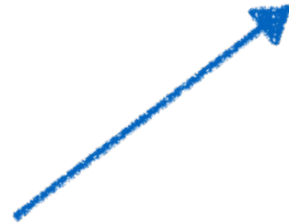
Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project





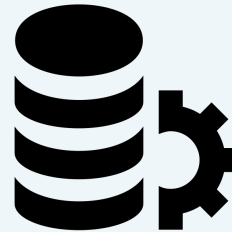
Created by To Uyen
from Noun Project

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



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



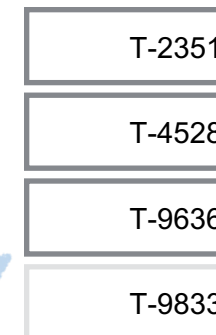
Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project



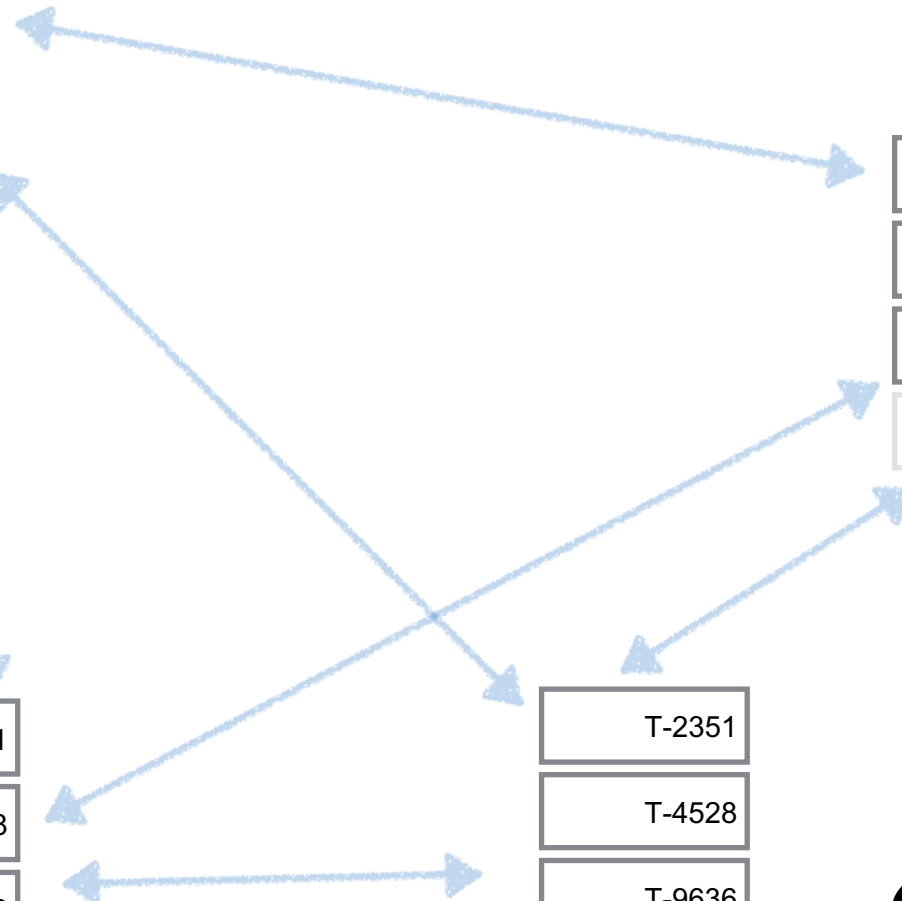
Created by To Uyen
from Noun Project

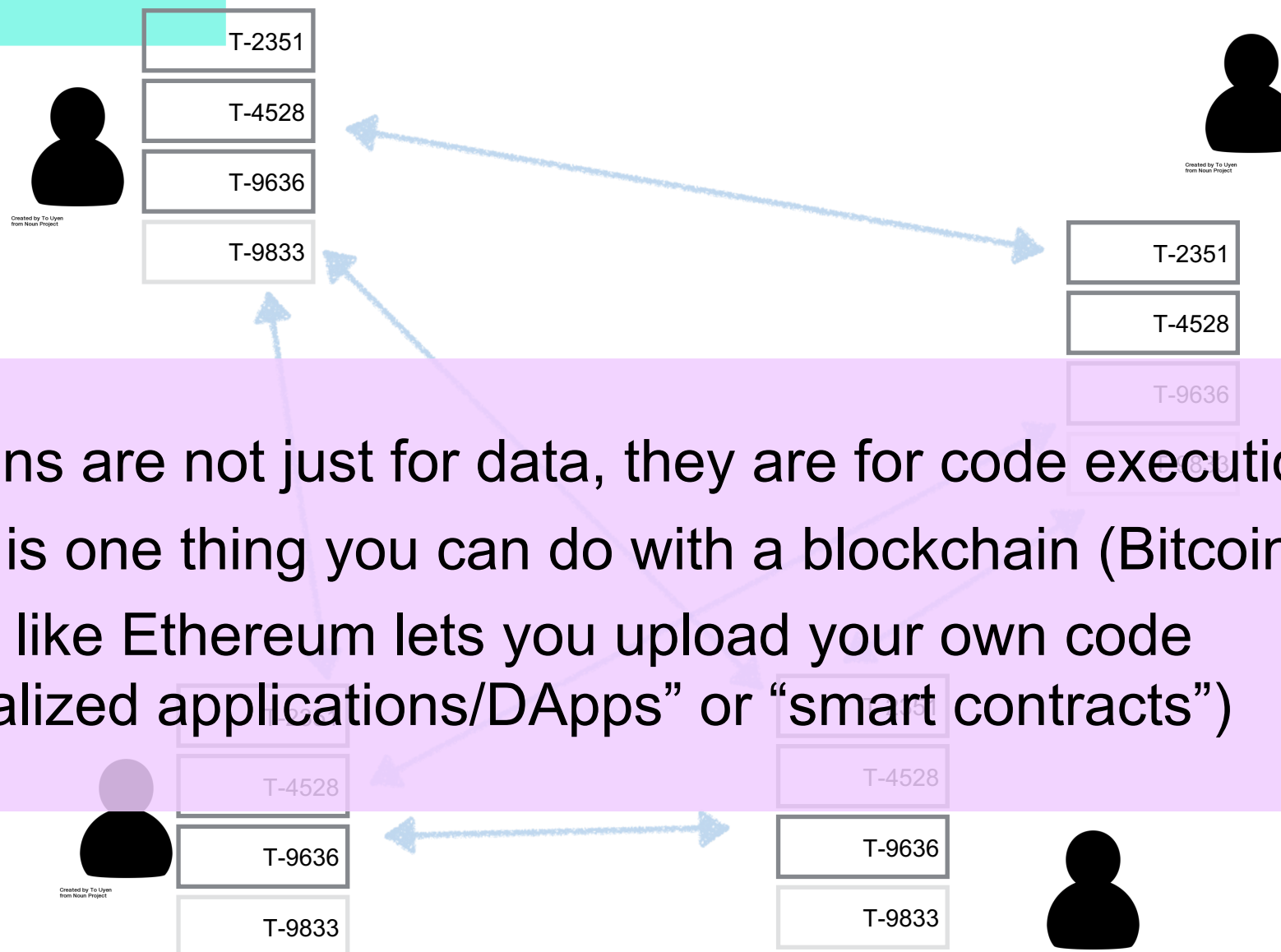


Created by To Uyen
from Noun Project



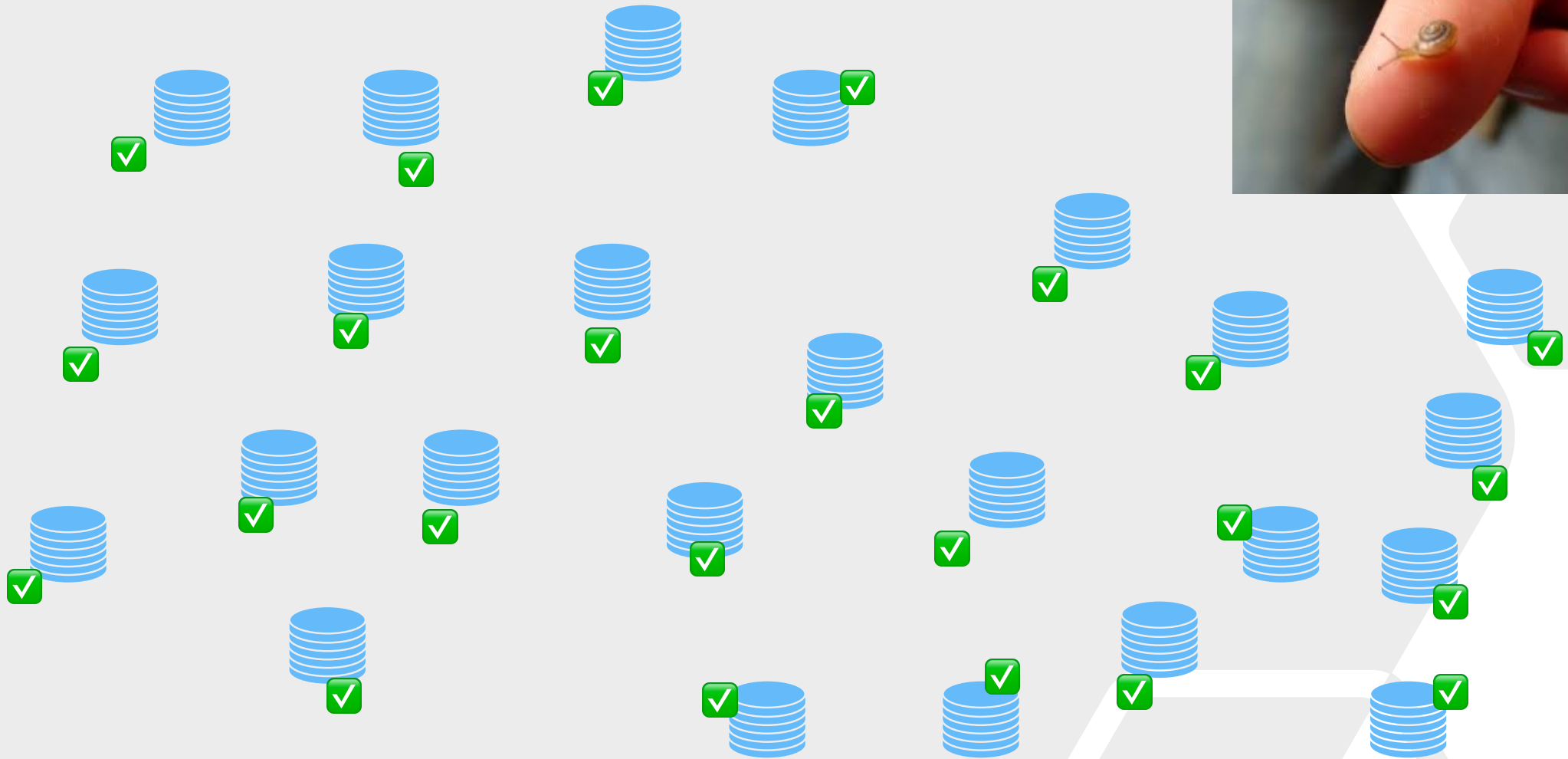
Created by To Uyen
from Noun Project





- Blockchains are not just for data, they are for code execution
- Currency is one thing you can do with a blockchain (Bitcoin)
- Platforms like Ethereum lets you upload your own code (“decentralized applications/DApps” or “smart contracts”)





Why Bill Gates Is Worried About Bitcoin

It's all about the carbon footprint.

f w t e r b

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

March 9, 2021

Sign Up

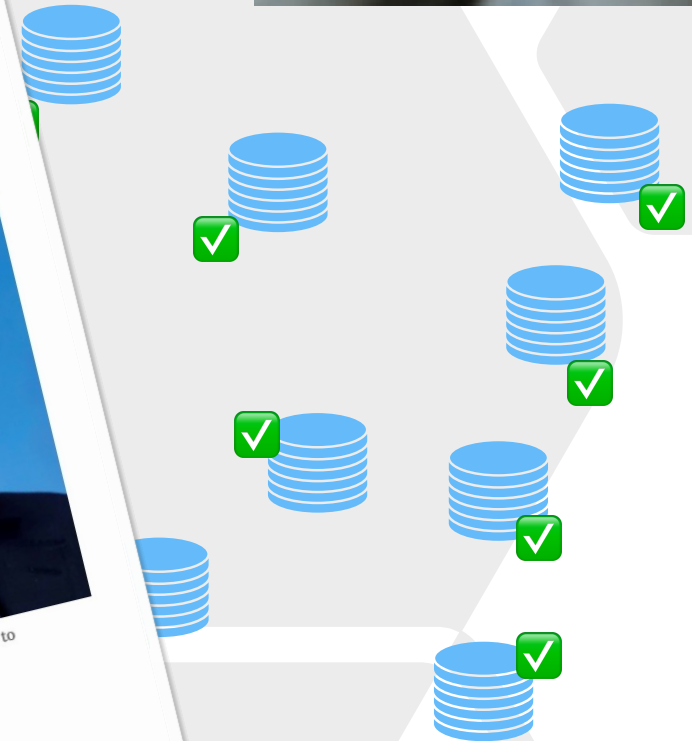
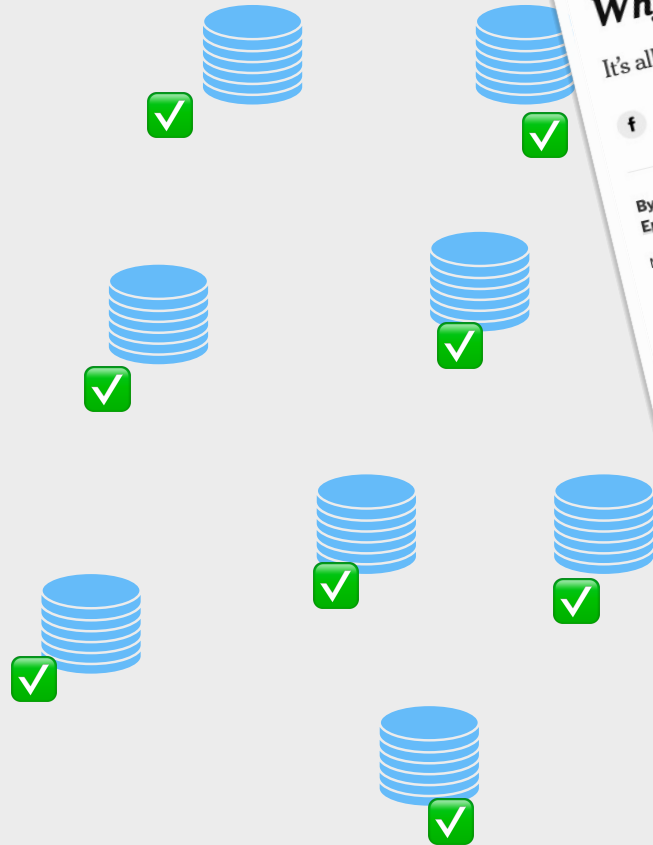
SIGN UP: Want this in your inbox each morning?



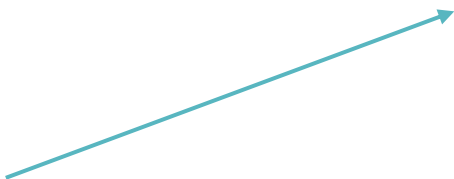
"Bitcoin uses more electricity per transaction than any other method known to mankind," Bill Gates noted. Yuri Gripas/Reuters

'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







```
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

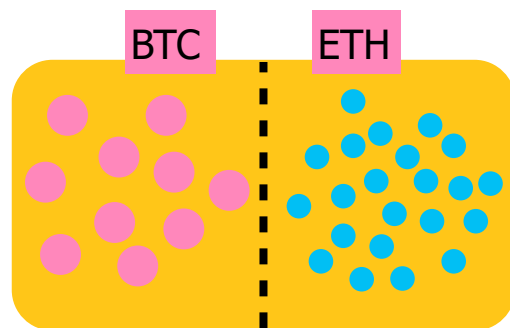
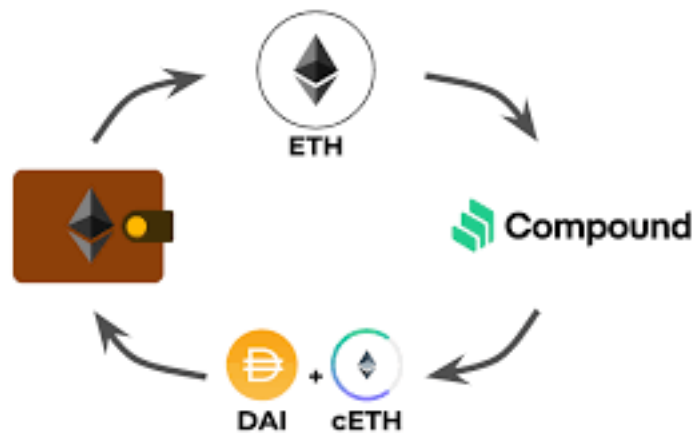


2022: \$10B USD

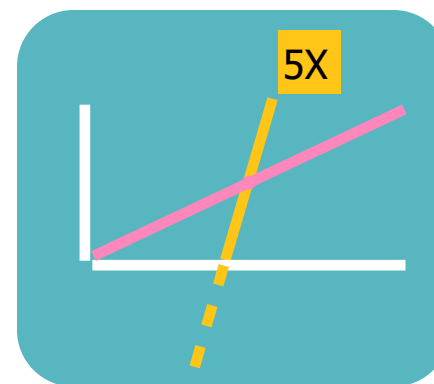




Stablecoins



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

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



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

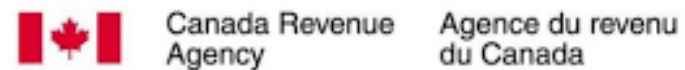


Canada Revenue
Agency

Agence du revenu
du Canada

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 official 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 formalization.

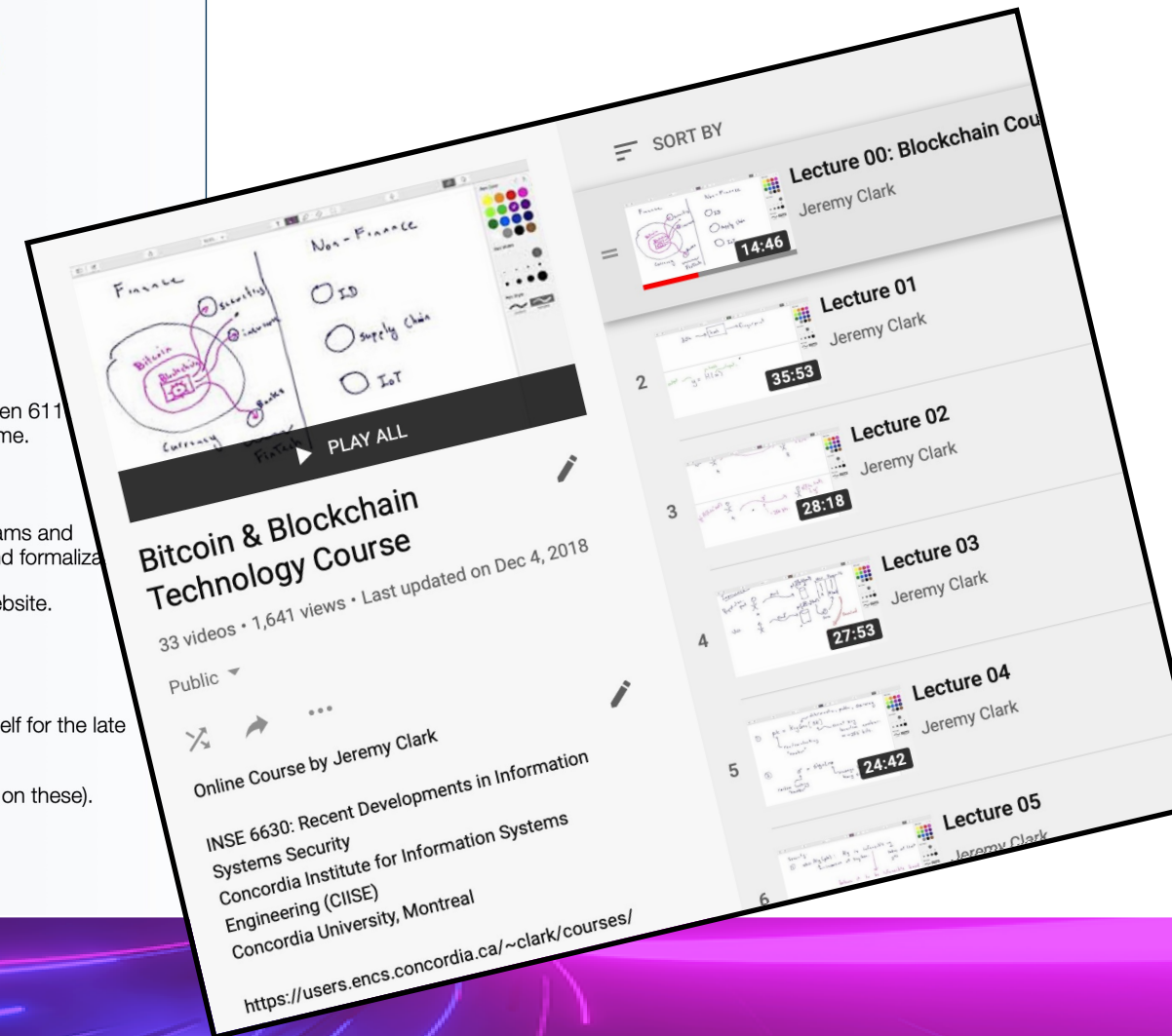
- [Bitcoin and Cryptocurrency Technology \(Narayanan et al\)](#): Free pre-print (as PDF) is available from the book website. Hardcopies are available in the Concordia bookstore or from Amazon

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](#)]





Q

@PulpSpy