UNIVERSITY OF TRENTO

Complexity, Cryptography, and Financial Technologies

Lecture 1 – Introduction

Fabio Massacci

UNIVERSITY OF TRENTO

- **Lecturer**
  - Fabio MASSACCI
  - Office hours: by appointment in class
- **Instructor**
  - Chan Nam NGO
  - Office hours by appointment via email
  - Name.Surname@disi.unitn.it

What is FinTech

UNIVERSITY OF TRENTO

- **FinTech = a buzzword to describe novel technologies adopted by financial service institution**
  - internet & mobile payments
    - Digital signature for e-banking (MPS in 1998, by 2004 only 4 banks in Italy, Monte dei Paschi di Siena, Intesa, San Paolo, Banca di Roma)
    - M-Pesa by Safaricom in Kenya and Vodacom in Tanzania launched in 2007. Airtime as a proxy for cash. Now the de facto P2P small payments system in the countries.
  - Crowd-funding and lending,
    - Zopa started in the UK in 2004 as peer-to-peer lending, Lending Club in 2006. In 2016 Lending Club CEO Laplanche was forced to step down after some internal scam, basically sold a loan to himself (company had 1/5 of its value since initial OPA in 2014).
  - Capital market and trading
  - Insurance services (InsureTech)
  - Wealth management (Robo-advisor)
- **Most recentely cryptograph-based financial servics**
  - Blockchain, cryptocurrencies, smart contracts, initial coin offerings
  - Several other application (invoice factoring, trading etc.)
  - very popular BUT most people, including CS professionals, have no clue

Learning Outcomes

UNIVERSITY OF TRENTO

- **Technical Abilities: you should be able to**
  - Identify key security characteristics of a crypto-based FinTech problem;
  - Organize/integrate algorithms and information needed for solution;
  - Compare methods and tools and choose the ones most suited;
  - Apply methods to a complex industrial scenario
- **Soft Skills: you should be able to**
  - present solutions and perform a code review
- **Overall → have a clue on Crypto-FinTech**
  - whether a proposal is actually working or just packaged snake oil
  - and be able to read the fine prints

Course Content

UNIVERSITY OF TRENTO

- **Introduction to Crypto-based FinTech:**
  - Fintech Characteristics, Bitcoin as an example, Distributed systems overview
- **Complexity:**
  - Introduction to computing relations, P vs NP (search and decision problems), One-way functions, Interactive proofs, Zero knowledge proofs, Introduction to Multi-Party Computations
- **Cryptography**
  - Finite Field (Discrete Log, Quadratic Residuosity), recap of Digital Signatures, Elliptic Curves Digital Signature Algorithm, Quadratic Arithmetic Programs
- **Advanced Topics**
  - Pairing-based zk-SNARKS, Multy-party computation based on Garbled Circuits, Secret Sharing
- **Labs will be done for libraries implementing the above features**
  - Hyperledger (Java), libsnark (C), SPDZ (Python)
- **FinTech Case Studies in partnership with EIT Companies**
- **Students Presentations**
  - Proposal for FinTech case study 1, Hostile review for FinTech case study 1

Pre-requisites

UNIVERSITY OF TRENTO

- **General CS Knowledge**
  - Should be obvious but…
  - Algorithms and complexity notation
  - Computer networks
  - Programming skills in Java, C, Python
- **Introductory Security Knowledge**
  - Basics of Computer and Network Security
  - OR Basics of Cryptographic Algorithms
- **Useful but not needed**
  - Security testing, network security, etc.
  - Advanced computability and complexity theory
  - Advanced cryptographic techniques (discrete maths etc.)

Why we do need all that stuff?

UNIVERSITY OF TRENTO

- **So that you should be able to understand…**
- **What are the goals industry wants**
  - Guranteeing value of transactions (integrity)
  - Protecting confidentiality of one's assets (confidentiality)
  - Leaving no trace behind (zero-knowledge and anonymity)
- **What can (or cannot) be digitally achieved by**
  - Using unpredictables values (randomness)
  - Leveraging hard to invert constructions (computational complexity)
- **What can actually be digitally implemented by**
  - mathematical functions (cryptography)
    - We "use" them, don't study them →Elliptic Curves and Cryptography
  - distributed implementations (consensus)
    - We "use" them, don't study them → Distributed Systems II

Course Principles

UNIVERSITY OF TRENTO

- **Lectures**
  - Point to key issues, important steps in proofs
  - not every detail of the lectures is in the slides.
  - They are the START of your study (and not the end)
- **Active Exercises**
  - Students try to answer questions at home and submit results at scheduled date
  - Students submit results after each lab
  - (Some) students present it in class on that date
  - Instructor/professor discuss solution and mark submitted papers
- **Reading Material**
  - chapter at the basis of each argument is indicated
  - you don't get it? try the additional reading material maybe the same concept is expressed in way that you find more palatable
  - Proficiency based on understanding, not rote-learning

Cognitive Levels: why the course is tough

UNIVERSITY OF TRENTO

- **Knowledge**
  - Recall things by memory (eg repeat a proof from a book)
- **Comprehension ← Most theory course stops here**
  - Justify methods and procedures
- **Application ← Most design courses stops here**
  - Apply concepts and principles to new situations
- **Analysis**
  - Understanding relationships between parts (content & structure)
- **Synthesis ← The best should arrive here**
  - Ability to put parts together to form a new whole
- **Evaluation**
  - Conscious ability to judge the value of material

Grading

UNIVERSITY OF TRENTO

- **General participation**
  - Participation and submission of lab materials → 7 points
  - Midterm theory evaluation→ 8 points
  - Presentations on the UNBIAS case study → 4 points
- **Case study development**
  - Participation, lab materials, and final implementation of UNBIAS→ 8 points
  - Participation, lab materials, and final implementation of IOP → 8 points
    - OPTIONAL: alternative to IOP a fully interoperable UNBIAS solution
- **No Copy Cat**
  - If you are not able to present/defend your solution you get a negative grade
- **Your grade will be essentially determined during the course**
  - This approach is common in the USA and rare for Italian courses
  - EXPECTATION: 100% of active students will pass by end of January
  - DISCLAIMER: no warranty either implicit or explicit that your grade will be high

What students think of it

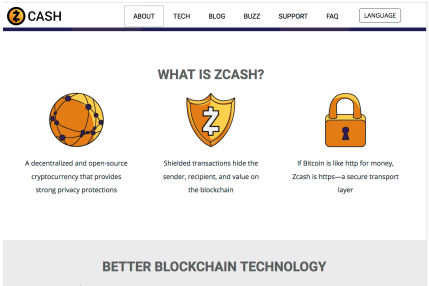
UNIVERSITY OF TRENTO

- **This course is new so we have no history**
- **So we take another example: ICT Innovation**
  - Students forced to take it: 50% satisfied
  - Students who choose to take it: 92% satisfied
- **Since your grade will be determined during the course**
  - You will be able to realize how you are doing
  - Empirical scientific research on education tells that students realizing they are doing badly will say they are not satisfied (it is rational behavior after all)
    - B. Uttl et al. Meta-analysis of faculty's teaching effectiveness: Student evaluation of teaching ratings and student learning are not related, *Studies in Educational Evaluation* 54 (2017) (http://www.sciencedirect.com/science/article/pii/S0191491X16300323)
    - M. Braga et al. Evaluating students' evaluations of professors, *Economics of Education Review* 41 (2014) (http://www.sciencedirect.com/science/article/pii/S0272775714000417)
- **Still, if you think something should be fixed → speak during the course**
  - I did it myself several times when student and don't bear grudges
  - Don't wait for the Course Evaluation → you can still give us a poor evaluation (see above) but at least we can fix it for your course

Crypto Currencies

UNIVERSITY OF TRENTO

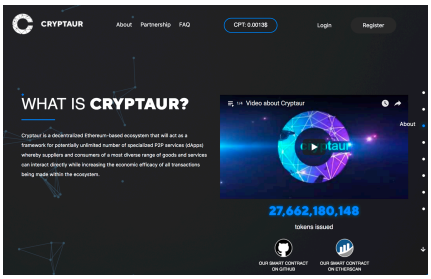
- ***Zcash* is**
  - "the first open, permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography."
  - Motto: "We created Zcash, but its ultimate destiny lies not in our hands, but in yours."
  - https://z.cash/
- **Explicit crypto ceremony to make it secure**
  - https://youtu.be/D6dY-3x3teM



Initial Coin Offerings

UNIVERSITY OF TRENTO

- ***Cryptaur* is**
  - "a decentralized Ethereum-based ecosystem that will act as a framework for potentially unlimited number of specialized P2P services…"
  - Motto: "Bye bye middleman"
  - https://cryptaur.com/
- **Explicit business case to make it viable**
  - https://youtu.be/l2lQAZRRJ1E



Why…

UNIVERSITY OF TRENTO

- **Questions**
  - Why do we need complexity and cryptography?

  And
  - can't you just teach blockchains?
- **Answers**
  - Because otherwise you'll have no clue of what you are doing

  and
  - The first passer by can sell you a blockchain-based, privacy preserving machine learning quantum computer

  and
  - you'll get a toaster for the price of a nuclear reactor
- **Ultimate goal is giving you a "security mindset"**

Let's start with a very simple FinTech

UNIVERSITY OF TRENTO

- **We want to adjudicate a coin toss**
  - Head I win, Tail you lose
- **Physical Toss has several important properties**
  - Cannot be guessed
  - Cannot be duplicated
  - Cannot be run in parallel
  - Cannot be affected by order of execution
- **Digital Toss requires a protocol**

The Digital Coin Toss

UNIVERSITY OF TRENTO

- **Alice**
  - Selects randomly a number x
  - Send x to Bob
  - Receive y from Bob
- **Bob**
  - Selects randomly a number y
  - Send y to Alice
  - Receive x from Alice
- **Adjudication**
  - IF x ***xor*** y =1 THEN Alice wins ELSE Bob wins
- **Communication is asynchronous**
  - Messages can be received in any order.
- **What can go wrong?**

The Digital Coin Toss + 1-way Function

UNIVERSITY OF TRENTO

- **Suppose h is a 1-way function: easy to compute but hard to invert**
  - There is a relation H = { (x,h_x) … } s.t.
    - given x it is easy to find an h_x such that (x,h_x) is in H
    - given h it is hard to find x_h such that (x_h,h) is in H
- **Alice**
  - Selects randomly a number x
  - Send h(x) to Bob
  - Receive h(y) from Bob
  - Send x to Bob
- **Bob**
  - Selects randomly a number y
  - Send h(y) to Alice
  - Receive h(x) from Alice
  - Send y to Alice
- **Adjudication**
  - IF x ***xor*** y =1 THEN Alice wins ELSE Bob wins

The Digital Coin Toss + 1-way Function (II)

UNIVERSITY OF TRENTO

The Protocol

- **Suppose h is a1-way function**
- **Alice**
  - Selects randomly a number x
  - Send h(x) to Bob
  - Receive h(y) from Bob
  - Send x to Bob
- **Bob**
  - Selects randomly a number y
  - Send h(y) to Alice
  - Receive h(x) from Alice
  - Send y to Alice
- **Adjudication**
  - IF x ***xor*** y =1 THEN Alice wins ELSE Bob wins

Cheating possibilities

- **Alice can**
  - wait for Bob h_{Bob}
  - Try all possible values y until she finds $h(y)=h_{Bob}$
  - Try all possible values x until she finds a x s.t.
    - x ***xor*** y =1
  - Send h(x) and then continue as normal
- **Alice can**
  - Try all possible values x, x' until she found a pair s.t.
    - x ***xor*** x' =1 and h(x)=h(x')
  - Send h(x)
  - Wait for y_{Bob}
  - IF x ***xor*** y=1
    - THEN send x
    - ELSE send x'

The Digital Coin Toss + 1-way Function + Random

UNIVERSITY OF TRENTO

- **Suppose h is a function that is easy to compute but hard to invert**
  - There is a relation H = { (x,h_x) … } s.t.
    - given x it is easy to find an h_x such that (x,h_x) is in H
    - given h it is hard to find x_h such that (x_h,h) is in H
- **Alice**
  - Selects randomly a number x and a number r_x in $(0,1)^n$
  - Send $h(x,r_x)$ to Bob
  - Receive $h(y,r_y)$ from Bob
  - Send x,r_x to Bob
- **Bob**
  - Selects randomly a number y and a number r_y in $(0,1)^n$
  - Send $h(y,r_y)$ to Alice
  - Receive $h(x,r_x)$ from Alice
  - Send y,r_y to Alice
- **Adjudication**
  - IF x ***xor*** y =1 THEN Alice wins ELSE Bob wins
- **What still needs to be fixed?**

The Digital Coin Toss + 1-Way Function + Random (IV)

UNIVERSITY OF TRENTO

Protocol

- **Suppose h is a 1-way function**
- **Alice**
  - Selects randomly a number x and a number r_x in $(0,1)^n$
  - Send $h(x,r_x)$ to Bob
  - Receive $h(y,r_y)$ from Bob
  - Send x,r_x to Bob
- **Bob**
  - Selects randomly a number y and a number r_y in $(0,1)^n$
  - Send $h(y,r_y)$ to Alice
  - Receive $h(x,r_x)$ from Alice
  - Send y,r_y to Alice
- **Adjudication**
  - IF x ***xor*** y =1 THEN Alice wins ELSE Bob wins

Cheating

- **Collision is still partly unsolved**
  - We have fixed only one problem of collision
  - Not yet the problem of Alice doing a pre-calculation of values that collides
- **Bob is a machine, not a human**
  - he can toss several (millions) coins with the Alices of the world → can we use this information to guess the next toss?
  - If Bob generate millions of tosses, for various Alices → needs to be "hard on average" not just "hard on the worst case"
  - We have not really made sure that Bob is talking to Alice → can Alice launch millions of parallel coin tosses extracting some information?
- **What if**
  - Alice desn't want to reveal x to Bob but just show that she has lost
    - For example showing her financial portfolio has been under/over performing the index without disclosing her portfolio

Some things are easier said than done...

UNIVERSITY OF TRENTO

- **Being easy to compute and hard to invert is not so trivial**
  - Hard to find a collision ex post
  - Hard to find in advance a pair that collides
  - Hard on average when several queries can be made
  - Hard to find results when a honest guy can be used as an oracle
- **There are also other issues**
  - Generate random numbers
  - Implementation details
- **More Sophisticated properties**
  - Committing to a value without ever showing it
- **Understanding details makes a difference**

Zcash – The Ceremony - Revisited

UNIVERSITY OF TRENTO

- **Protocol**
  - Six participants were chosen and each was tasked with generating one shard of the public/private key set.
  - Once the public/private pair shards were complete the six combined their public key shards to generate the public parameters of Zcash, and then each destroys their shard of the private key.
- **Organizational Security**
  - These six were geographically dispersed, and were also unknown to each other prior to the conclusion of The Ceremony
  - […] only brand new computers are used. Bought exclusively for the purpose of The Ceremony, these machines are never connected to any network, and the wifi and Bluetooth cards are physically removed
- **Evidence protection**
  - A secure hash chain of all messages was compiled and has been posted to Twitter […].
  - For example, all the details of The Ceremony, including when it would occur, who was participating, and the source code, were kept secret until it was completed.
- **Continue reading for the un-initiated**
  - https://www.coinbureau.com/education/zcash-ceremony/

Zcash – The Ceremony – Revisited (II)

UNIVERSITY OF TRENTO

Crypto Movies and Authenticity

- **The protocol**
  - Six participants were chosen and each was tasked with generating one shard of the public/private key set.
  - Once the public/private pair shards were complete the six combined their public key shards to generate the public parameters of Zcash, and then each destroys their shard of the private key.
- **Organizational Security**
  - These six were geographically dispersed, and were also unknown to each other prior to the conclusion of The Ceremony
  - only brand new computers are used. Bought exclusively for the purpose of The Ceremony, these machines are never connected to any network, and the wifi and Bluetooth cards are physically removed
- **Evidence protection**
  - A secure hash chain of all messages was compiled and has been posted to Twitter (below) and to the Internet Archive as well as being time-stamped into the Bitcoin blockchain.
  - For example, all the details of The Ceremony, including when it would occur, who was participating, and the source code, were kept secret until it was completed.
- **Reading for the un-initiated**
  - https://www.coinbureau.com/education/zcash-ceremony/

Sex Movies and Authenticity

- **What you see is *never* what happens**
  - You very rarely see the actual naked body of the main (typically female) character, you only see a "body double"
  - Same for all (typically male) heros doing all their stunts. It is a "stuntman".
  - Even in most porn movies, sex is mostly simulated
- **Why's that?**
  - 1minute video takes hours to shoot from different angles under strong lights
    - you can't have two persons going continuously on real sex for hours without exhaustion
    - You don't want to keep an expensive member of staff naked for several hours nor risk breaking his/her neck
  - Video Software can fix it for you
- **But what you see looks ok and the same applies to crypto…**

Zcash - The Ceremony – Revisited (III)

UNIVERSITY OF TRENTO

- **Did they burned the computer they used?**
  - There's the video..
- **How have they put the shards together**
  - if they didn't know each other?
- **How do we know they used the code that they claimed to have used?**
  - They posted all hashes on twitter and published the code
- **How many of those people mentioned in The Ceremony**
  - hold shares or a controlling interest of "Zcash Electronic Co."?
  - hold Zcash Coins?

Zcash - The Ceremony – Revisited (III)

UNIVERSITY OF TRENTO

- **They actually burned the computer they used**
  - There's the video..
- **How have they put the shards together**
  - if they didn't know each other?
- **How do we know they used the code that they claimed to have used?**
  - They posted all hashes on twitter and published the code
- **How many of those people mentioned in The Ceremony**
  - hold shares or a controlling interest of "Zcash Electronic Co."?
  - hold Zcash Coins?
- **There is a video that they burned some computer**
  - Remember the sex movies…
- **Somebody picked them…**
  - and by chance it was the head of the company
- **They posted some code and some hashes on the internet**
  - Nobody can't read the original input of the original computers (as they have been aptly destroyed)
  - So all hashes, twitter messages, code etc. are meaningless
- **They never told us…**
  - Which is normally the only relevant question in "normal" due diligence proceedings

Initial Coin Offering – A Century Ago, in California

UNIVERSITY OF TRENTO

Republic Mill and Mining

Greenwater Furnace Creek Copper

Initial Coin Offering Aren't a Modern Invention (II)

UNIVERSITY OF TRENTO

- **Greenwater Furnace Creek Copper Co.**
  - Furnace Creek is a town in the Greenwater Mining District, in Inyo County, California.
  - Company incorporated in Arizona in 1906
  - Stock advertised and sold but, alas, no mine existed.
- **You can try to buy these historical certificates at**
  - http://www.oldwesthistorystore.com/california_page.htm

Gold Rush vs Coin Offering

UNIVERSITY OF TRENTO

- **Geological surveys and mine plans**
  - If you can't read them, how do you know there is really gold there?
- **Registration not on official land registry**
  - You can't possibly enforce it…
- **Money Transfer to Western Union Address**
  - This is a donation...
- **Paper Share Certificate**
  - This is a line in a notebook and not traded on the stock market so only valid if company honors it

Gold Rush vs Coin Offering

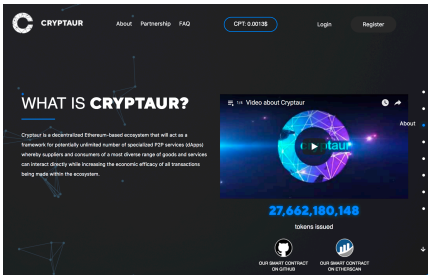
UNIVERSITY OF TRENTO

- **Geological surveys and mine plans**
  - If you can't read it, how do you know there is really gold there
- **Registration not on official land registry**
  - Same here…
- **Money Transfer to Western Union Address**
  - This is also a donation...
- **Paper Letter with share certificates**
  - This is a line in a notebook and not traded on the stock market so only valid if company honors it
- **Crypto Smart Contracts on Github**
  - If you can't read it, how do you know this is working code?
- **Contract not on the BTC/ETH blockchain**
  - You can't possibly enforce it
- **Crypto-transfer to a BTC address**
  - This is a donation…
- **Web account with "Coin Number"**
  - This is row in a SQL database and not a public key for BTC so only valid if web server honors it

Initial Coin Offerings - Revisited

UNIVERSITY OF TRENTO

- ***Cryptaur* is**
  - "a decentralized Ethereum-based ecosystem that will act as a framework for potentially unlimited number of specialized P2P services…"
- **Question**
  - SD, phd student of this department, has a small company that wanted to sell its services to Cryptaur.
  - He invested 500US$, his fellow co-owner invested 5000US$ in Cryptaur Coin Offering
  - THEN he sought our advice
- **Exercise**
  - Gold Mine or Fools' Mine?



Course Material

UNIVERSITY OF TRENTO

- **Main Books on Theory**
  - Complexity and Cryptography: An Introduction. Book by DJA Welsh and J Talbot
  - Cryptography: An Introduction. Book by N Smart
  - Computational Complexity: A Conceptual Perspective. Book by O Goldreich.
- **Slides of the lectures**
  - Available on the web after the lectures.
  - Everything is Google Classroom and on the Wiki

Suggested Readings

UNIVERSITY OF TRENTO

- **All articles below are available free of charge from UNITN Network**
- **FinTech General Overview**
  - I Lee, YJ Shin, Fintech: Ecosystem, business models, investment decisions, and challenges, Business Horizons 61, 2018,
    - http://www.sciencedirect.com/science/article/pii/S0007681317301246
- **Some case studies for specific areas**
  - RJ. Kauffman, D Ma, Special issue: Contemporary research on payments and cards in the global fintech revolution, Electronic Commerce Research and Applicatione 14, 2015,
    - http://www.sciencedirect.com/science/article/pii/S1567422315000678
    - This is article just describes further articles, you should read it briefly and then pick the case study that seems most interesting for you
  - J Jagtiani, C Lemieux, Do fintech lenders penetrate areas that are underserved by traditional banks?, Journal of Economics and Business, 2018,
    - http://www.sciencedirect.com/science/article/pii/S0148619518300390
  - BS. Thompson, Can Financial Technology Innovate Benefit Distribution in Payments for Ecosystem Services and REDD+?, Ecological Economics 139, 2017,
    - http://www.sciencedirect.com/science/article/pii/S0921800917301295
  - TC Yan, P Schulte, D Lee, K Chuen, Chapter 11 - InsurTech and FinTech: Banking and Insurance Enablement, In Handbook of Blockchain, Digital Finance, and Inclusion, Academic Press, 2018
    - http://www.sciencedirect.com/science/article/pii/B9780128104415000117
- **Security and Privacy Requirements for general FinTech**
  - K Gai, M Qiu, X Sun, A survey on FinTech, J of Network and Computer Applications 103, 2018,
    - http://www.sciencedirect.com/science/article/pii/S1084804517303247
- **Important: none of this article is specifically about blockchain, etc. on purpose.**
  - So that you have an idea of the broader field of FinTech
  - AND you have an idea of the broad security, privacy and business issues