CS Undergraduate Research Opportunities

Information Page

- The page below provides information on various ways of participating in undergraduate research, and also a link to the past undergraduate senior thesis.

https://cs.georgetown.edu/undergraduate-research/

- Slides from 6 faculty presenters are included here
  - Ben Ujcich
  - Sasha Golovnev
  - Lisa Singh
  - Eric Burger
  - Shin'ichiro Matsuo
  - Nitin Vaidya
- Note that many other CS faculty are also interested in mentoring undergraduate researchers. Please visit the faculty webpages to find the faculty working in research areas of your interest.

Benjamin E. Ujcich

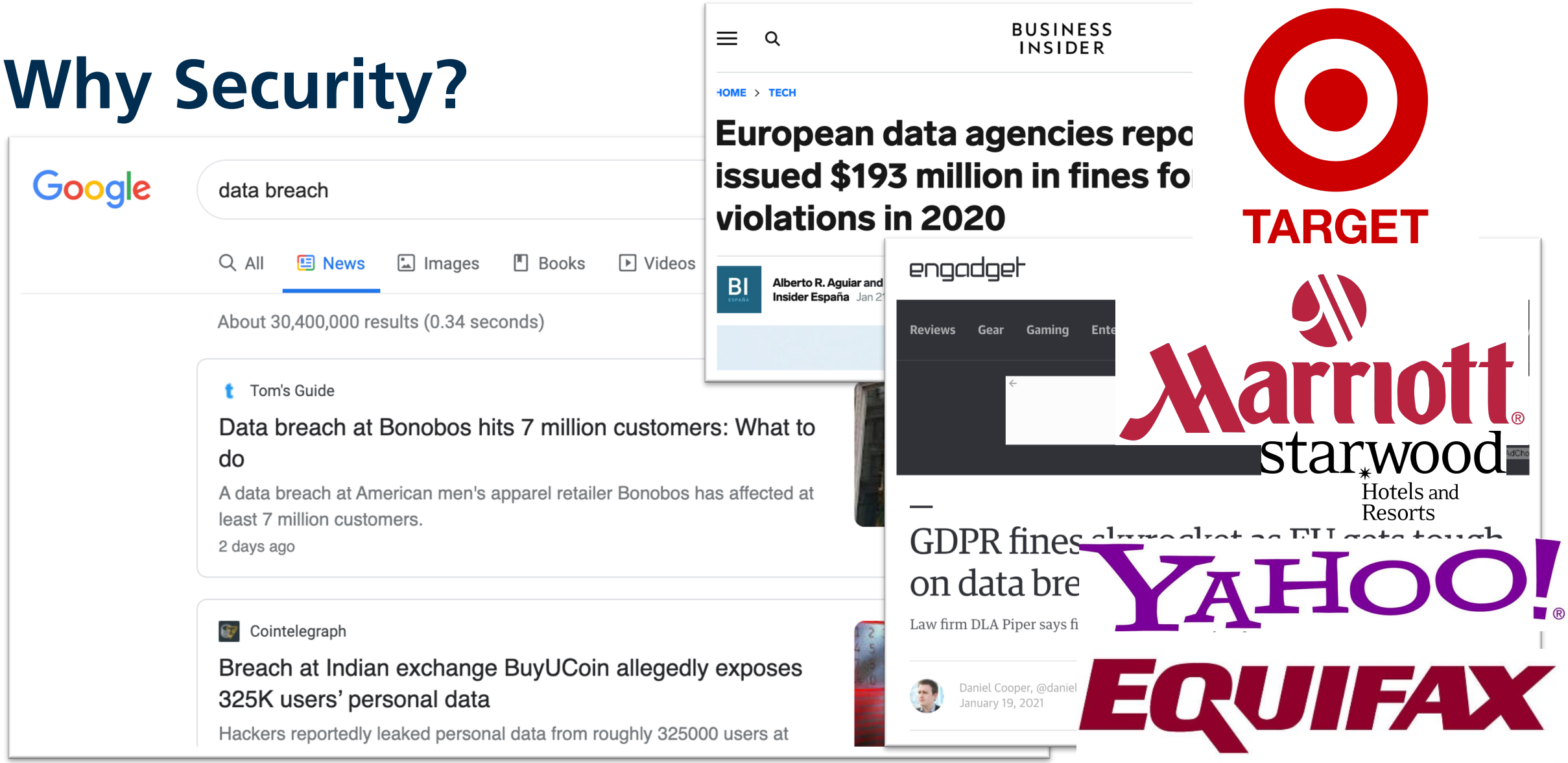
Assistant Professor, CS @ Georgetown

GEORGETOWN UNIVERSITY

About Me

- Joined CS @ Georgetown in Fall 2020
- Member of the Georgetown SecLab
- Broad research interests:
  design of **secure** and **accountable systems** and **networks**

Why Security?

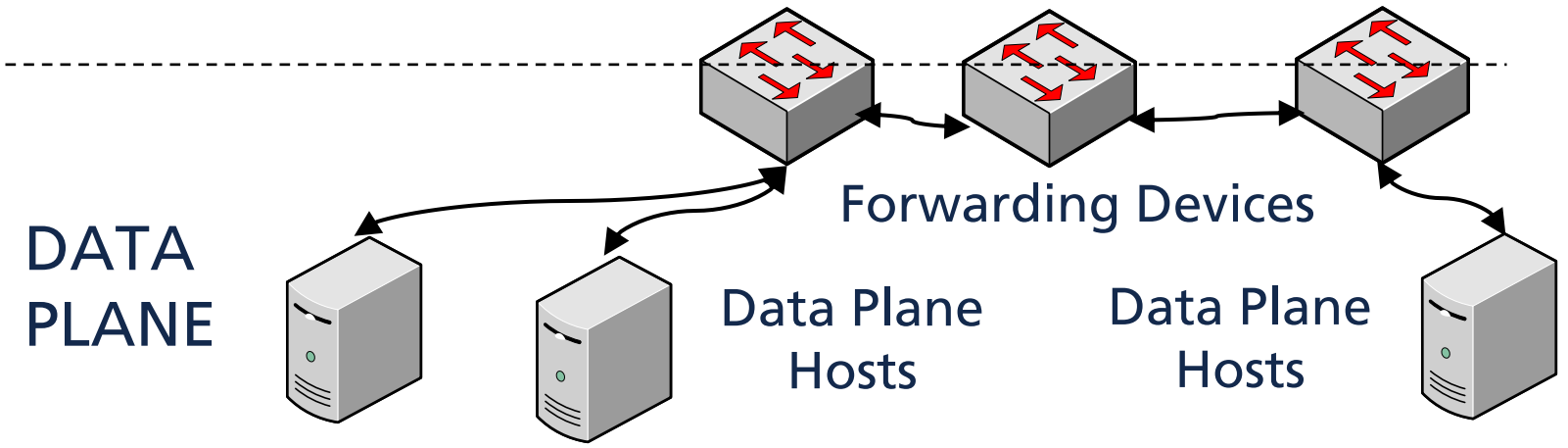


Current Research Projects

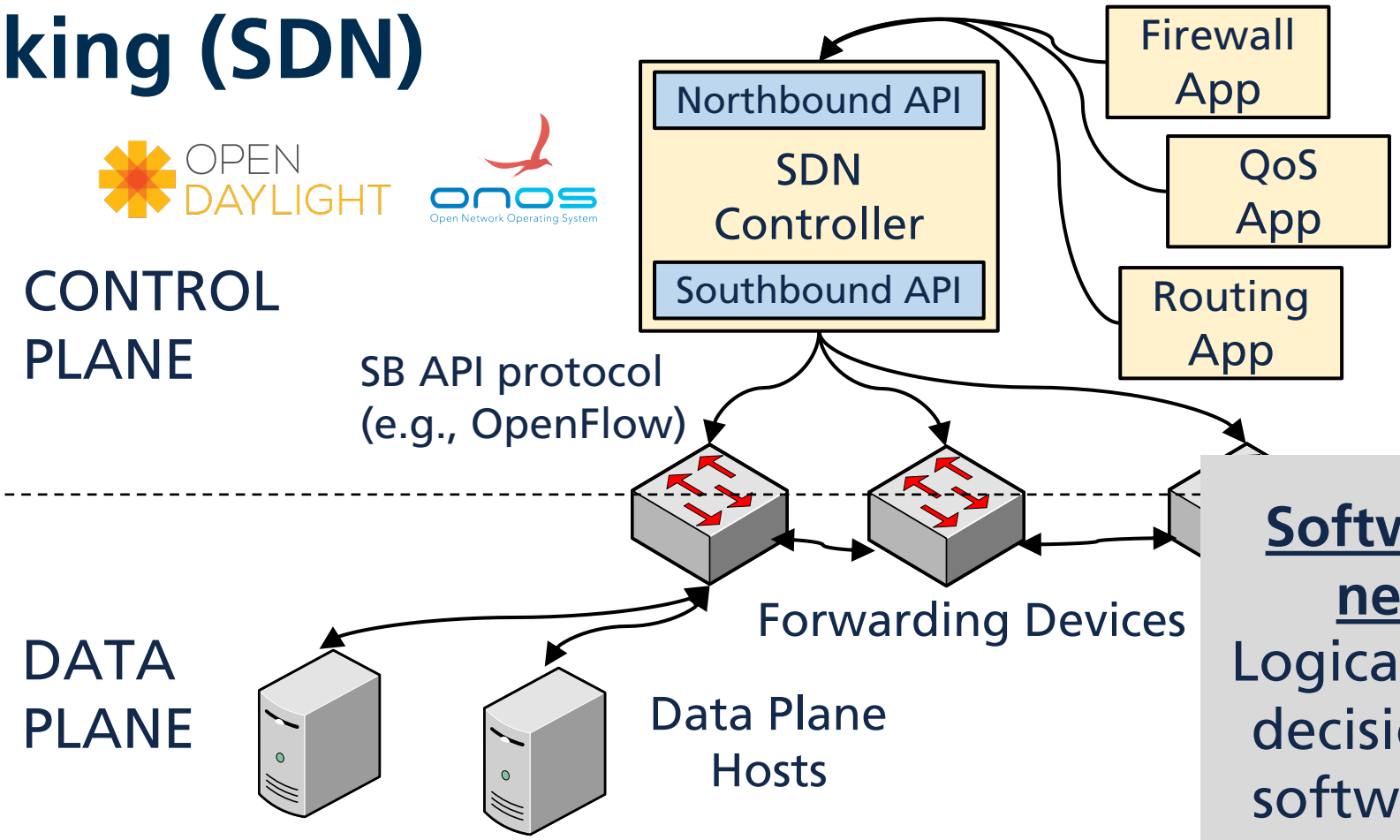
- Secure & accountable software-defined networking (SDN)
- Secure & accountable next generation networks
- Data provenance and data protection regulations

Secure & Accountable Software-Defined Networking (SDN)

Traditional networks:
Distributed decision-making (STP for forwarding, RIP/OSPF for routing, etc.)



Secure & Accountable Software-Defined Networking (SDN)



Software-defined networking: Logically centralized decision-making in software processes

Secure & Accountable Next Generation Networks

5G networks

Programmable data planes

Intent-based networking

Data Protection Regulations

- How do data protection regulations inform systems and networking design?
- How can secure and accountable systems and networking design inform data protection regulations?
- **Data provenance** as an accountability mechanism

Thanks!

Benjamin E. Ujcich
E-mail: bu31@georgetown.edu
Web: https://personal.benujcich.georgetown.domains

Theoretical Computer Science

Sasha Golovnev

Georgetown University, 2021

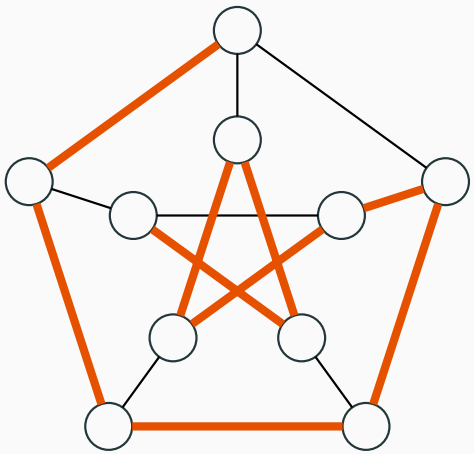
Motivating Question

What resources are required to solve a given computational problem?

Motivating Question

What resources are required to solve a given computational problem?

Traveling Salesman

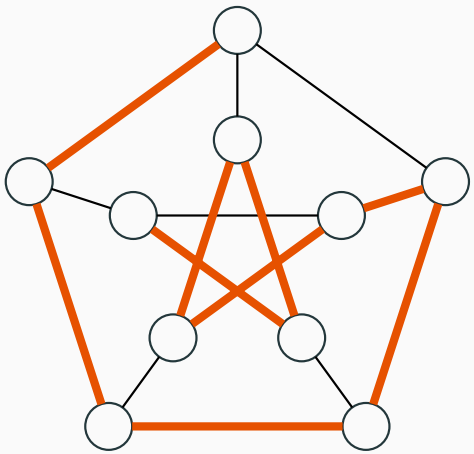


2^n

Motivating Question

What resources are required to solve a given computational problem?

Traveling Salesman



2^n

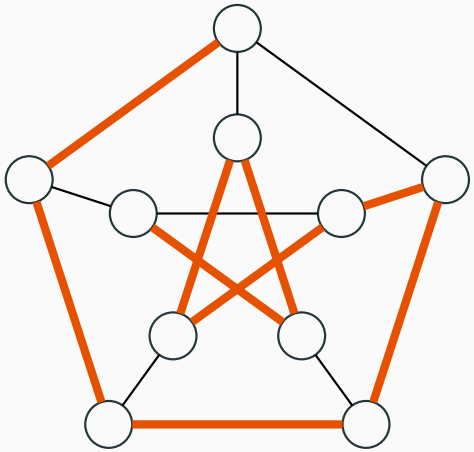
$P = NP?$

$\text{poly}(n)$

Motivating Question

What resources are required to solve a given computational problem?

Traveling Salesman



2^n

$P = NP?$

Edit Distance

e l e p h a n t

r e l e v a n t

p

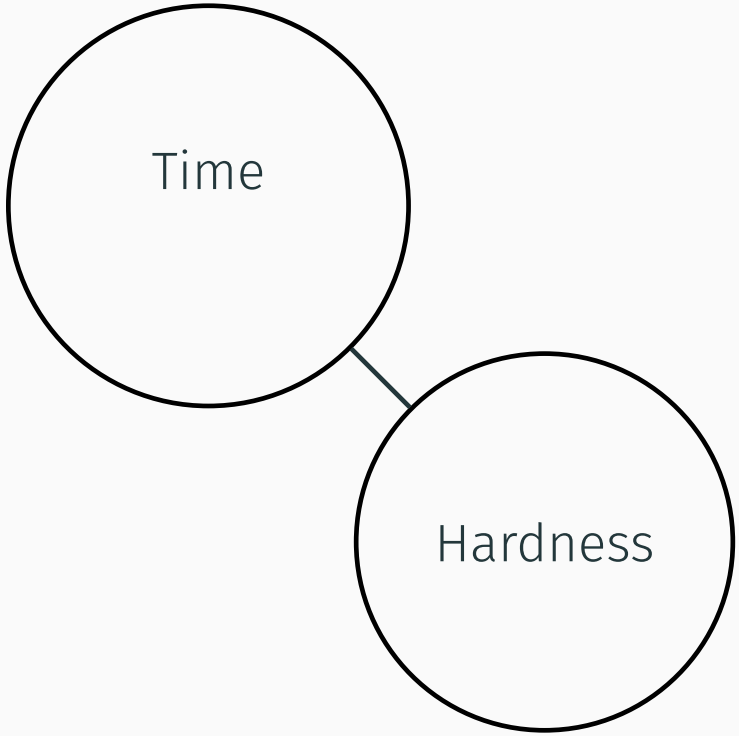
n^2

Motivating Question

What resources are required to solve a given computational problem?

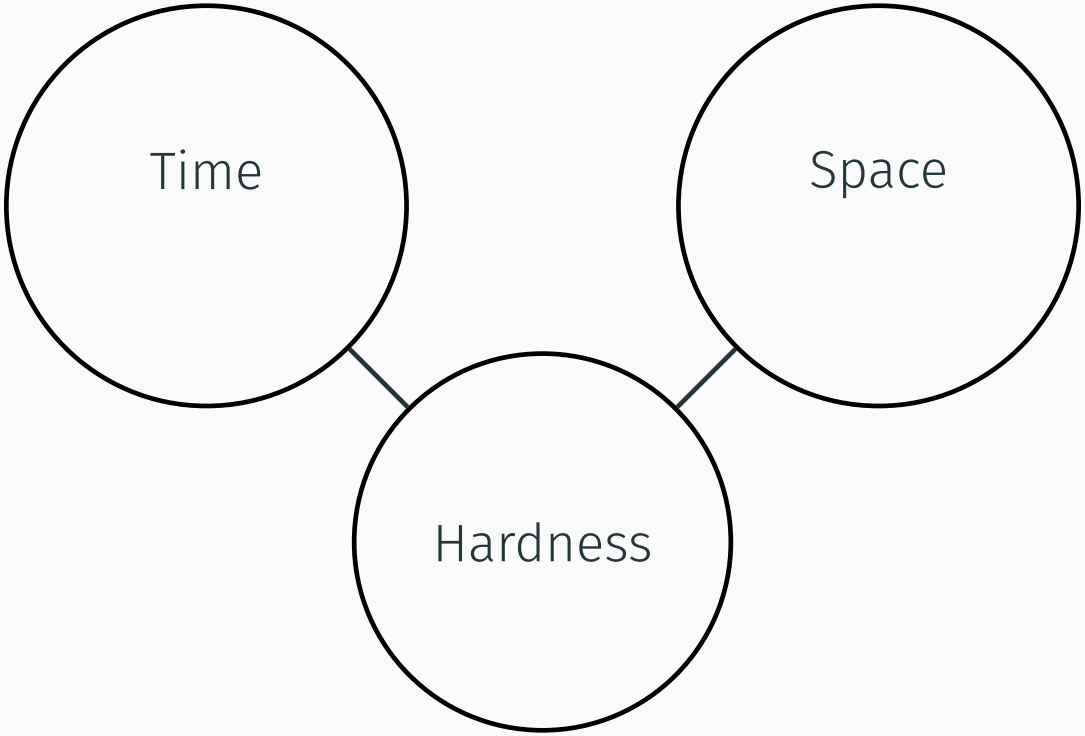
Motivating Question

What resources are required to solve a given computational problem?



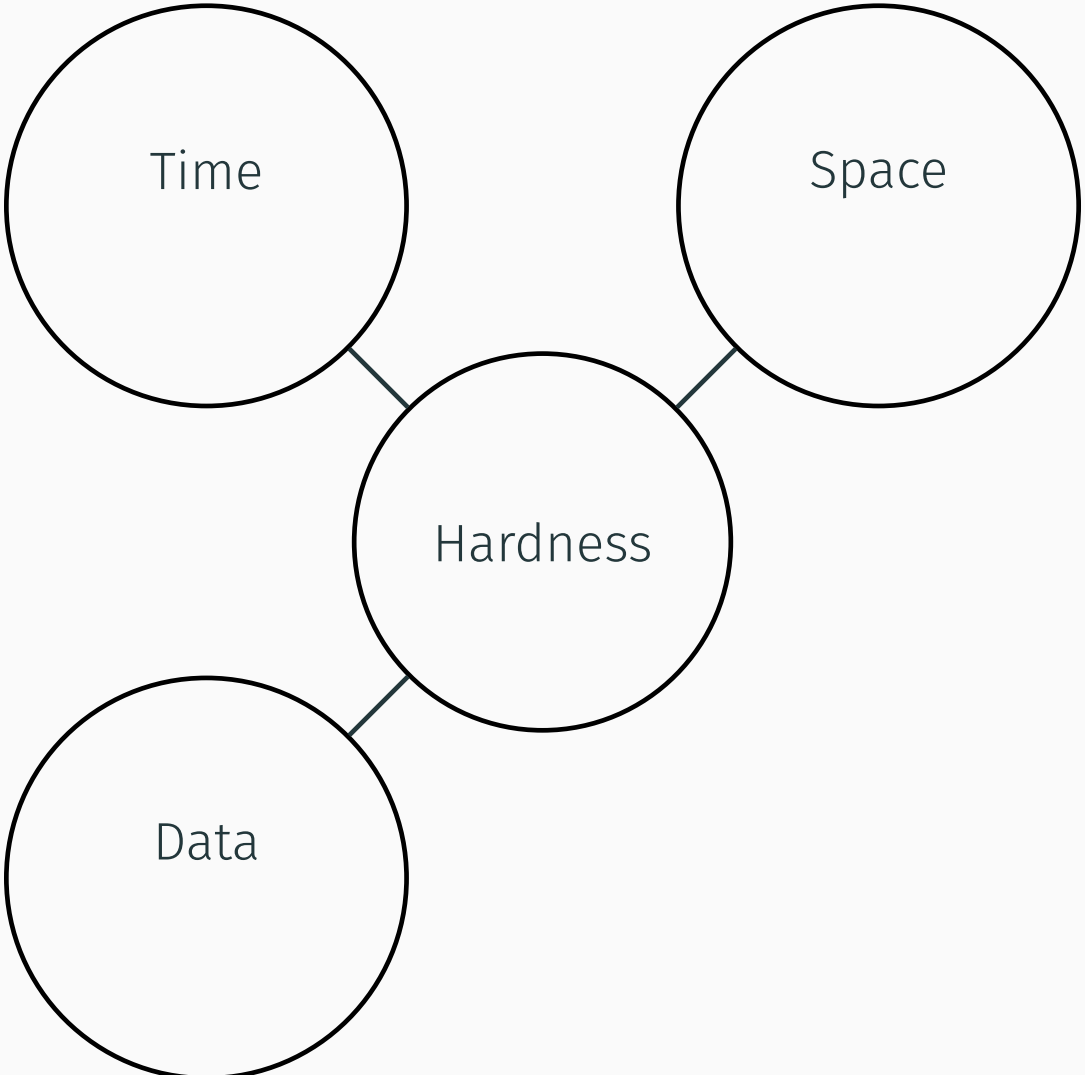
Motivating Question

What resources are required to solve a given computational problem?



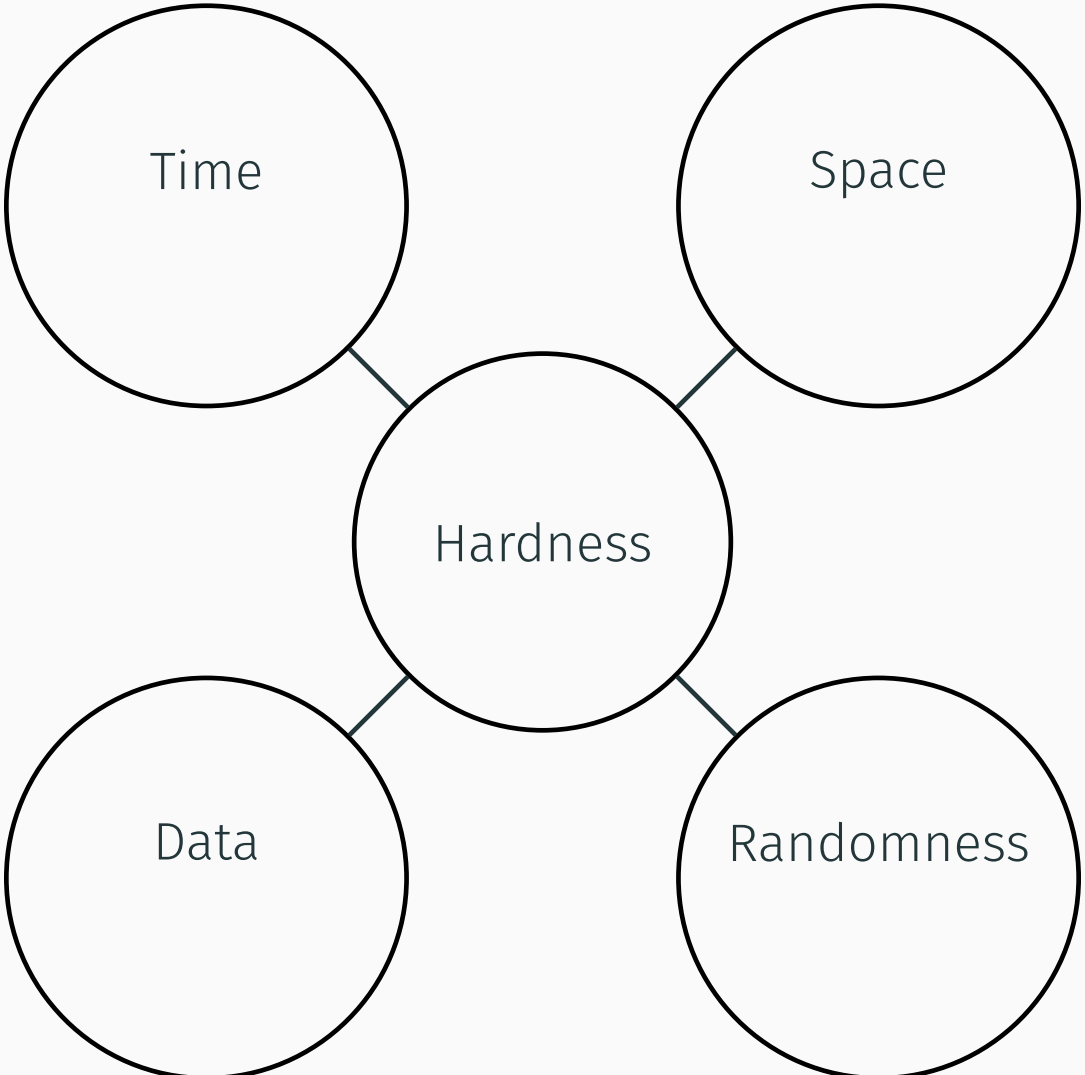
Motivating Question

What resources are required to solve a given computational problem?



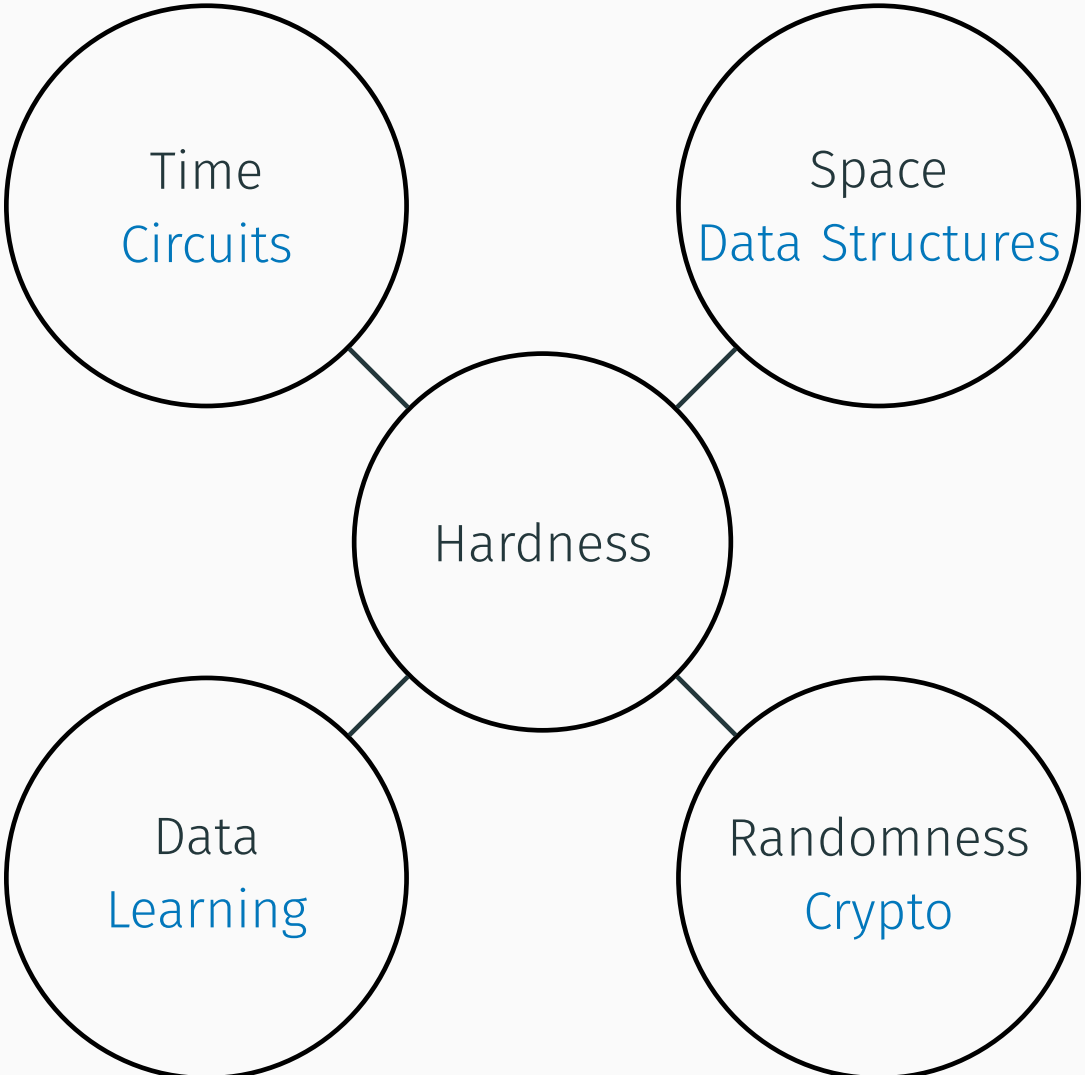
Motivating Question

What resources are required to solve a given computational problem?



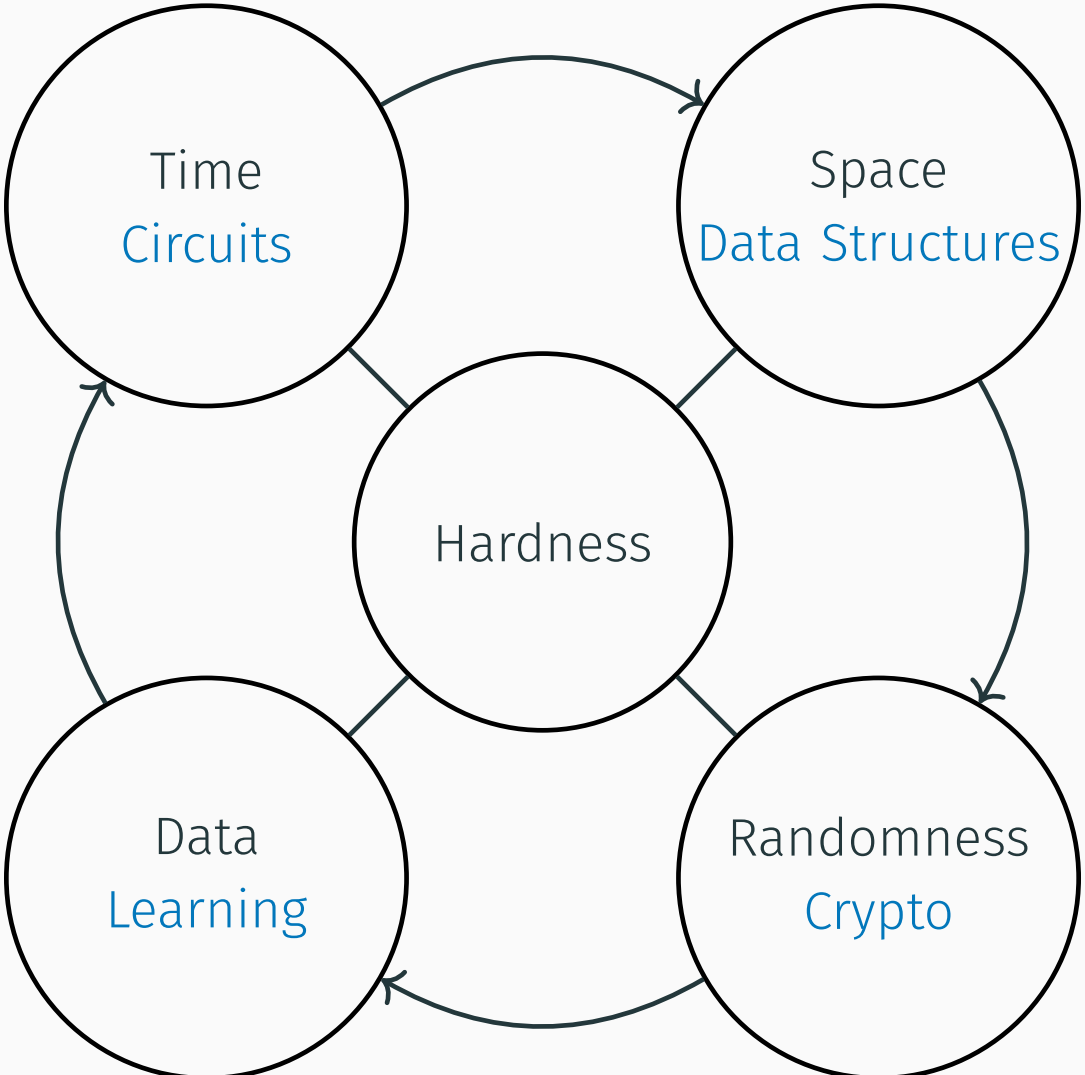
Outline

What resources are required to solve a given computational problem?



Outline

What resources are required to solve a given computational problem?



Contact me!

alex.golovnev@gmail.com

Undergraduate Opportunities

Prof. Eric Burger
eric.burger@georgetown.edu
https://people.cs.georgetown.edu/~eburger

GEORGETOWN UNIVERSITY
CyberSMART

1

SELECTION OF YOUR PREDECESSORS

GEORGETOWN UNIVERSITY | CyberSMART

2

Methods for Secure Caller Identification: Female (CS)

S²ERC Project: Next Generation Caller Identification
Authors: Dr. Eric Burger and [redacted]
Date: 23 June 2016

Abstract

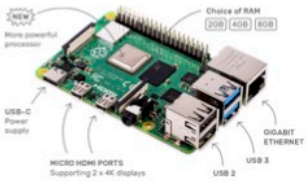
This report, a result of the *Next Generation Caller Identification* project in the PSTN Transition program in the S²ERC, examines a proposal for asserting caller identity in the all-IP telecommunications network, 4474bis in conjunction with the work being progressed in the ATIS SIP Forum IP NNI Task Group.

STIR is the standard developed by IETF that defines a signature to verify the calling number, and specifies how it will be transported in SIP "on the wire" whereas SHAKEN is the framework document developed by ATIS/SIP Forum IP-NNI task force to provide an implementation profile for service providers implementing STIR. The objective of SHAKEN is to provide guidance to implementers to ensure interoperability. The mechanism passes a JWT token (JSON Web Token) in the SIP INVITE request in the Identity header. It also integrated the IETF passport mechanism, which specifies a token format for authenticating sent information. This report describes the mechanism and how it addresses the caller identification challenges faced by telecommunications users.

- Drove industry and FCC to a single solution
- Invited to AT&T to talk about work
- Invited to Congress to talk about work
- First job AT&T
- Now at Palantir

3

Play with Hardware Security Modules: Male (CS)



An Affordable Solution for Authenticated Communications for Enterprise and Personal Use

[redacted]
Department of Computer Science
Georgetown University
37th & O St, NW
Washington, DC 20057 USA
Email: mlc248@georgetown.edu

Eric Burger
Department of Computer Science
Georgetown University
37th & O St, NW
Washington, DC 20057 USA
Email: eric.burger@georgetown.edu

***Abstract*—The top complaint received by both the U.S. Federal Trade Commission and Federal Communications Commission is illegal robocalling. One of the issues enabling illegal robocalling is the relative ease of a bad actor to spoof, or lie, about who is calling. Specifically, the bad actor can set their Caller ID, or the number that is displayed when one receives a phone call, to whatever they want. The Internet Engineering Task Force (IETF), the SIP Forum, and the Alliance for Telecommunications Industry Solutions (ATIS) have been jointly working on a solution, called STIR, to provide authentication** payments"; SWATting, where a criminal targets another for assassination or arrest by placing a 911 call with the target's phone number as the Caller ID, usually with a report of an armed and dangerous situation underway, resulting in the police responding in force; and so on. Furthermore, in the US, illegal robocalls are the #1 complaint at both the Federal Communications Commission (FCC) and Federal Trade Commission (FTC). RFC 7340 [1] gives a more detailed description of the problem.

- Fun to work with HSM, Raspberry Pi, Play with phone network
- Filled important hole in the state of STIR art
- First job: Appian
- Now at AWS

Trip to Las Vegas to present paper

4

Economic Impact of Cyber Breaches: Male (MSB)

JOURNAL OF INFORMATION PRIVACY AND SECURITY
https://doi.org/10.1080/15536548.2017.1394070

Routledge
Taylor & Francis Group

Check for updates

Long-term market implications of data breaches, not

[redacted] and Eric W. Burger [b]

[a]McDonough School of Business, Georgetown University, Washington, DC, USA; [b]Department of Computer Science, Georgetown University, Washington, DC, USA

ABSTRACT
This report assesses the impact disclosure of data breaches has on the total returns and volatility of the affected companies' stock, with a focus on the results relative to the performance of the firms' peer industries, as represented through selected indices rather than the market as a whole. financial performance is considered over a range of dates from 3 days post-breach through 6 months post-breach, in order to provide a longer-term perspective on the impact of the breach announcement.

Introduction: data breaches and leaks

An increasingly common cost of doing business

Commensurate with an increasingly connected and digital business environment, the incidence of cyber-attacks and consequences of data breaches has been growing. Research from ThreatMetrix (2016) shows that the volume of cyber-attacks is up 50% from the second

- Highly cited paper
- Invitations to FTC
- Started in investment banking, now in commercial real estate investment

5

Ensure Calls Complete to Rural Customers: Female (CS & Math)

Federal Communications Commission **FCC 19-23**

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Rural Call Completion	)	WC Docket No. 13-39
	)	

FOURTH REPORT AND ORDER

Adopted: March 15, 2019 **Released: March 15, 2019**

By the Commission: Commissioners Rosenworcel and Starks approving in part, concurring in part and issuing separate statements.

TABLE OF CONTENTS

- Joined Clinton campaign
- Analytics for Beto, Warren, and Biden

flexibility to self-monitor rural call completion performance. We therefore decline to adopt Inteliquent's proposal for performance targets on a weekly and LATA/OCN basis. We agree, as described by Georgetown University, that while evaluation of these and other metrics over time is a valuable tool to ensure call completion, specific performance targets are not useful.[109]

[109] *See* [redacted] Geo. Sec. & Software Eng'g Research Ctr., *Issues, Analysis, and Tools for Rural Call Completion Issues* 3 n.9, 7 (2017), https://ecfsapi.fcc.gov/file/104180548507226/S2ERC%2013-39%20Filing.pdf. Most performance metrics vary widely between OCN pairs based on factors unrelated to completion issues. *See id.*

6

ISP Consumer Privacy: Male (STIA)

Federal Communications Commission FCC 16-148

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services) WC Docket No. 16-106
)

REPORT AND ORDER

Adopted: October 27, 2016 Released: November 2, 2016

By the Commission: Chairman Wheeler and Commissioner Rosenworcel issuing separate statements; Commissioner Clyburn approving in part, concurring in part and issuing a statement; Commissioners Pai and O'Rielly dissenting and issuing separate statements.

TABLE OF CONTENTS

- Work referenced in order 11 times
- For comparison, Georgetown Law *Professor* referenced only 3 times
- Finishing his PhD in Cyber Security at Oxford on a Rhodes Scholarship

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services) WC Docket No. 16-106
)

COMMENTS OF THE SECURITY AND SOFTWARE ENGINEERNIG RESEARCH CENTER AT GEORGETOWN UNIVERSITY

The Security and Software Engineering Research Center (S²ERC) at Georgetown University is an industry supported and NSF-sponsored[1] research center working on the safety, security, and stability of communication networks. These comments reflect the research results and opinions of the center's researchers and staff and do not necessarily reflect the opinions of Georgetown University, the NSF, or the affiliate members of the S²ERC. Dr. Eric Burger, Mr. James Pavur, and Ms. Marika Van Laan prepared these comments.

7

Super Fast Rundown

- You want to be in government or influence government?
- Interested in cyber security, policy, business?
- Want a project that can turn into a company?
- Interested in communications networks, secure communications, how the Internet runs or can be better?

See Me!

- Opportunities for independent study, thesis, and funding

8

So – You Want Money? Current Sponsored Projects:

- Characterization, thoughts, and policy proposals for next-generation mobile wireless services (Beyond 5G)
- Tools for detecting and protecting against telecommunications fraud
- Applications of blockchain for various financial and other applications

9

Interested?

- **After** reviewing my web site, https://people.cs.georgetown.edu/~eburger/
- **Send** me an email, eric.burger@georgetown.edu

10

Undergraduate Research Opportunities
EventBlockchain Research

Shin’ichiro Matsuo
Shinichiro.Matsuo@georgetown.edu

GEORGETOWN UNIVERSITY

About me

@Shanematsuo

- Member of SecLab
- Director of Cyber SMART research center
- Co-chair of Blockchain Governance Initiative Network (BGIN)
- Co-Founder of Bsafe.network (Blockchain Global Testbed)
- A member of OECD Blockchain Expert Policy Advisory Board(BEPAB)
- Founder of CELLOS Consortium (Evaluation of Cryptographic Protocols)

I have no Bitcoin and any cryptoassets.

Current People at Georgetown University CyberSMART

Faculties

Computer Science

Shin'ichiro Matsuo
(Director: Cryptography and security)

Eric Burger
(Network Security)

Ophir Frieder
(Communication Systems)

McDonough School of Business

Reena Aggarwal
(Stock market, IPO)

James Angel
(Regulation)

John Jacobs
(Former CMO of NASDAQ)

Vlad Babich

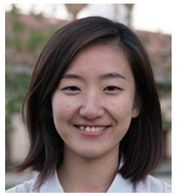
Perianne Boring
(FinTech and Blockchain)

Center for National Security and the Law

Clare Sullivan
(Managing Director, Digital identity and privacy)

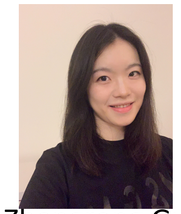
Researchers / Students

Research Assistant



Jianna SU

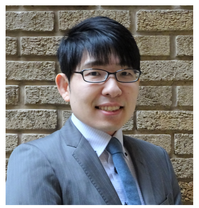
Michael Bartholic



Zhengrong Gu

Sachin Meier

Visiting Research Fellow



Ryosuke Ushida

Yusuke Ikeno

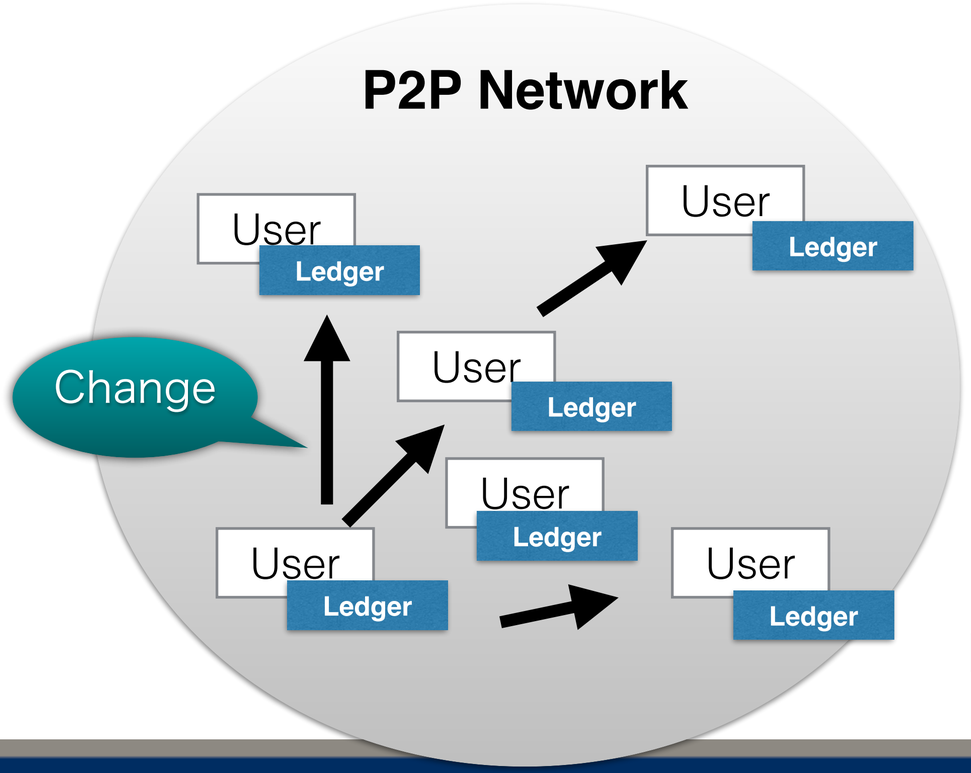
Intern

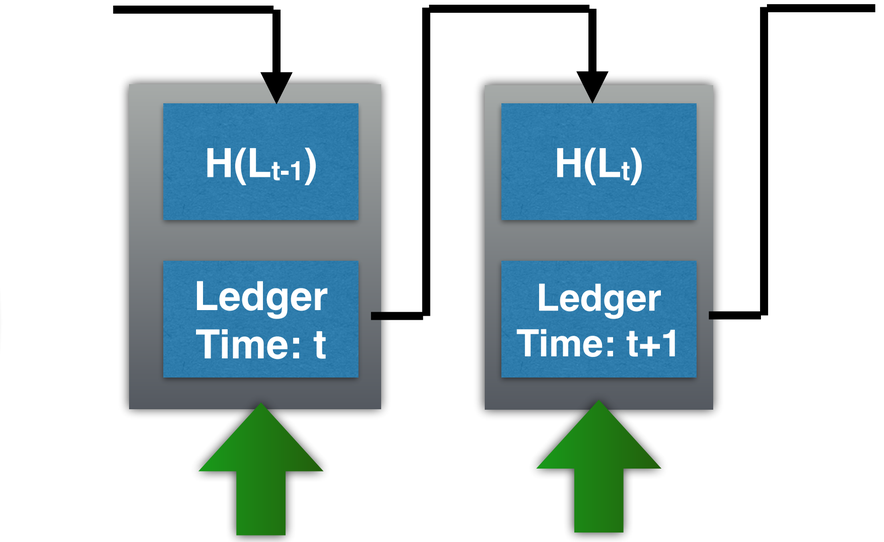
Kentaro Sako

Blockchain

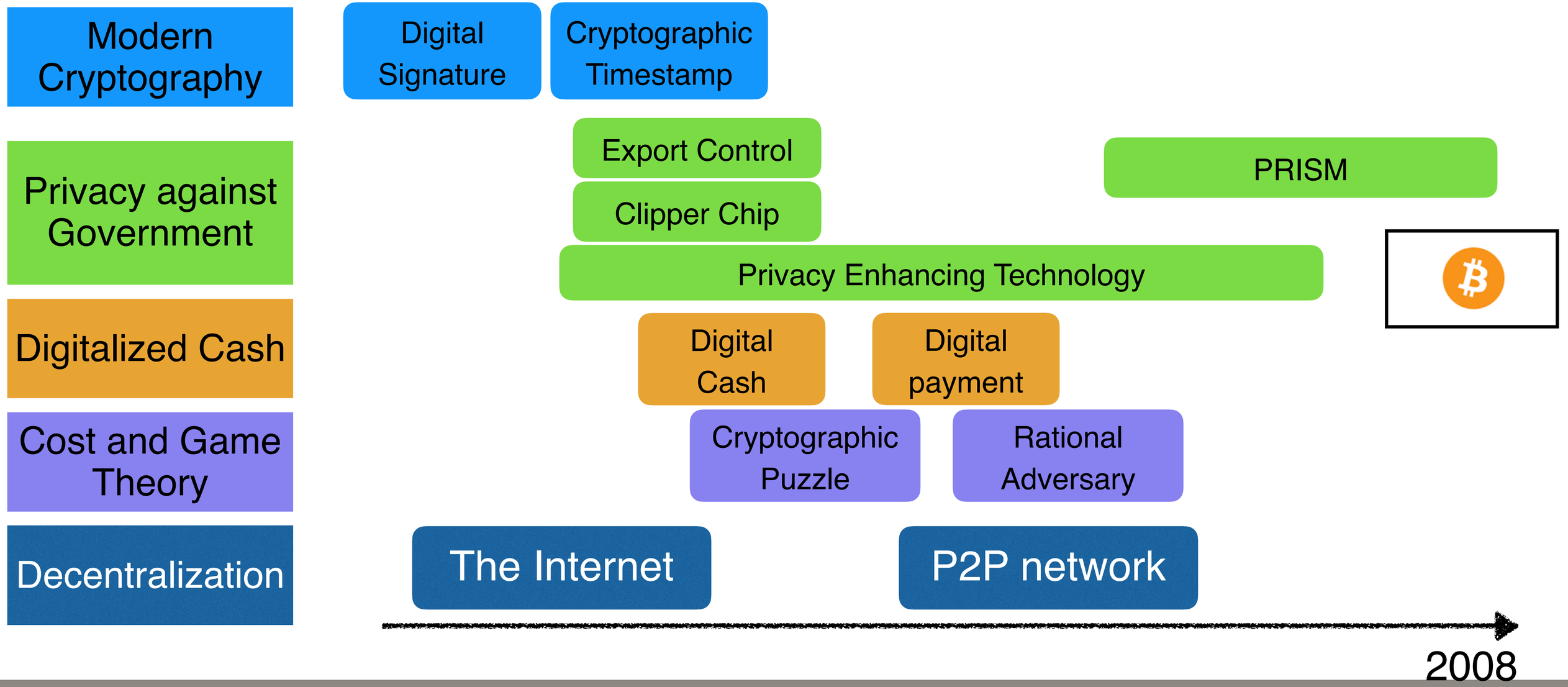
- **Fundamental techniques to realize “Public Ledger” using P2P network and chained digital signature**
- **Used in digital assets like Bitcoin**
- **Anyone can join/leave at any moment**

Each node updates its distributed ledger





Chronology Before Bitcoin



Research Challenge

1. Security of Blockchain/Smart Contract
   1. Protocol Security
   2. Custodians (with Coinbase)
   3. Game theory (with NTT)
2. Applications of smart contract
3. Digital Currency and CBDC

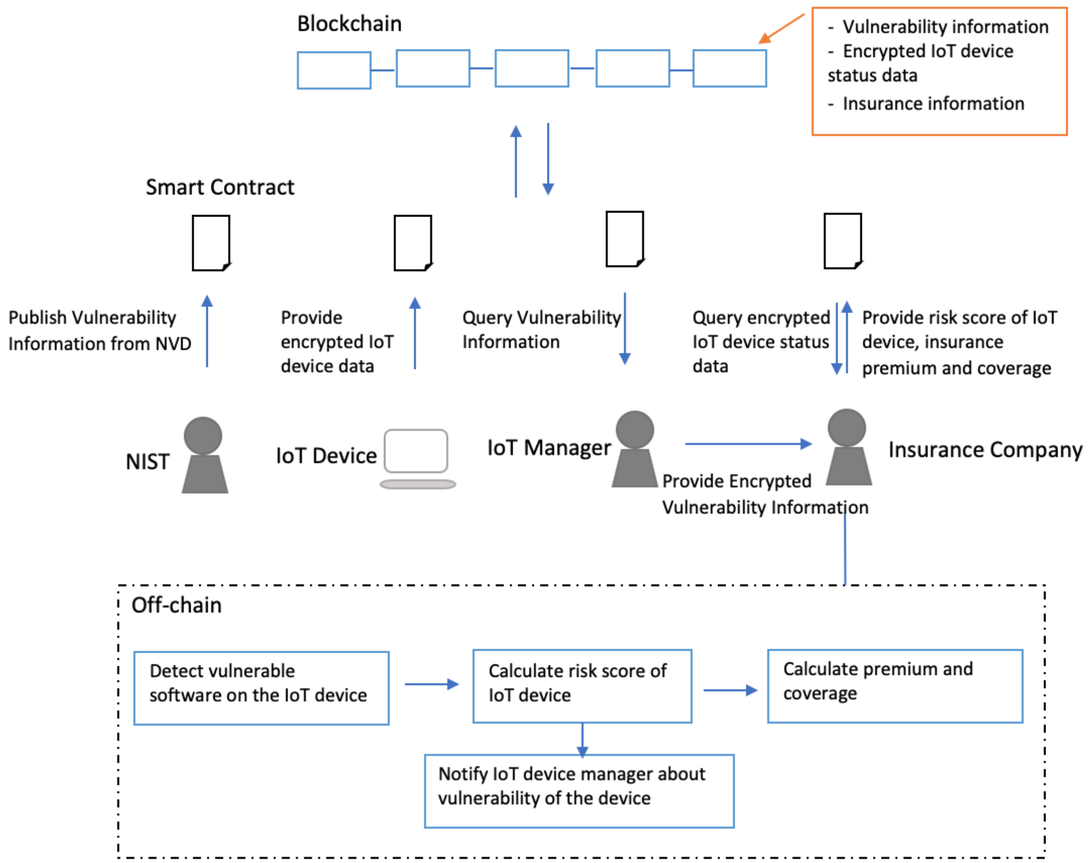
Examples of undergraduate research

1. How to Dynamically Incentivize Sufficient Level of IoT Security (accepted at WTSC 20)
2. Proof of No-Work: How to Incentivize Individuals to Stay at Home (accepted at CBT 20)
3. Fairness in ERC token markets: A Case Study of CryptoKitties (accepted at WTSC 21)

How to Dynamically Incentivize Sufficient Level of IoT Security

- Cyber insurance, as a way to transfer risk of losses to insurer, drives improvements in cyber security by incentivizing insured party to take security controls.
- Cyber insurance covers risks caused by technical and human factors. This project concentrates on those technical factors.

- Provide a dynamic view into an enterprise's vulnerabilities and responses to vulnerabilities
- Provide a financial incentive to enterprises to proactively secure their network environment
- Provide a dynamic insurance pricing scheme for traditional cyber insurance
- Provide timestamped information for public verification
- Automate insurance processes to a certain extent



Use of Searchable Encryption, Plaintext Equality Test

J. Su, M. Bartholic, A. Stange, R. Ushida and S. Matsuo, "How to Dynamically Incentivize Sufficient Level of IoT Security," WTSC 20

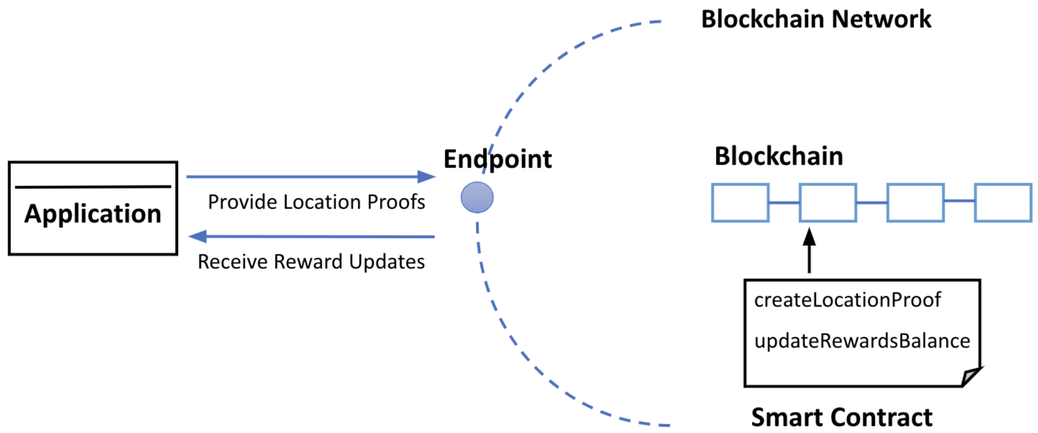
Proof of No-Work: How to Incentivize Individuals to Stay at Home

- Contact tracing applications:
  - 2020 global pandemic greats new challenges for addressing
  - Invasive data collection (usually bluetooth and GPS based)
  - Focused on tracking infections and possibly exposed individuals (follow ups)
  - Individuals often still behave without concern for elevated risks
- Problems include:
  - Unnecessary data collection and tracking
  - It may be more effective to incentivise behavioral change rather than track possible exposures after they've happened
  - No concrete incentive mechanism to act in ways that reduce risks

M. Bartholic, J. Su, R. Ushida, Y. Ikeno, Z. Gu and S. Matsuo,
"Proof of No-Work: How to Incentivize Individuals to Stay at Home," CBT20

Proof of No-Work: How to Incentivize Individuals to Stay at Home

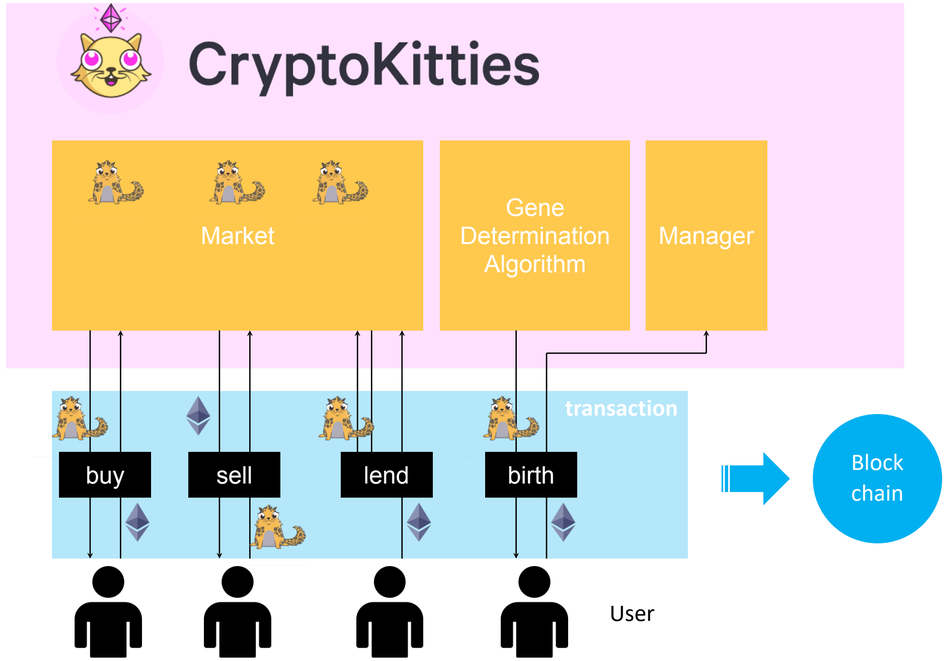
- In order to adequately incentivize individuals to act to the benefit of the community, we must develop an individualized incentive that responds to each person's own behavior. We also need to pay mind to minimize data collection and maintain reasonable computational efficiency.
  - Basic Requirements:
    - Proof of location, over time
    - Verifiable time to prevent replay attack
    - Scoring system (incentive mechanism) that can be publicly verifiable



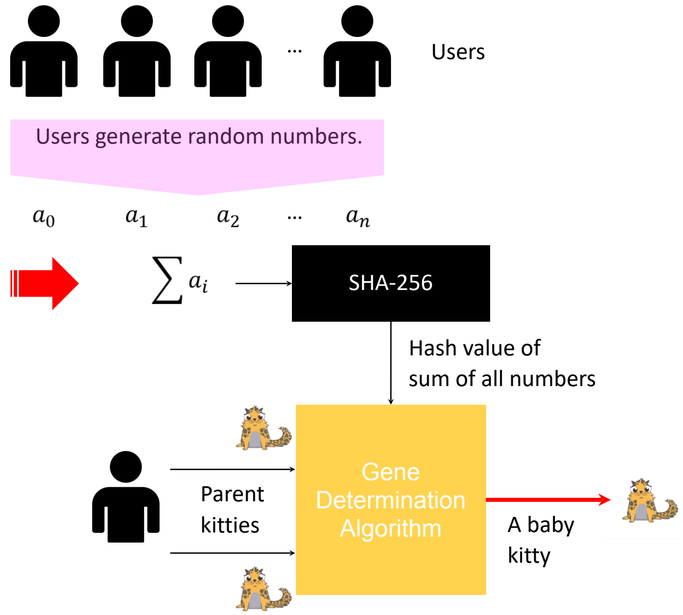
M. Bartholic, J. Su, R. Ushida, Y. Ikeno, Z. Gu and S. Matsuo, "Proof of No-Work: How to Incentivize Individuals to Stay at Home," CBT20

Fairness in ERC token markets: A Case Study of CryptoKitties

- Players try to earn ETHs by trading ERC-721 tokens.
  - This token is a kitty.



- Fix unfairness of the game caused by imperfect random function



K. Sako, S. Matsuo and S. Meier, "Fairness in ERC token markets: A Case Study of CryptoKitties," WTSC21

Thank you!

Email: Shinichiro.Matsuo@georgetown.edu

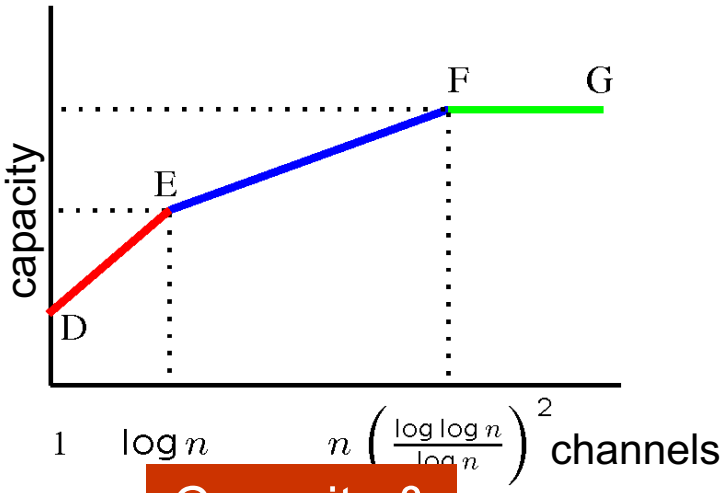
GEORGETOWN UNIVERSITY

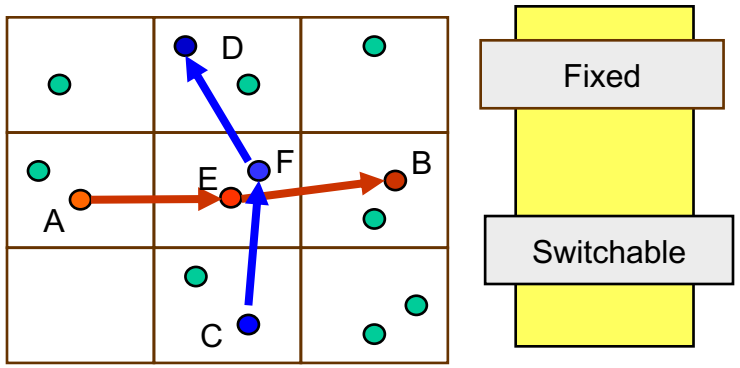
Distributed Algorithms

Nitin Vaidya
Georgetown University

Multi-Channel Wireless Mesh

Talk Outline



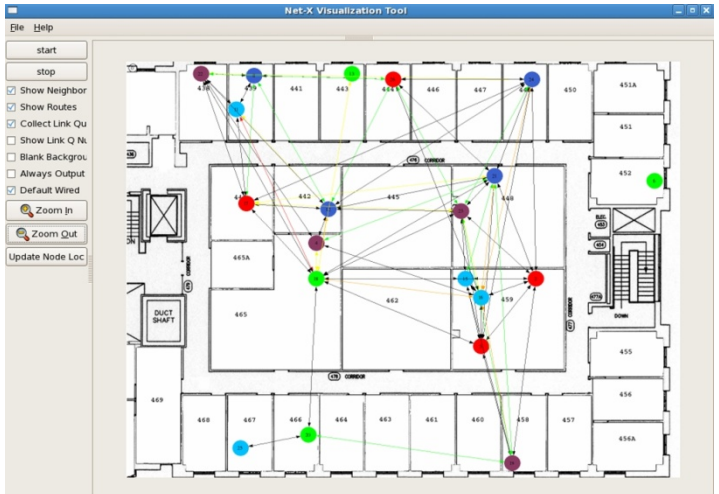


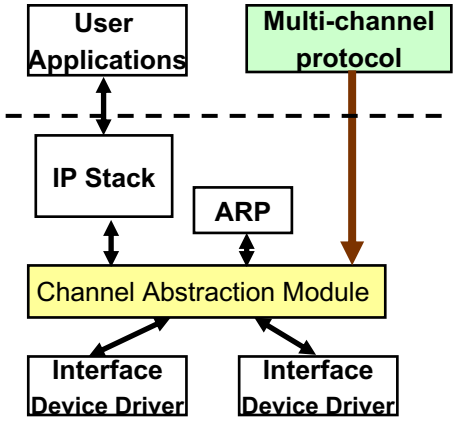
Capacity & Scheduling

Insights on protocol design

OS improvements Software architecture

Net-X testbed





Distributed Algorithms

- Distributed algorithms have wide-ranging applications
  - Cloud computing
  - Machine learning
  - Social networks
  - Swarm robotics
  - Multi-core processors
  - Supercomputing
  - …

My Current Research

- Distributed optimization and machine learning:
  Security & Privacy
- Consistency of key-value stores
- Distributed consensus
- Graph algorithms

Other Faculty in Parallel & Distributed Algorithms

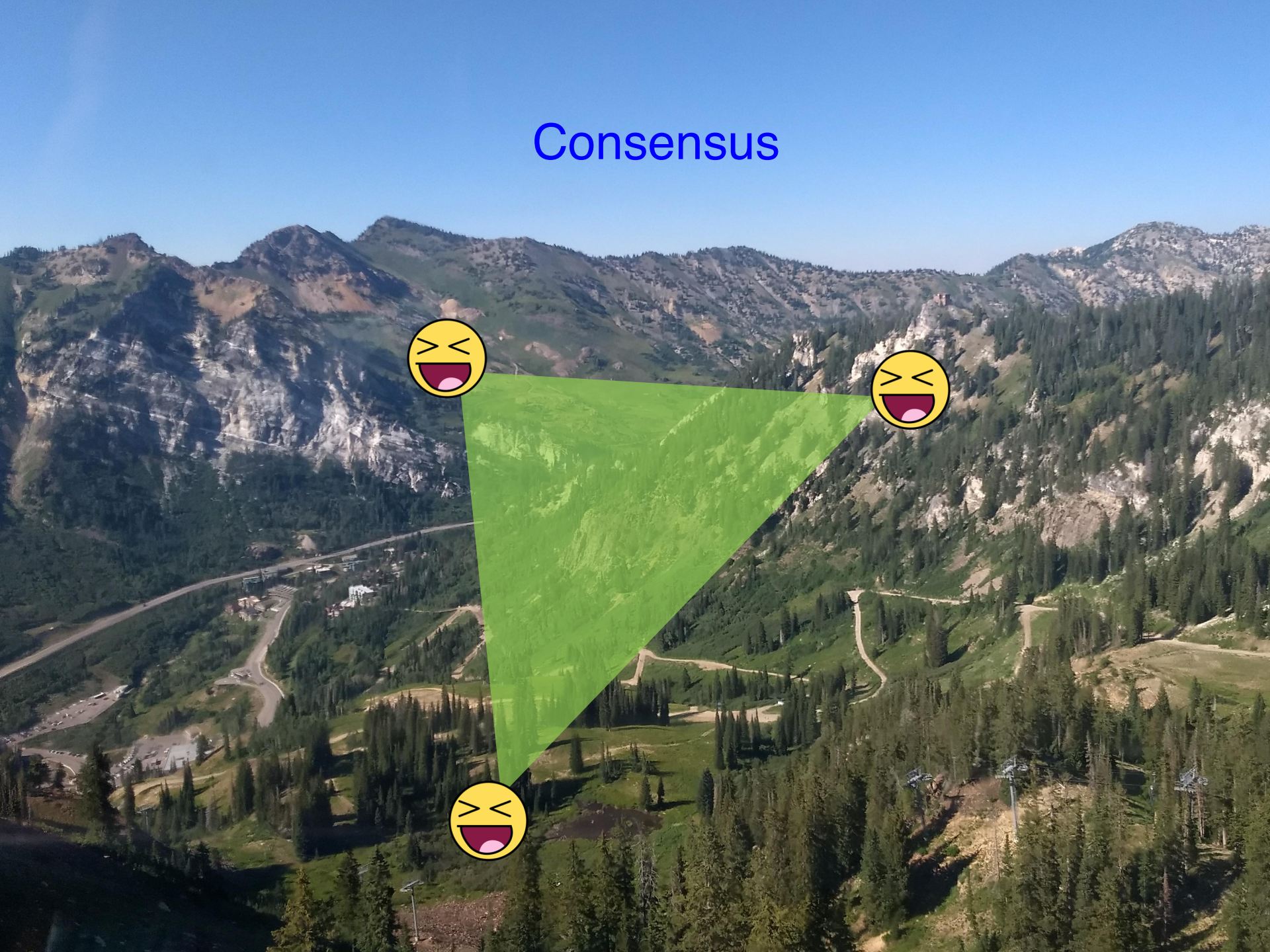
- Jeremy Fineman
- Cal Newport

Security and Privacy

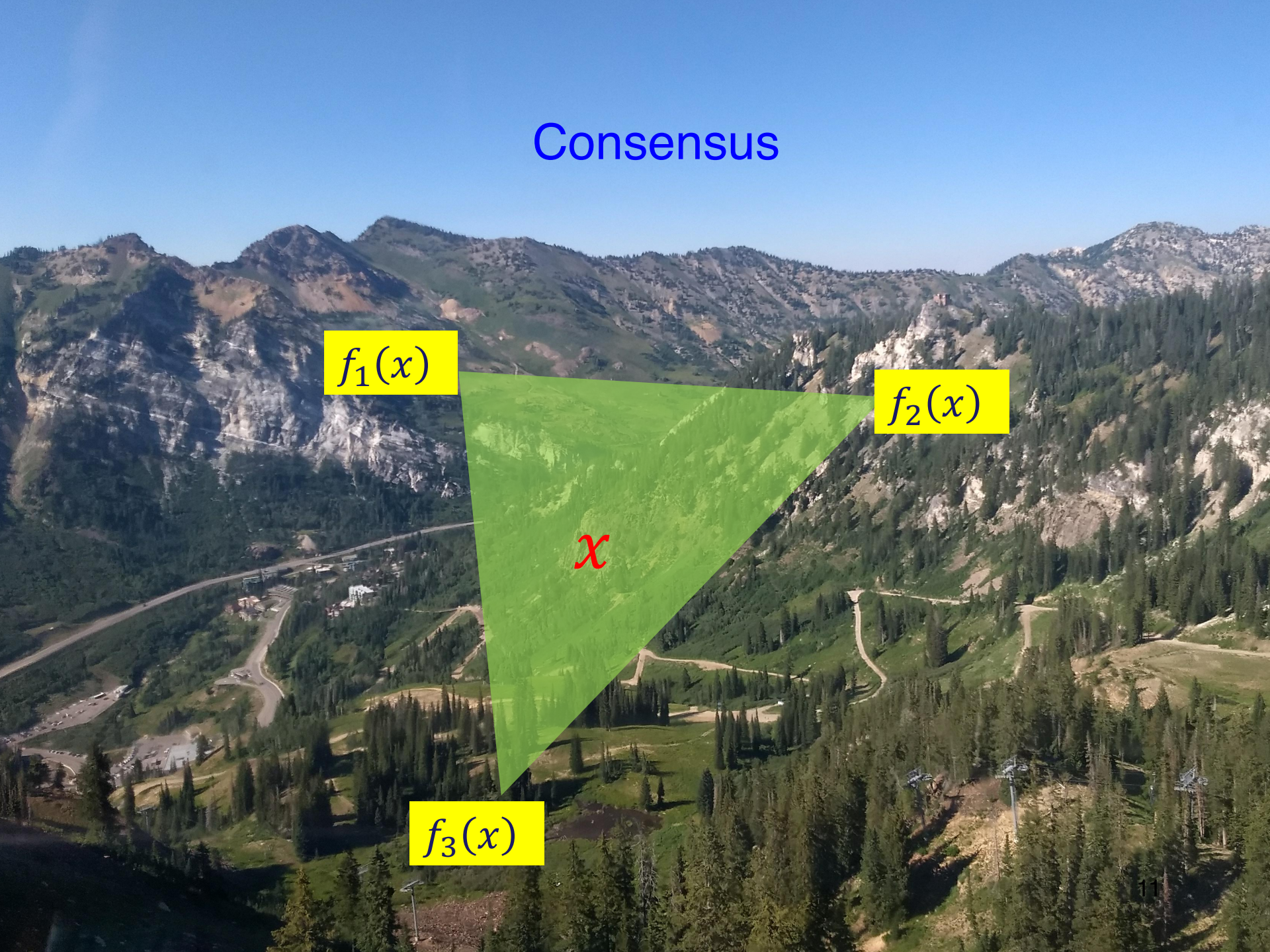
for

Distributed Optimization and Learning

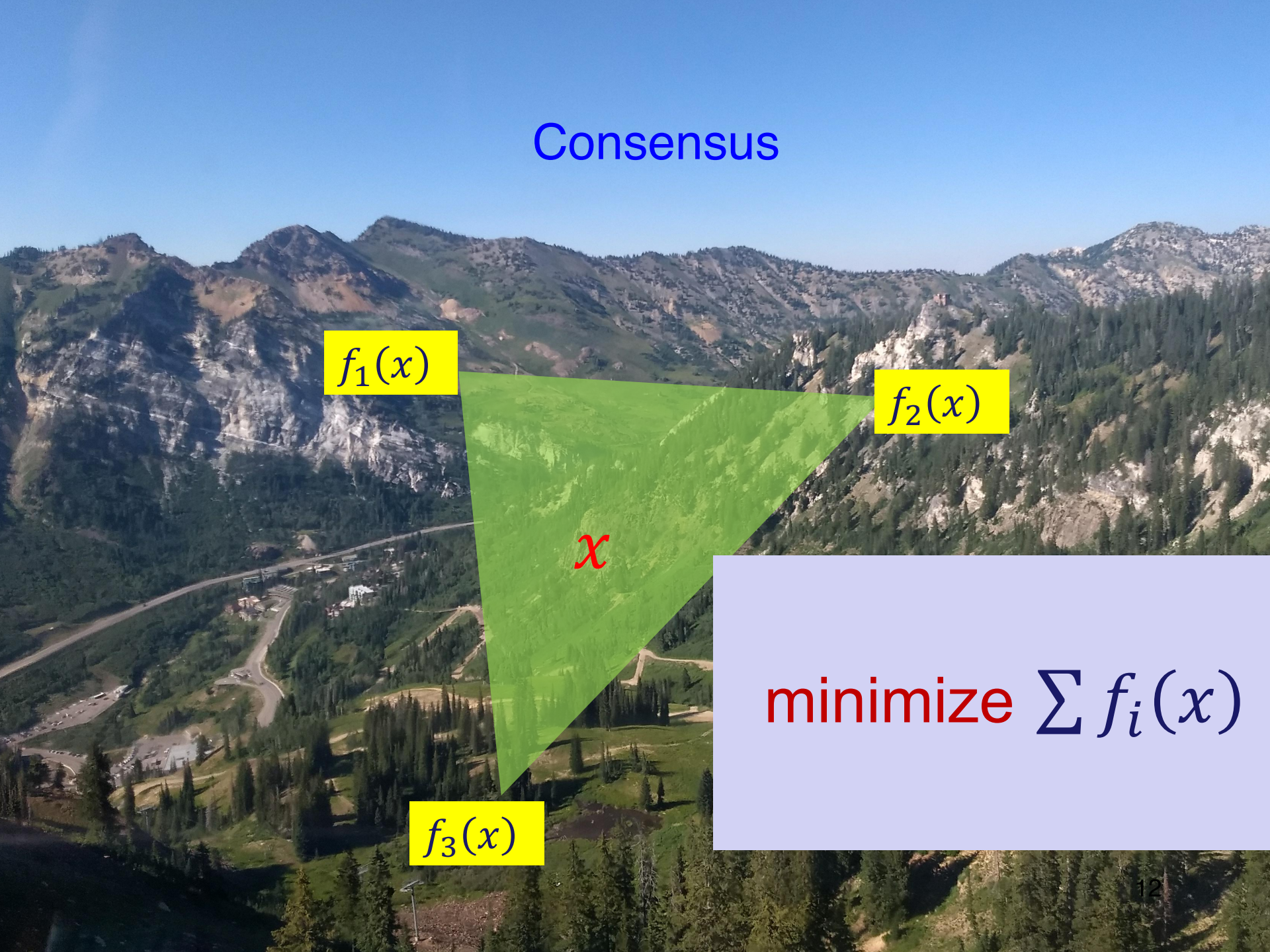
Consensus



Consensus



Consensus

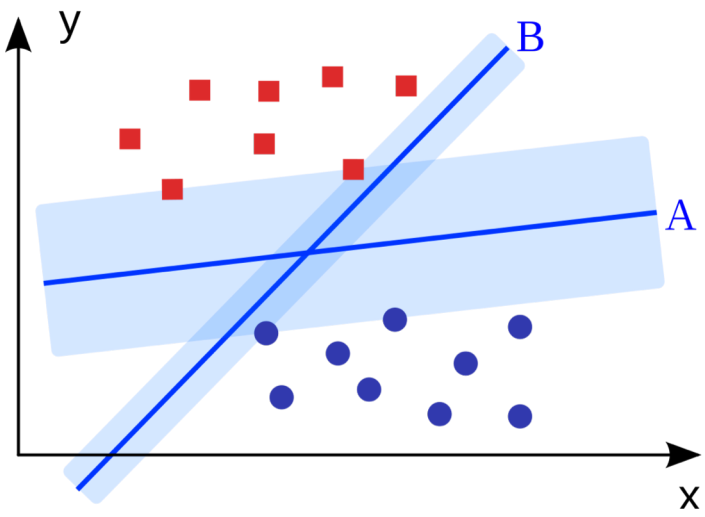


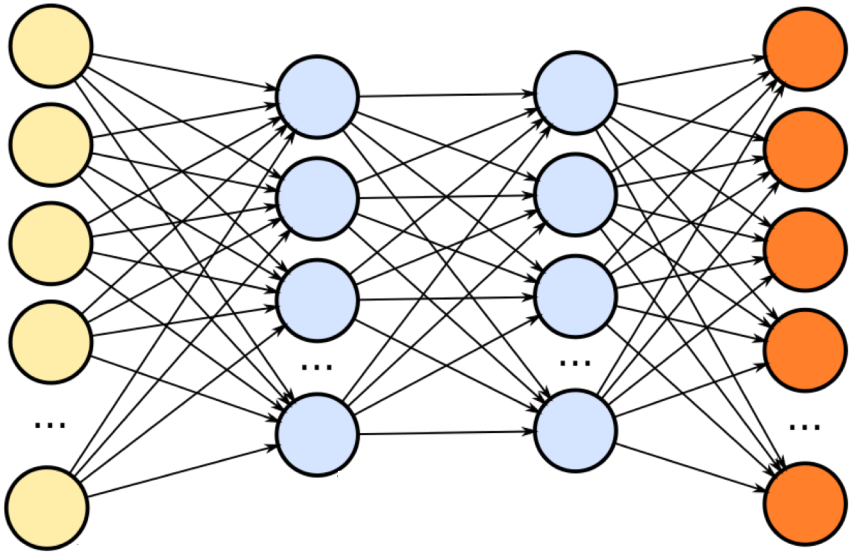
minimize $\sum f_i(x)$

Machine Learning

- Data is distributed across different agents

- Data is distributed across different agents ➔ Collaborate to learn





Machine Learning

Minimize global loss

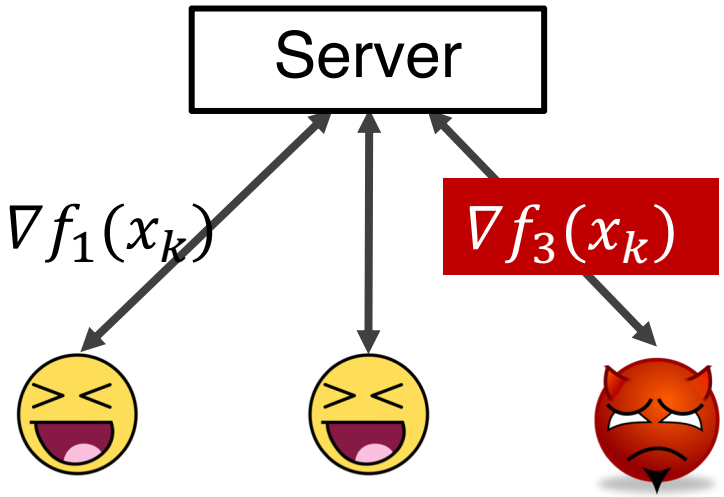
$$\sum f_i(x)$$

Challenges

Challenge #1

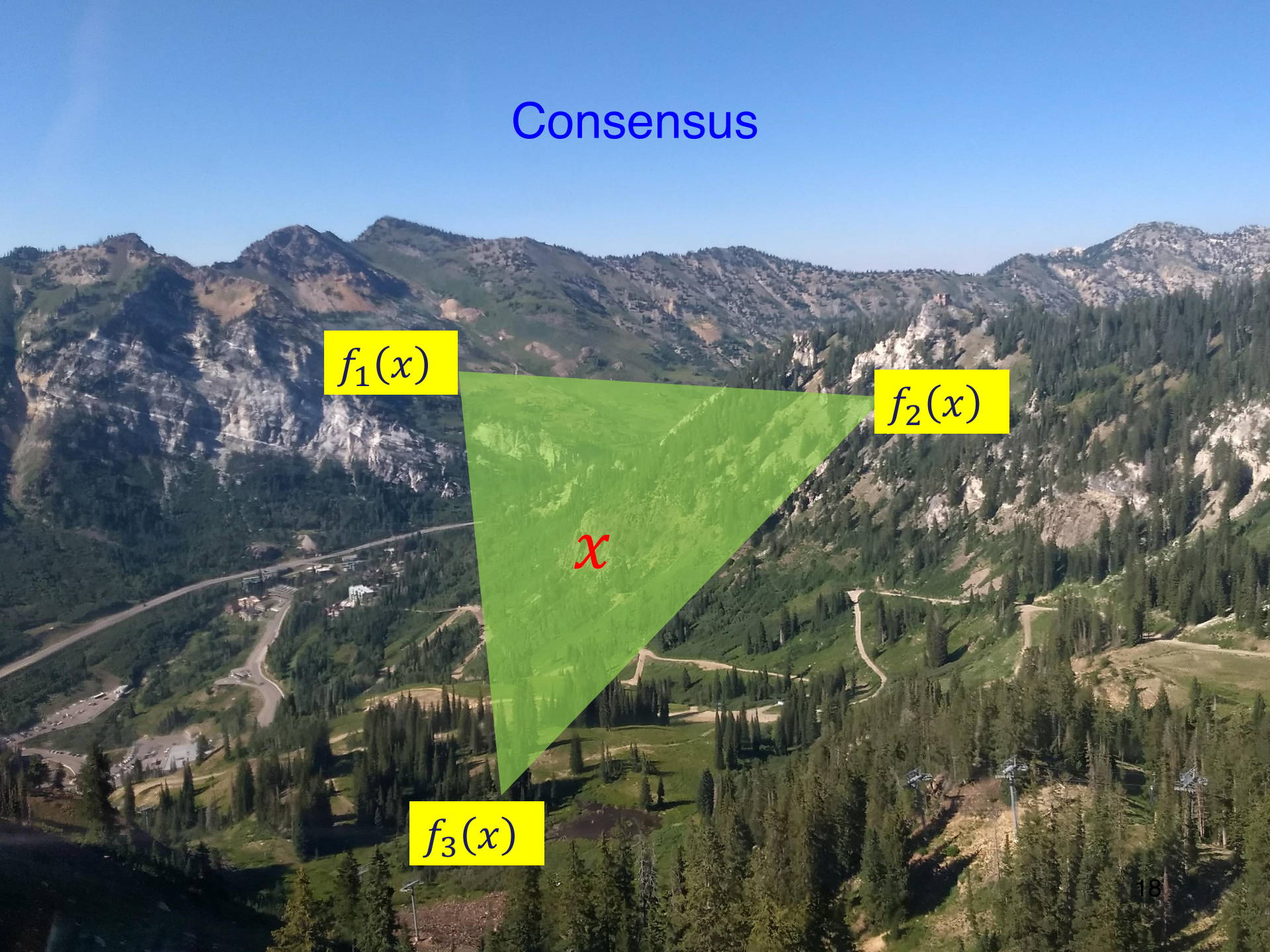
- Fault-tolerant (secure) distributed optimization

$$f_1(x) + f_2(x) + f_3(x)$$

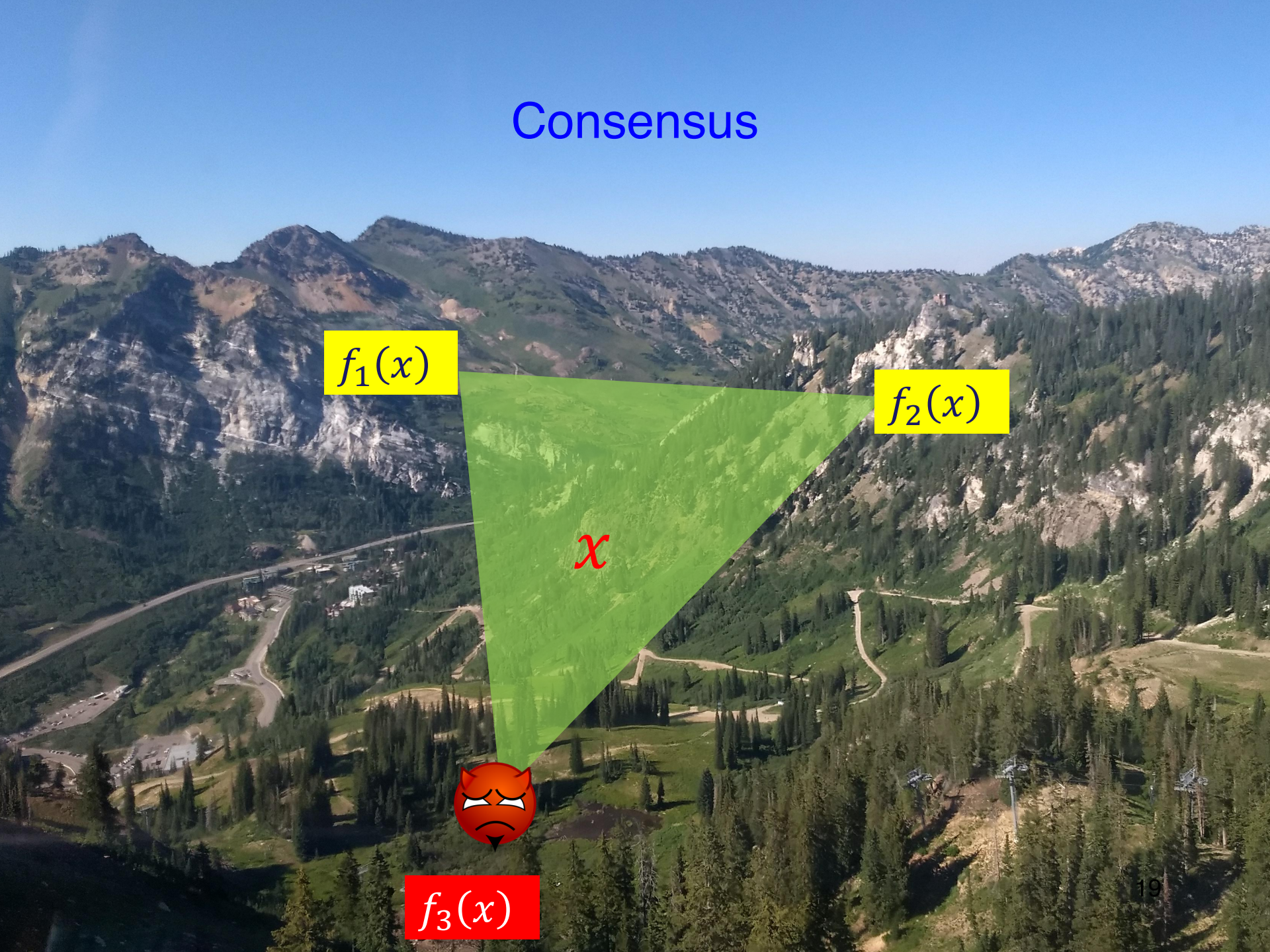


How to optimize if agents inject bogus information?

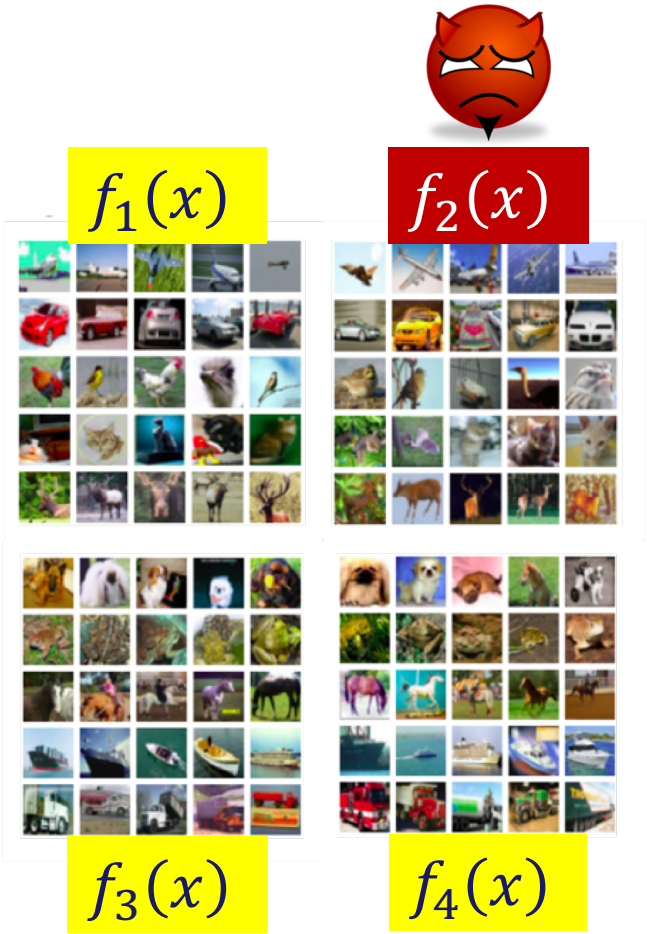
Consensus



Consensus



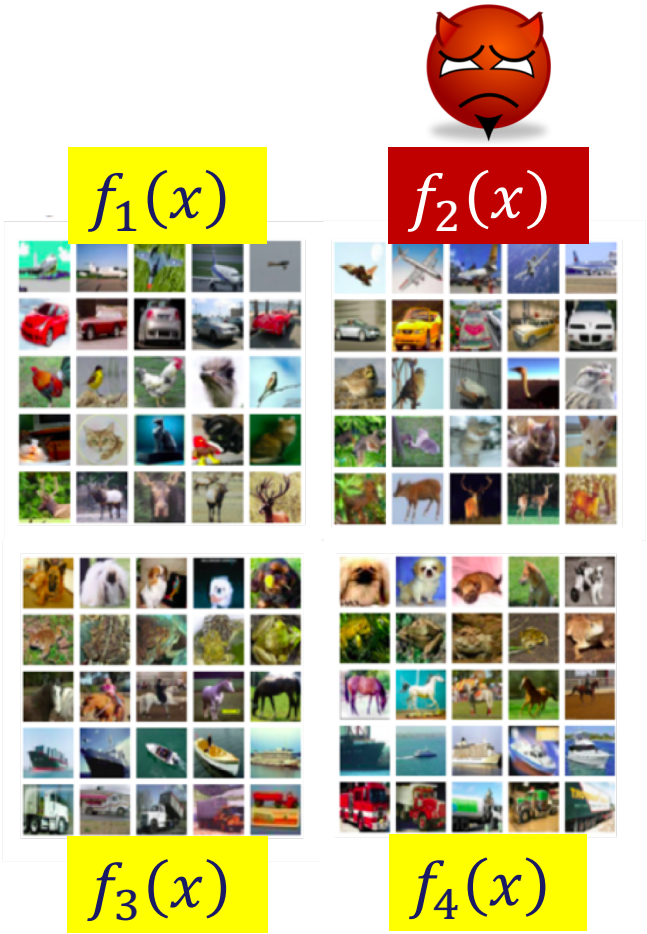
Machine Learning



Minimize global loss

$$\sum f_i(x)$$

Machine Learning



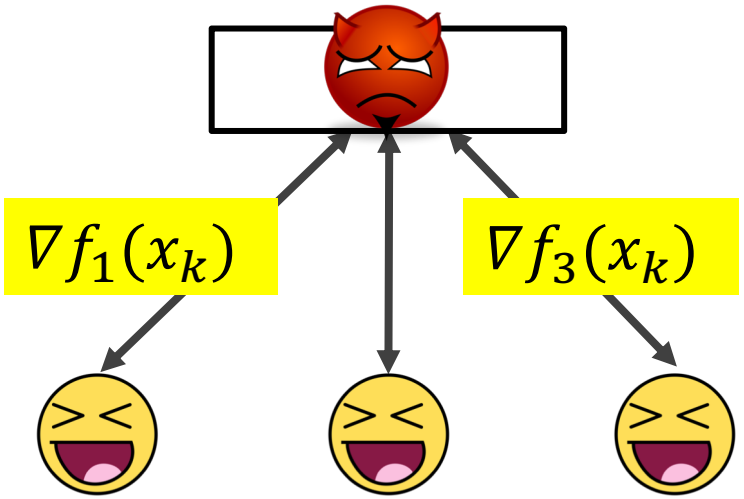
Faulty agents can adversely affect model parameters

Minimize global loss

$$\sum f_i(x)$$

Challenge #2

- Privacy-preserving distributed optimization



How to collaborate without revealing own cost function?

My Current Research

- Distributed optimization and machine learning:
  Security & Privacy
- Consistency of key-value stores
- Distributed consensus
- Graph algorithms

For More Information

https://disc.georgetown.domains

Tutorial on Security and Privacy in Distributed Optimization and Learning

(above page, go to Talks)