Applying Cryptography to Arms Control

Neil Perry

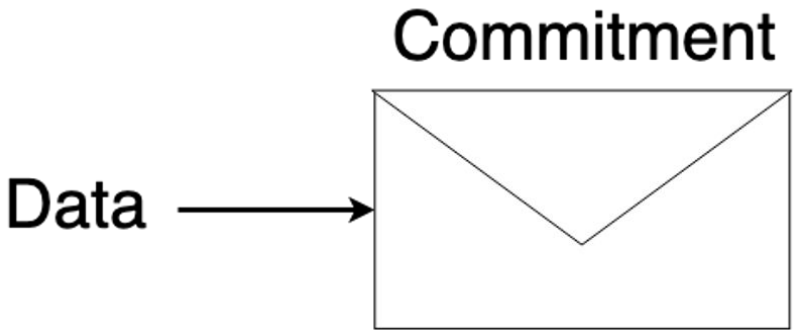
Outline

- Cryptographic Primitives
- Arms Control Principles
- Nuclear Warheads
- Biological Weapons

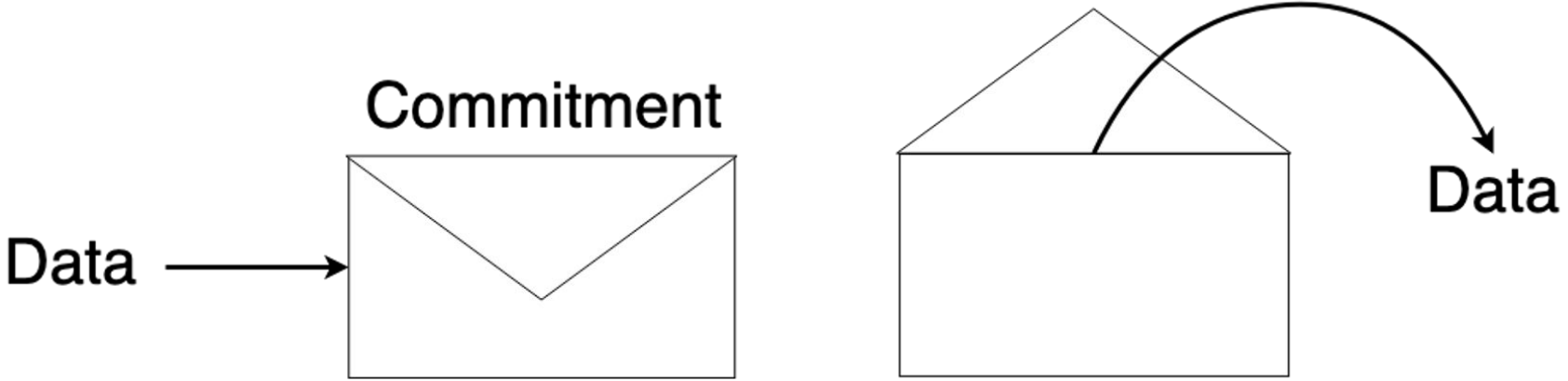
Tools We'll Be Working With

- Commitments
- Zero Knowledge Proofs
- MPC
- Blockchains

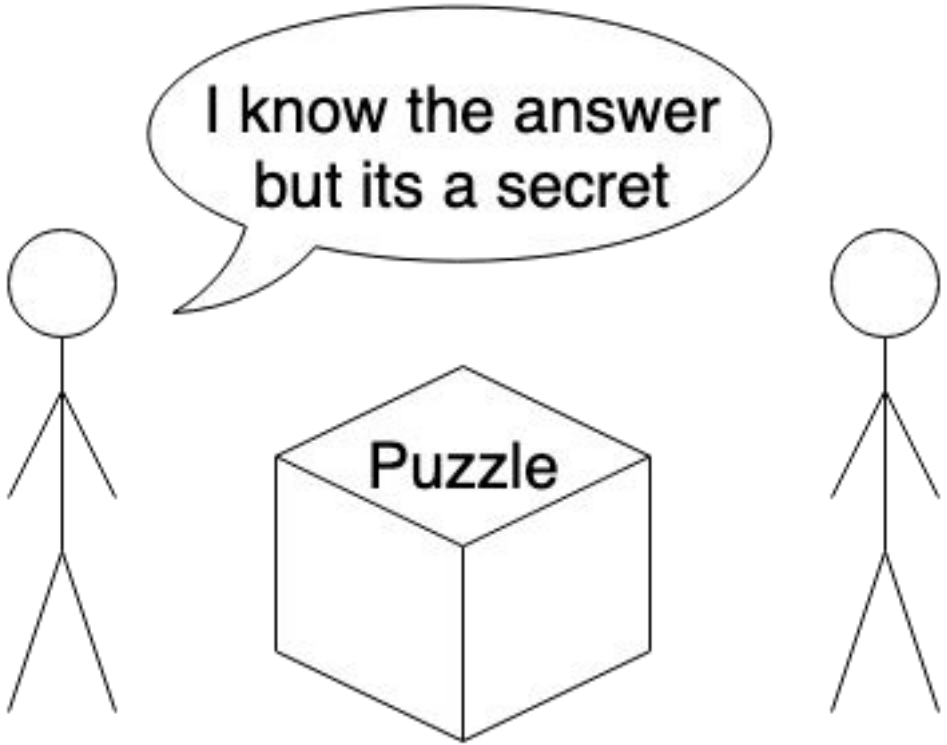
What is a commitment?



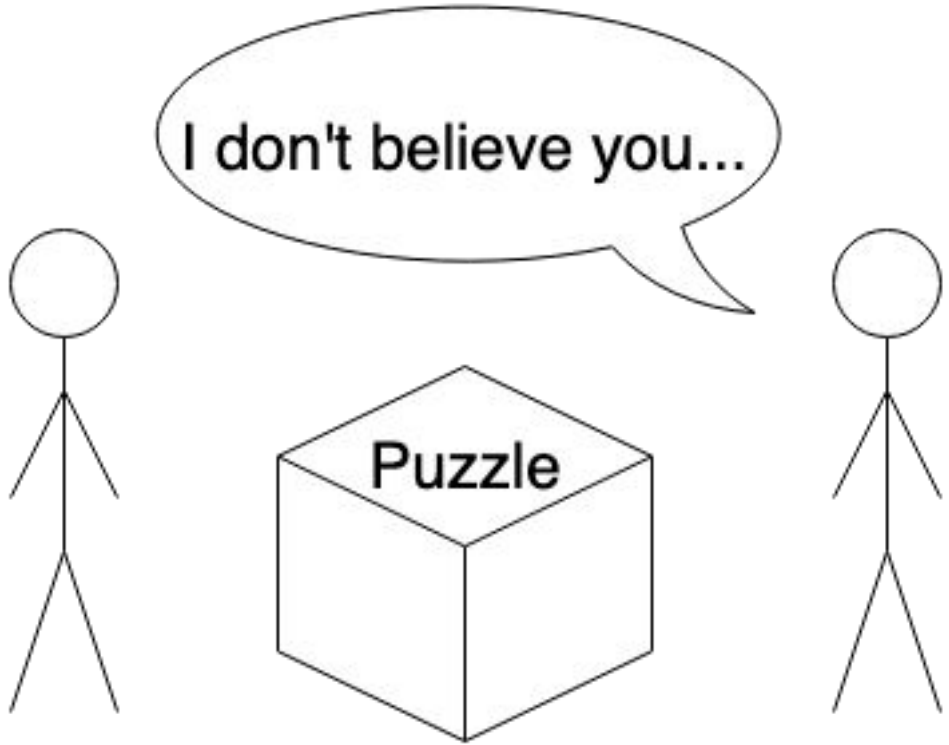
What is a commitment?



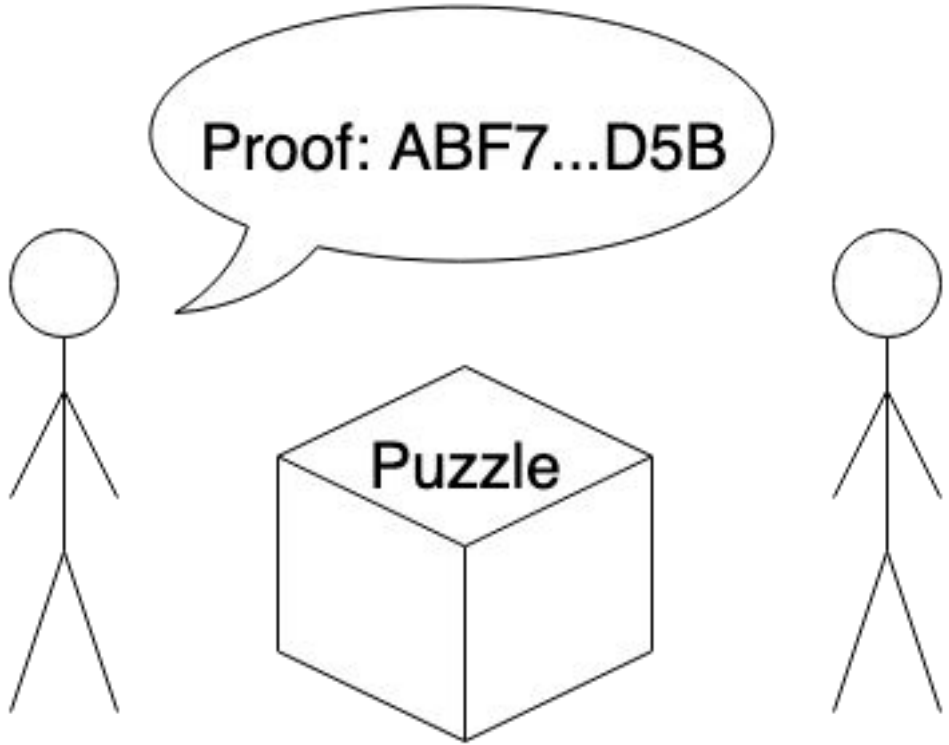
What is a Zero Knowledge Proof?



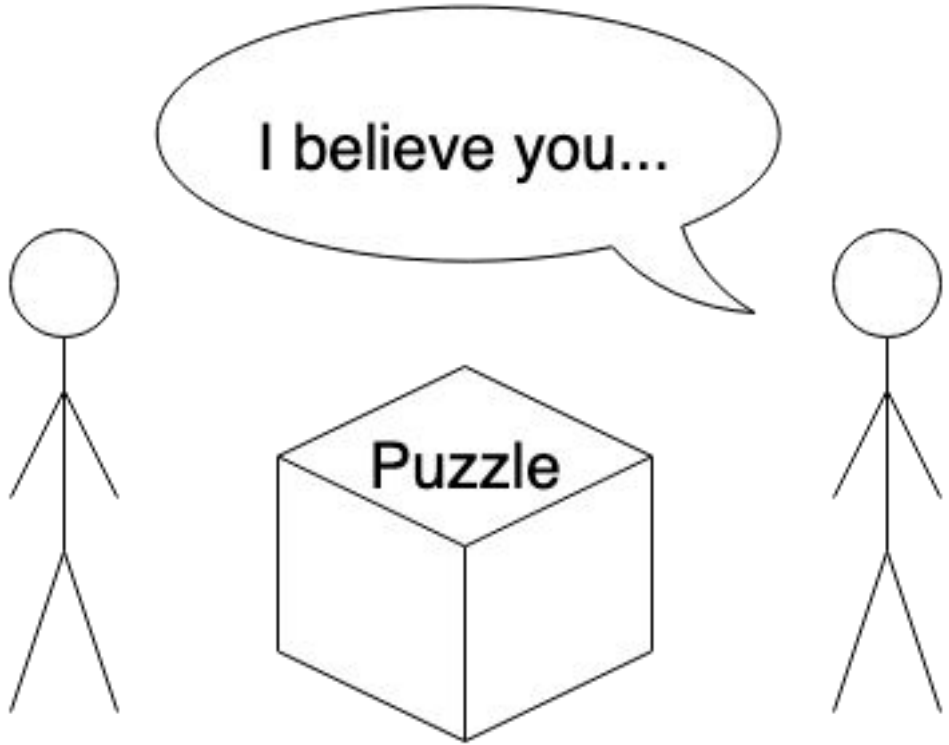
What is a Zero Knowledge Proof?



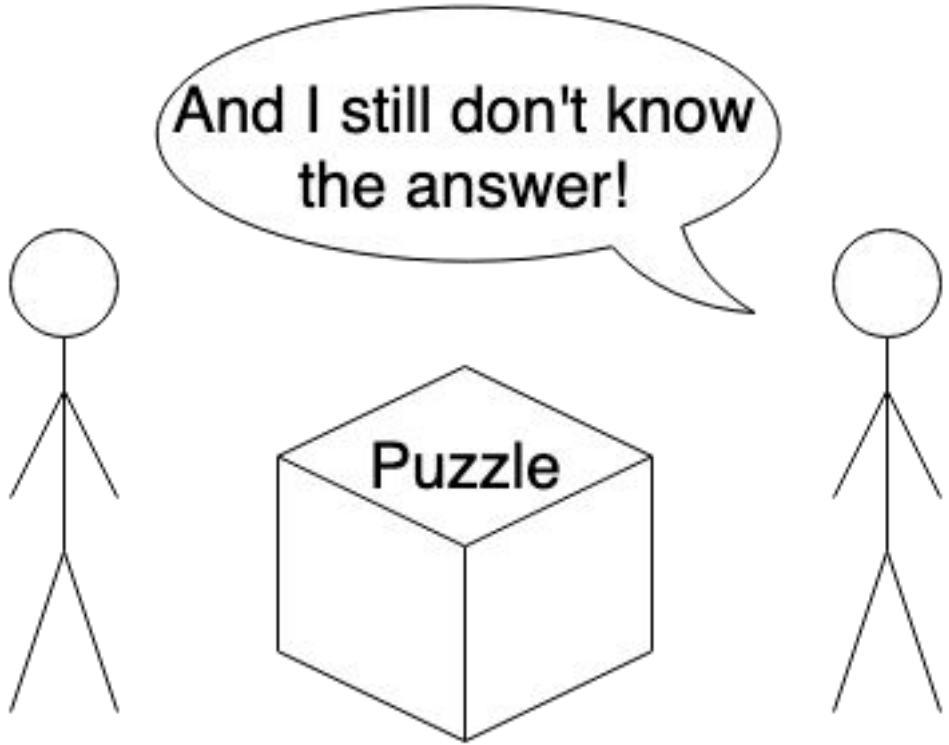
What is a Zero Knowledge Proof?



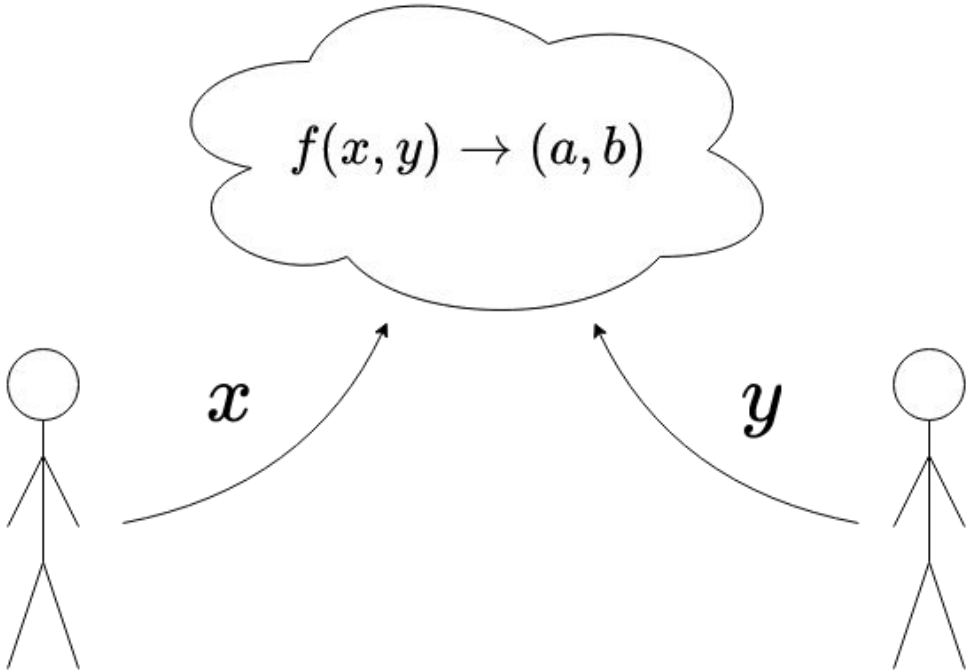
What is a Zero Knowledge Proof?



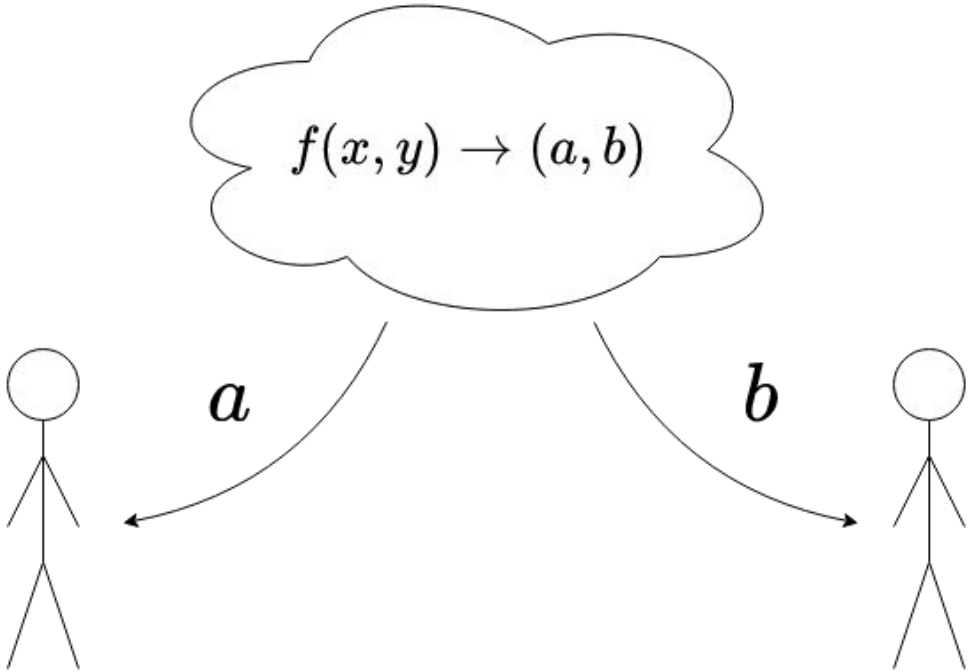
What is a Zero Knowledge Proof?



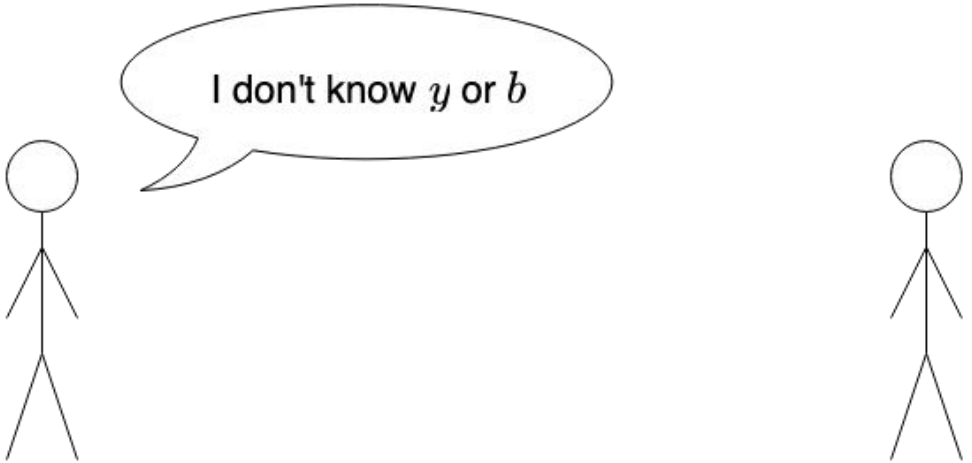
What is MPC?



What is MPC?

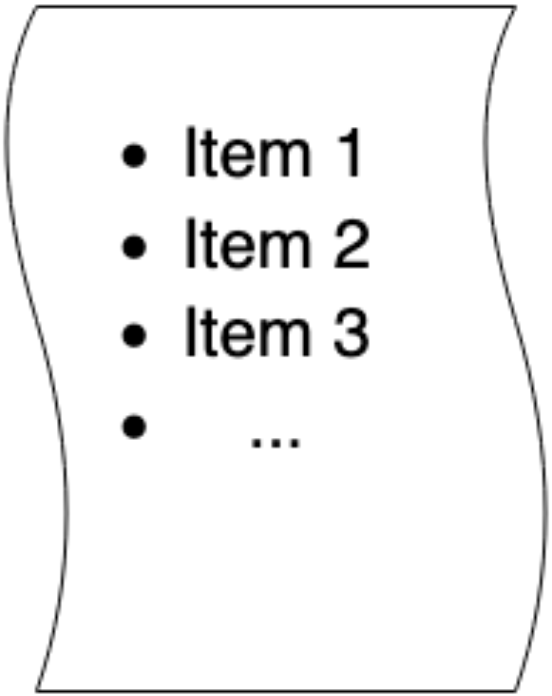


What is MPC?

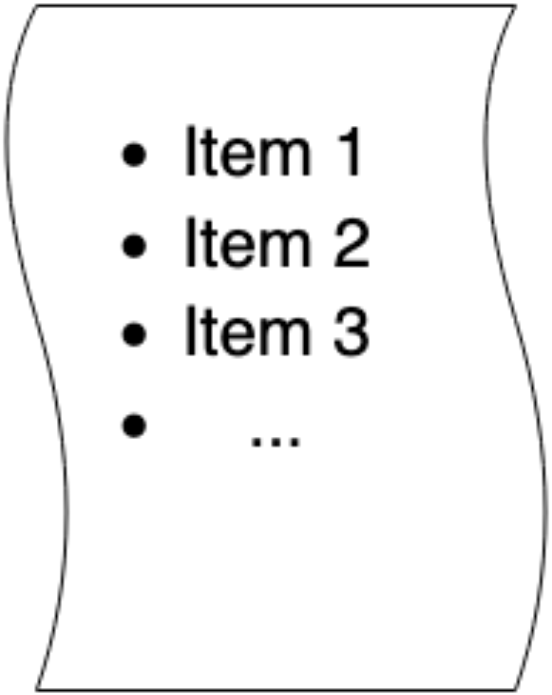


What is MPC?

What is a Blockchain?



What is a Blockchain?



Arms Control Principles

- Not looking for a magic bullet
- Layers of Defense
- Value in confidence and trust building measures
- Different WMDs have different problems

Nuclear Warhead Challenges

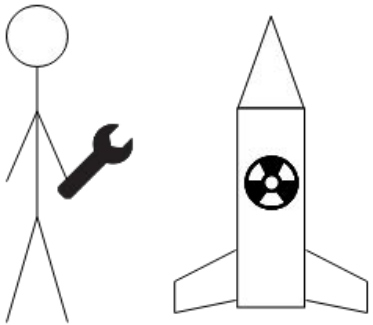
- Made up of multiple parts
- Require regular maintenance
- Frequently move
- On-site inspection is difficult
- Direct observation difficult

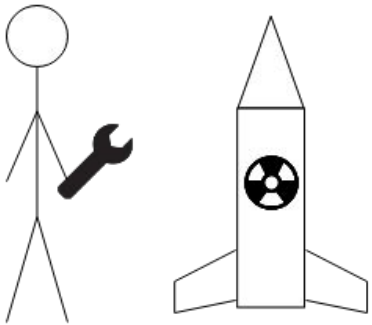
Goals

- Need to “tag” and track warheads
- Slowly reveal info to build trust
- Don’t reveal sensitive information
- Don’t create nuclear safety or security vulnerabilities
- Don’t disrupt warhead operations

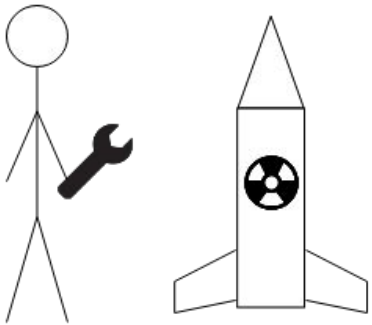
Starting Point?

- Both sides have WH databases
- We believe these DBs are accurate
- Defined locations, movements, other transactions
- Historical data not as sensitive

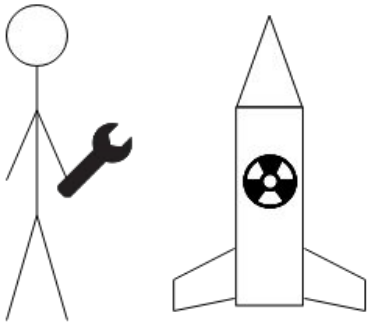




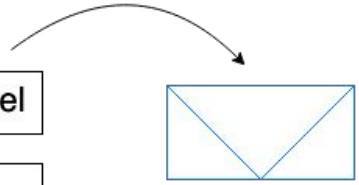
Time	Location	...	Operation	Personnel

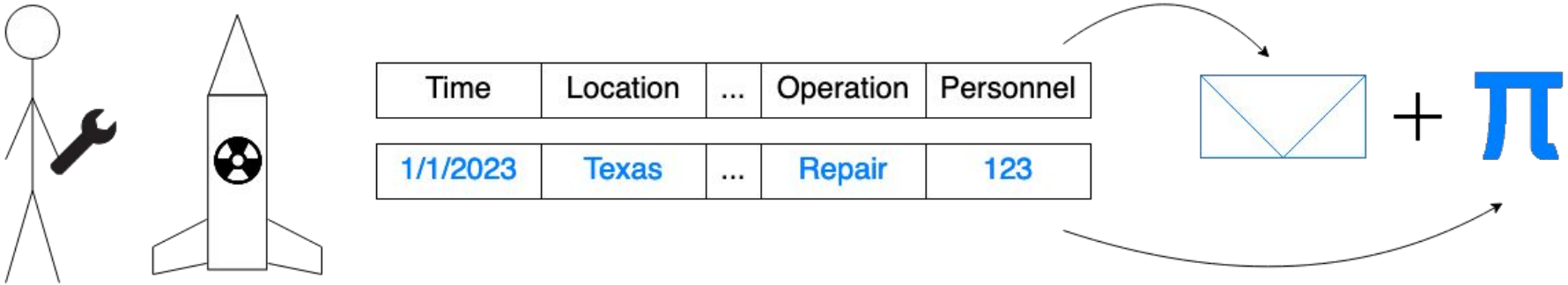


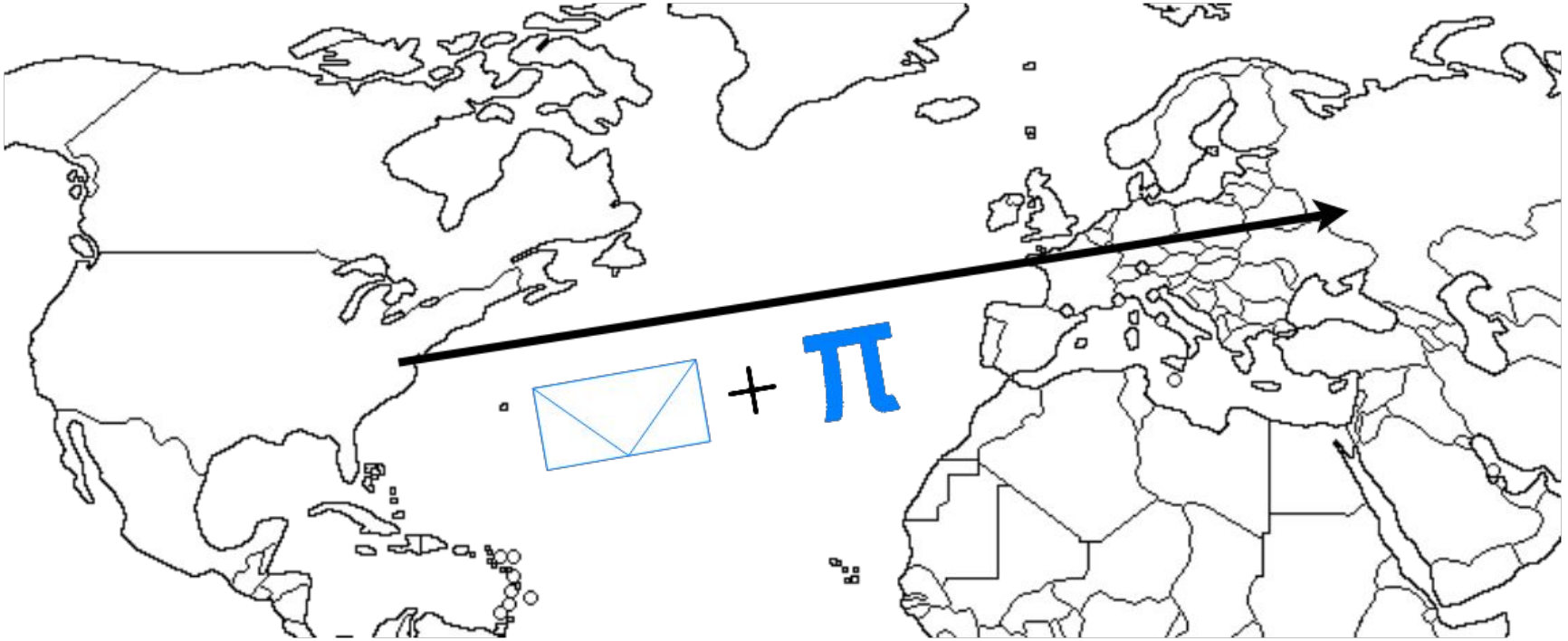
Time	Location	...	Operation	Personnel
1/1/2023	Texas	...	Repair	123

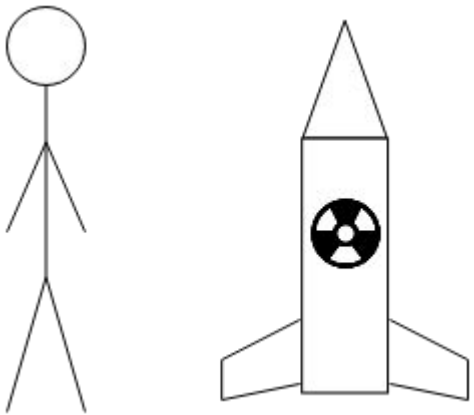


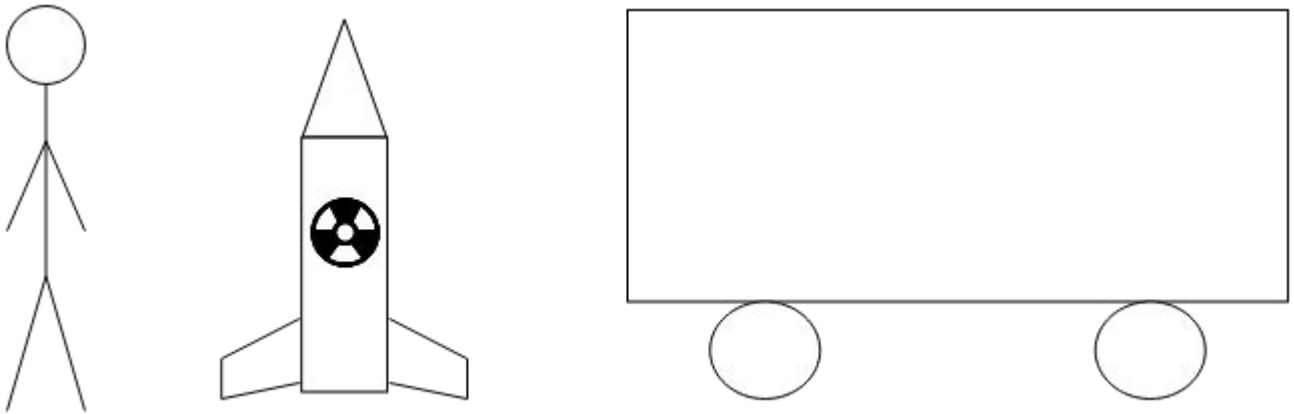
Time	Location	...	Operation	Personnel
1/1/2023	Texas	...	Repair	123

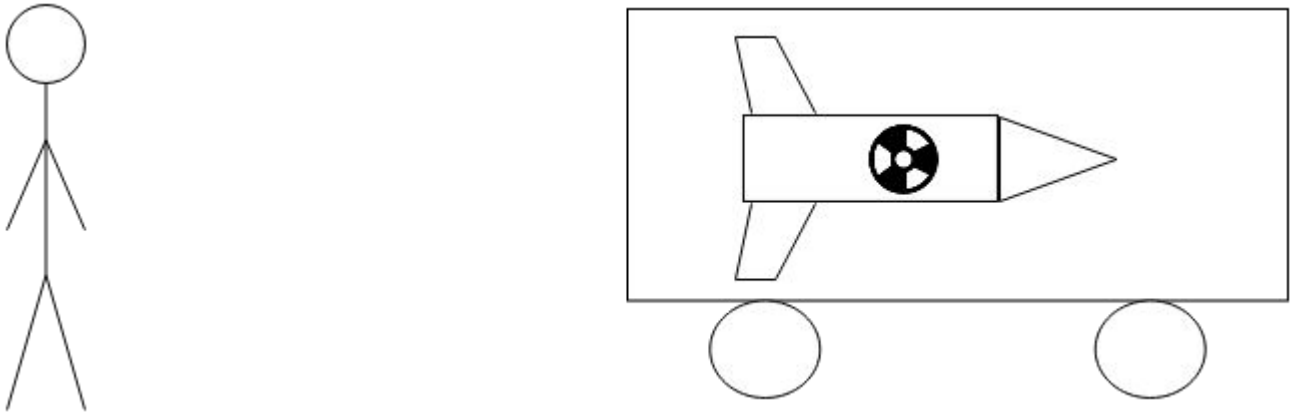


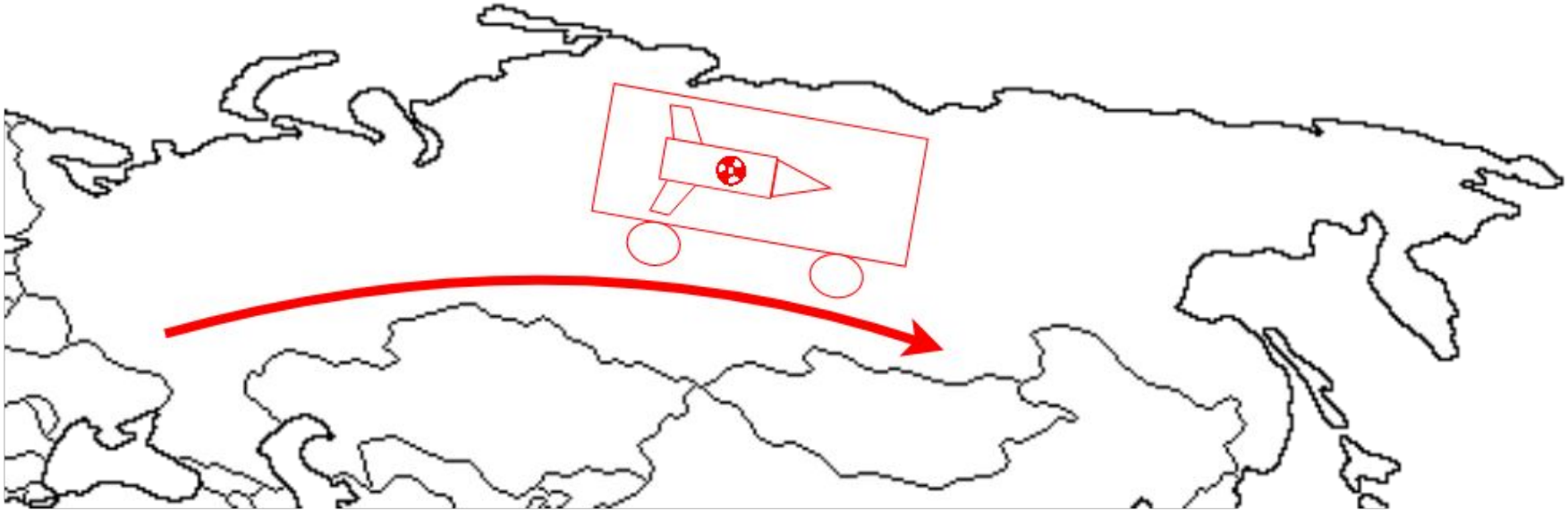

Time
Location
...
Operation
Personnel
1/1/2023
Texas
...
Repair
123

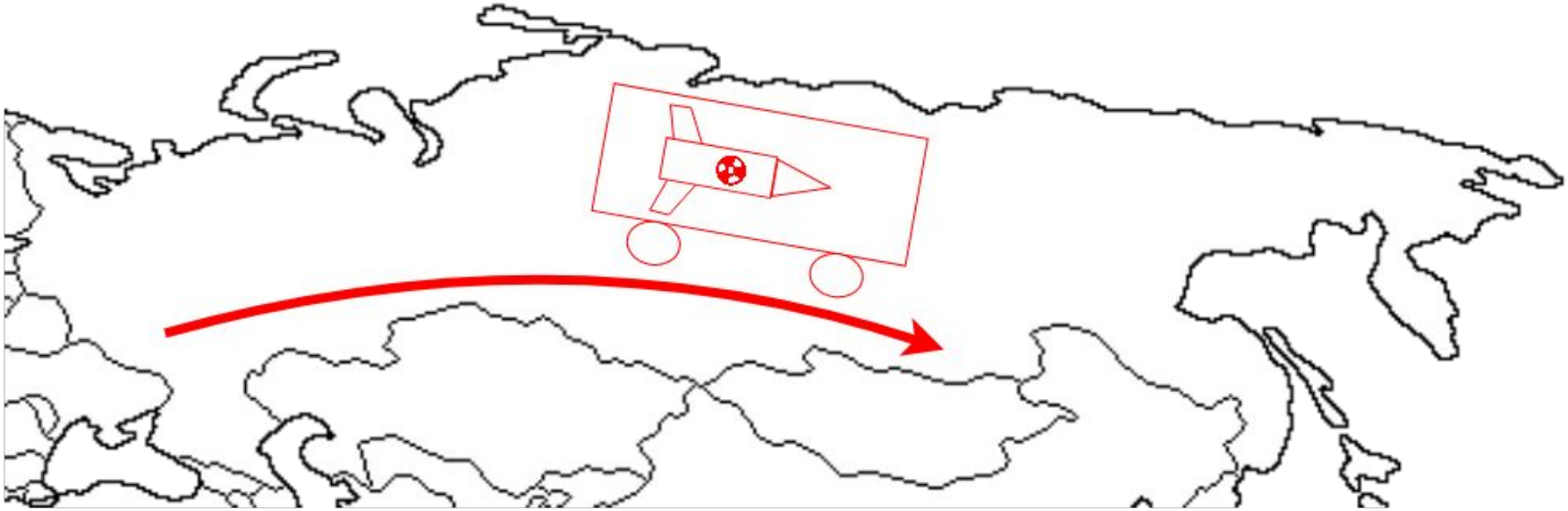




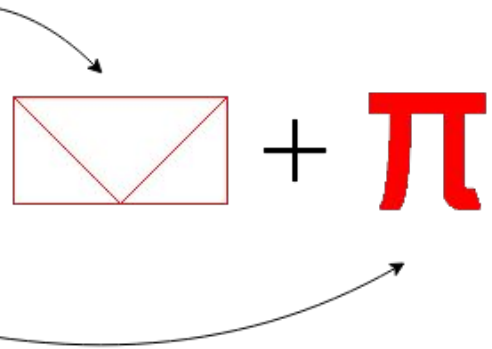


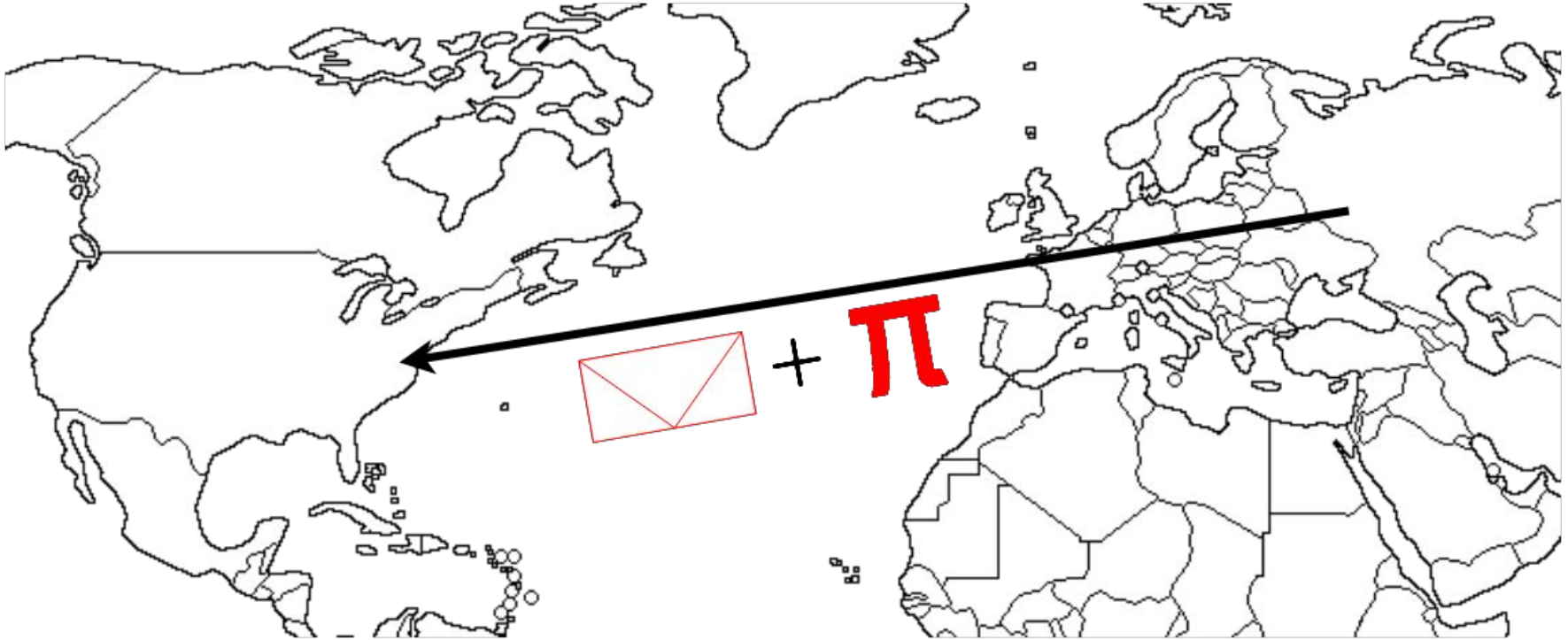




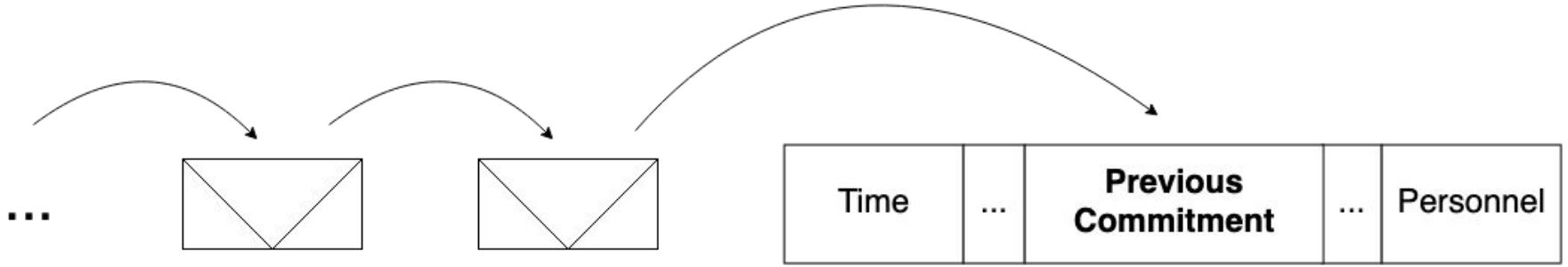


Time	Location	...	Operation	Personnel
1/2/2023	Moscow	...	Transfer	729




+
π

Linking Commitments Together



Passport

Date/Time	Location	Status	Secondary Component	Limited Lifetime Component 1	Limited Lifetime Component 2	Operation Conducted	Personnel	Previous Hash	ID Hash
11/13/2017 16:00	CAD0L	RP	S01001	LLC101001	LLC201001	R11	AD1		
11/13/2017 17:00	CAD0L	RI	S01001	LLC101001	LLC201001	R21	R63S1		
11/14/2017 13:00	WR63S	RI	S01001	LLC101001	LLC201001	R322	R63S1		
11/15/2017 20:30	WR63S	RI	S01001	LLC101001	LLC201001	R23	R631		
11/15/2017 23:30	WA63E	RI	S01001	LLC101001	LLC201001	R311	A635		
11/16/2017 02:30	WA63E	RI	S01001	LLC101001	LLC201001	R25	A637		
11/16/2017 04:30	WA63E	RA	S01001	LLC101001	LLC201001	R16	A637		
05/16/2018 08:00	WA63E	RA	S01001	LLC101001	LLC201001	R43	A632		
11/15/2018 10:00	WA63E	RA	S01001	LLC101001	LLC201001	R44	A639		
05/15/2019 09:00	WA63E	RA	S01001	LLC101001	LLC201001	R41	A633		
11/16/2019 12:00	WA63E	RA	S01001	LLC101001	LLC201002	R45	A634		
05/20/2020 08:30	WA63E	RA	S01001	LLC101001	LLC201002	R47	A632		
11/17/2020 07:15	WA63E	RA	S01001	LLC101001	LLC201002	R41	A633		
05/19/2021 15:30	WA63E	RA	S01001	LLC101001	LLC201002	R44	A638		
10/13/2021 00:00	WA63E	RI	S01001		LLC201002	R46	A633		
11/15/2021 07:15	WA63E	RR	S01001			R46	A634		
12/01/2021 05:50	WA63E	RS	S01001			R12	A632		
12/02/2021 09:00	WA63E	RS	S01001			R26	A631		
12/02/2021 12:30	WR63S	RS	S01001			R313	A631		
12/02/2021 18:00	WR63S	RS	S01001			R24	R63S1		
12/03/2021 14:00	CAD0L	RS	S01001			R321	R63S1		
12/04/2021 01:30	CAD0L	RS	S01001			R22	AD1		b'MmYwZGJjMWE2OTMwNDI2OWQ4YTJmYzgyZWQzOThiNzU1NjlhNDlkZjFmZGYzZjJkMjEyNjVjMzllNTNmZjVlMwEVr/FkZ3lqidQzevR/NRcQjTDxuuxmoxlpT5+o8/Ll'
01/03/2022 12:00	CAD0L	RD				R14	AD1	b'MmYwZGJjMWE2OTMwNDI2OWQ4YTJmYzgyZWQzOThiNzU1NjlhNDlkZjFmZGYzZjJkMjEyNjVjMzllNTNmZjVlMwEVr/FkZ3lqidQzevR/NRcQjTDxuuxmoxlpT5+o8/Ll'	b'OGEyODMyZGJlZjUxYjU1Njk5ZWNiMmFlZTQxNTRhZTFiMzViMTk4ZWZhNzgxODVhODBlMDhiM2RiYjc3NzNhYpYi5HiO9MDAzqzCaPsDpxXhSDlLtobJ+3q3vG7lJgv8'
01/05/2022 13:30	CAD0L	RM				R15	AD1	b'OGEyODMyZGJlZjUxYjU1Njk5ZWNiMmFlZTQxNTRhZTFiMzViMTk4ZWZhNzgxODVhODBlMDhiM2RiYjc3NzNhYpYi5HiO9MDAzqzCaPsDpxXhSDlLtobJ+3q3vG7lJgv8'	b'YTJhNzAwZmNkNzlhOGIzZGNlNzE0ZmZiODI0N2EwNjBlMmJkMTA0YjAzYTYxZTM2YjVjZjc3NzVmZWY0ZjRkNEZhqg+t9OrkLwR2PnXTyfmp1+/ClxbMupZmZ3K2DY/i'

Data Challenge Process

1. The host party derives a hash from a passport entry or a notification

2. The hash is committed to the observing party

3. Later, the observing party issues a data challenge for the commitment

4. The host party decommits the original passport entry or notification and shares it along with a cryptographic proof

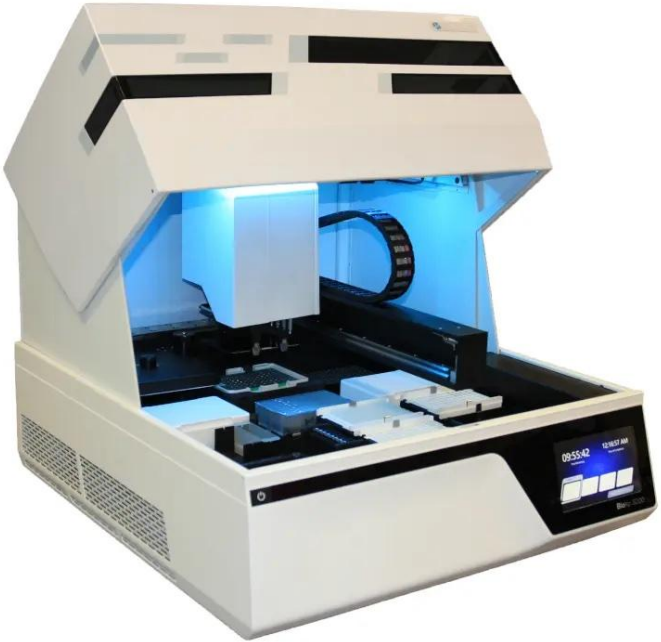
5. The observing party validates the decommitted data by using the proof to derive a hash and comparing it to the original commitment

Using Cryptography to Share Data

- Commitments create **unique identifiers** for warheads
- Allows sharing **partial** historical data
- Privately proves that treaty rules are being followed
- Updated as new events occur

DNA Printers

- Can print viruses and bacteria
- Hard to monitor
- User privacy matters



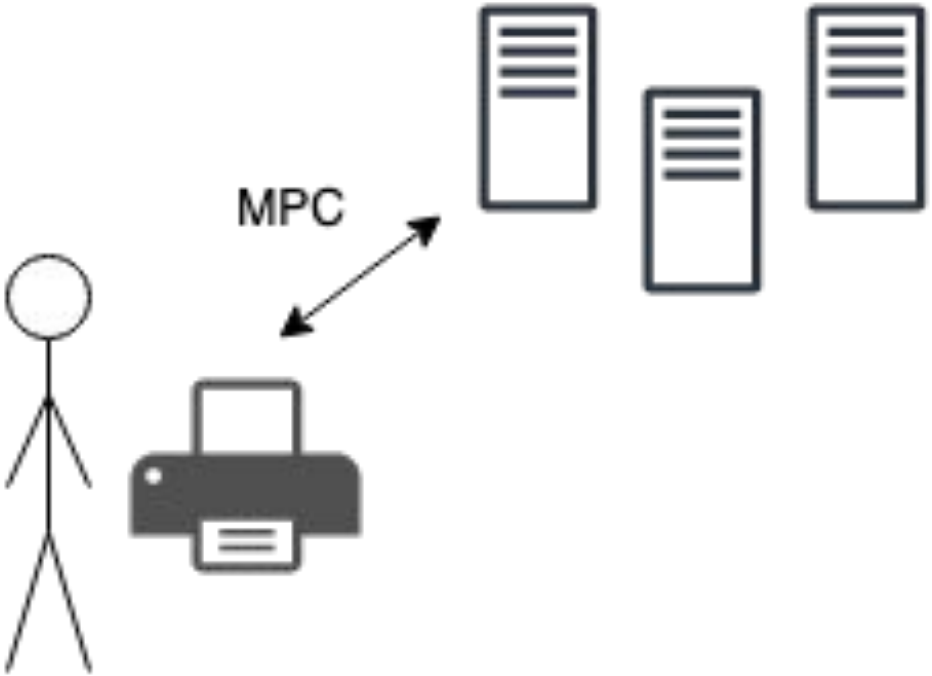
Voluntarily Proving Safety

- Lack of Regulation and Standards
- Allows for developing and testing methodology
- Build up a reputation of responsibility

Methodology

- User wants to print ATGCTT…

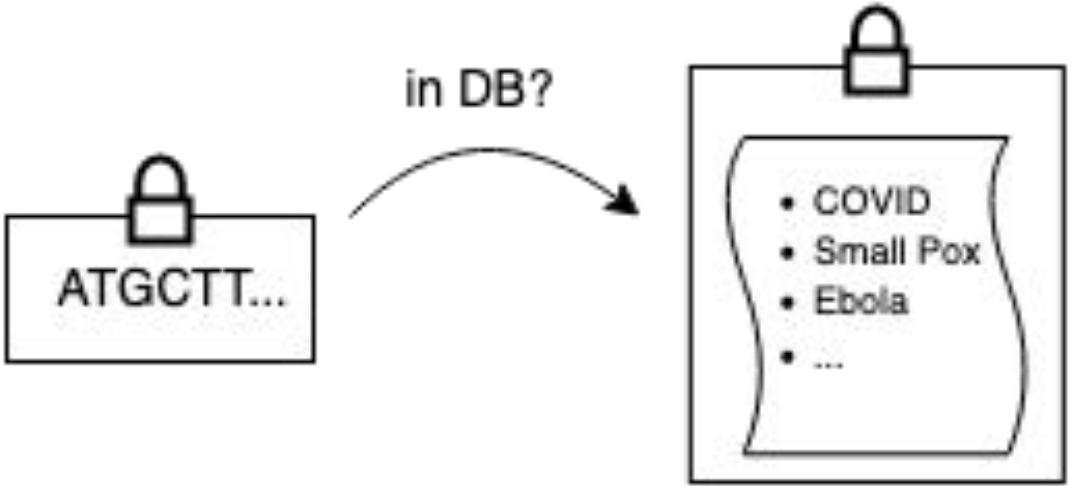
Methodology



- User wants to print ATGCTT…
- MPC to check for dangerous DNA sequences

Methodology

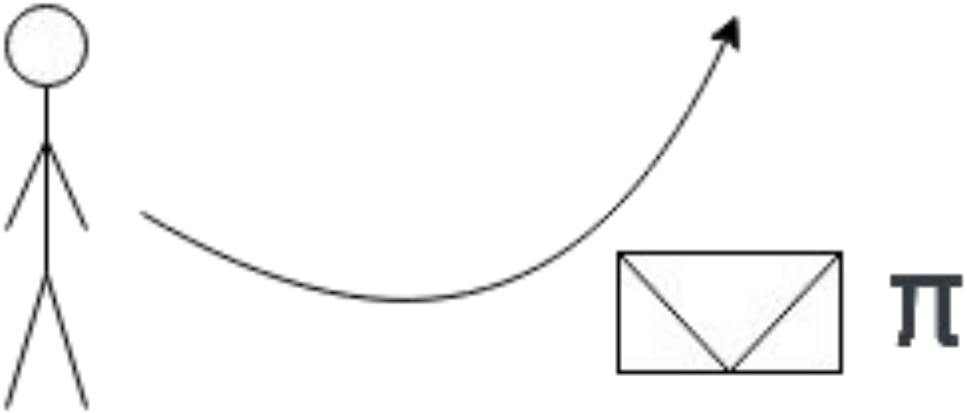
- User's sequence kept private
- Dangerous list kept private
- Sequence in list?



Methodology

- Sends proof of safety
- User can convince others

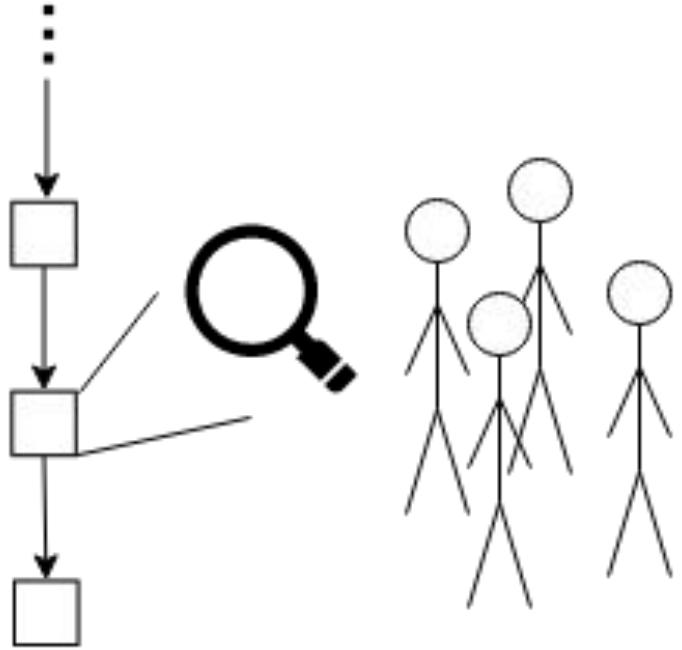
Methodology



- User posts proof and commitment to blockchain

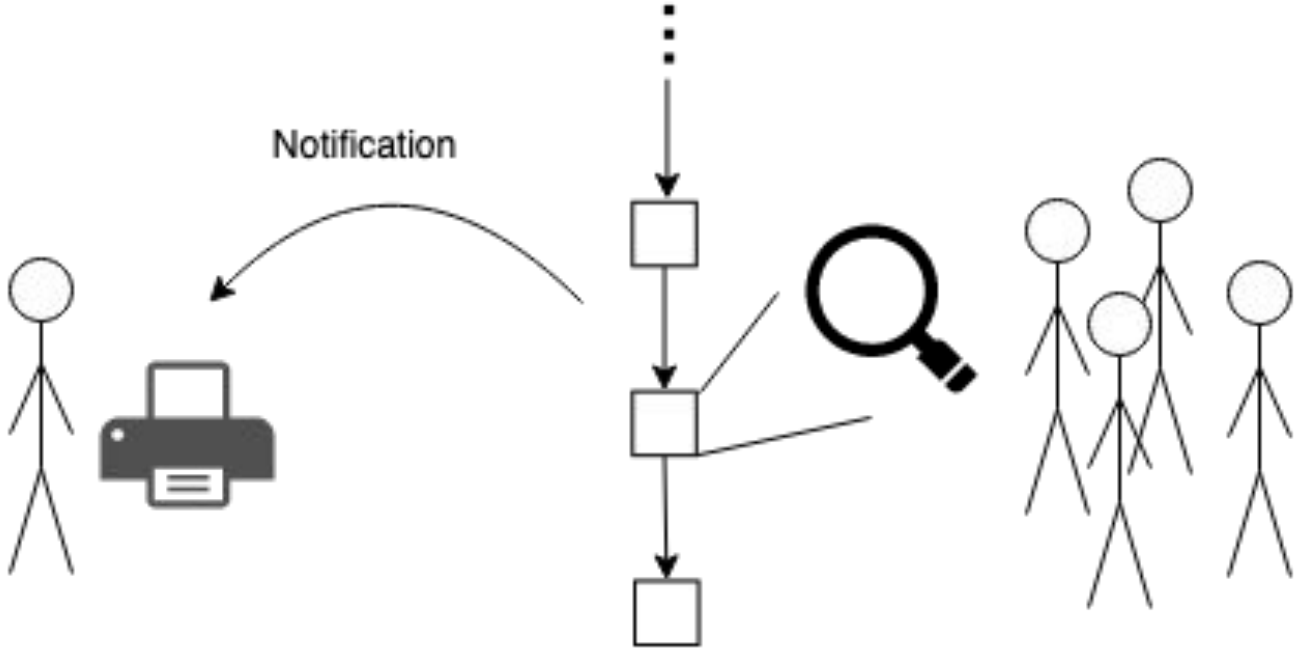
Methodology

- CDC has special permission
- Allowed to “search” a print

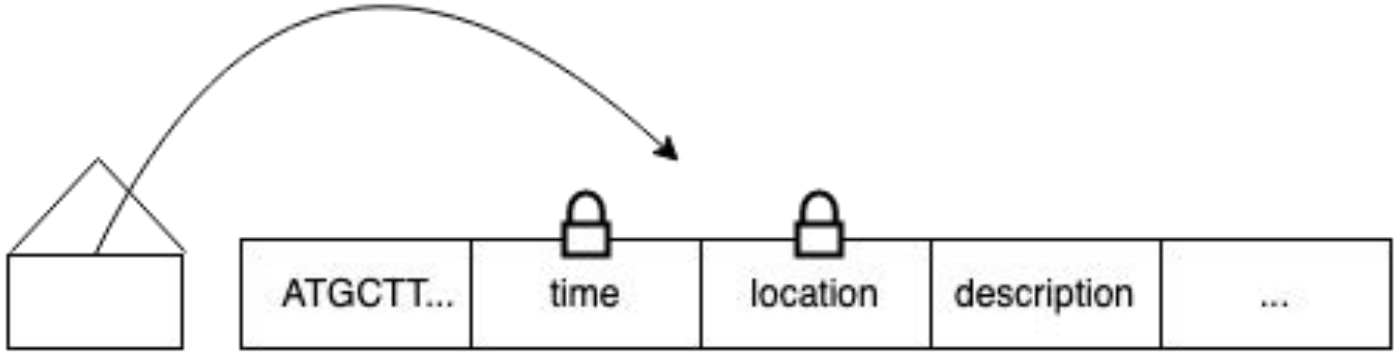


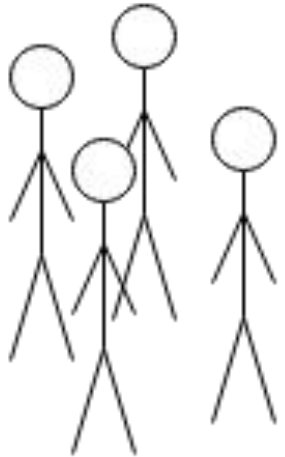
Methodology

- Automatic Search Notifications



Methodology





Key Takeaways

1. Solve important problems by combining fields
2. Ok to use black boxes
3. Focus on problems that actually matter

- Neil Perry
- naperry@stanford.edu
- LinkedIn

Links to Images Used

https://www.alternatehistory.com/wiki/lib/exe/fetch.php?media=blank_map_directory:worldv4.png
https://www.armytimes.com/resizer/OO8qGgWeXWelAzTFNxfMvS2jzkY=/1200x0/filters:quality(100)/arc-anglerfish-arc2-prod-mco.s3.amazonaws.com/public/7CN2X7EVKZAZ5FYZLC5LXYCLQY.jpg
https://novoengineering.com/wp-content/uploads/IMG_2672_800x800.jpg