This Lecture:

- Blockchain (Continued)
- Differential Privacy
- Privacy in ML
Blockchain

- Public ledger that everyone can view & verify
- Maintained by “miners” in a distributed way

**Step 1:** Charlie wants to make a transaction Charlie -> Starbucks $3
- Charlie broadcasts it to the entire network

**Step 2:** All miners collect all transactions in the network
- Verify validity
  1. Initiated by sender
  2. Enough balance in sender’s account
- Agree on next block

**Step 3:** Repeat
Byzantine Agreement

Byzantine Fault Tolerance (BFT) Protocol:

If $n \geq 3t+1$, then it's possible to reach consensus.

Assume $t < n/3$, then agree on a valid block.

Any problem?

Agree on a block

( Guaranteed Output Delivery)

Sybil Attack
Proof of Work (PoW)

Miner 1:

Hash \left( \begin{array}{c} \text{TX1} \\ \text{nonce} \end{array} \right) = 00\ldots01011\ldots0_{30}

Find nonce s.t. Hash(block) has \geq 30 leading 0's.

Consensus Protocol:

Whoever first finds a block that hashes to a value w/ \geq 30 leading 0's, that block becomes the next block.
Proof of Work (PoW)

Longest Chain Rule: Always adopt the longest chain.

Assuming honest majority of computation power, the longest chain is always valid.
Extensions

- Smart contracts
- Proof of Stake (PoS)
- Anonymous transactions (zk-SNARGs)
- Public bulletin board
Differential Privacy

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Gender</th>
<th>Race</th>
<th>Weight</th>
<th>ZIP</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emily</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fiona</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Want to make the (sensitive) data public/available to others (e.g. for medical study).

Attempt 1: "Anonymize" the data.
Delete personally identifiable information (PII): name, DOB, ...

Attempt 2: Only answer aggregate statistics queries.
Privacy Guarantee?

Access to the output shouldn't enable one to learn anything about an individual compared to one without access. With access to the output computed on a database without the individual.

Is this possible?

Privacy vs. Utility
Differential Privacy

\[ D \in \mathbb{X}^n \quad \rightarrow \quad M \quad \rightarrow \quad M(D) \]

**Def.** \( \varepsilon \)-Differential Privacy for a randomized mechanism:

\[ \forall \text{ neighboring datasets } D_1 \& D_2 \text{ (differing in one row)}, \]

\[ \forall T \subseteq \text{range}(M), \]

\[ \Pr[M(D_1) \in T] \leq e^{\varepsilon \cdot \Pr[M(D_2) \in T]} \]
Differential Privacy

Def $((\varepsilon, \delta))$-Differential Privacy for a randomized mechanism:

A neighboring datasets $D_1$ & $D_2$ (differing in one row),

$\forall T \subseteq \text{range}(M), \quad \Pr[M(D_1) \in T] \leq e^{\varepsilon} \cdot \Pr[M(D_2) \in T] + \delta$

Is a bigger $\varepsilon$ better for privacy, or worse? Worse

Is a bigger $\delta$ better for privacy, or worse? Worse
Randomized Response

Counting query: What percentage of individuals satisfy predicate $P$?

For each row $X_i$:

1. Sample $b \in \{0, 1\}$
2. If $b = 0$, then $y_i = P(x_i)$
   Otherwise, $y_i \in \{0, 1\}$

$M(D) = (y_1, y_2, \ldots, y_n)$

Thm Randomized Response is $\ln 3$-DP.

How to make the mechanism more private? Flip a biased coin in 1.

How to estimate the query output?

$E[\#1's] = \frac{1}{2} \cdot \alpha \cdot N + \frac{1}{2} \cdot \frac{1}{\alpha} \cdot N \approx \frac{k}{N}$
Laplace Mechanism

Def. Sensitivity of a function \( f: X^n \rightarrow R \)

\[ \Delta f := \max_{D_1 \sim D_2} \left| f(D_1) - f(D_2) \right| \]

Laplace Mechanism: \( M(D) = f(D) + \text{Lap}(\Delta f/\varepsilon) \)

Thm. The Laplace Mechanism is \( \varepsilon \)-DP.

Laplace distribution:

\( \text{Lap}(b) : \)

PDF(\( x \)) = \( \frac{1}{2b} \cdot \exp(-\frac{|x|}{b}) \)

For \( X \sim \text{Lap}(b) \), \( \Pr[|X| \geq bt] \leq \exp(-t) \)

Is a bigger \( b \) better for privacy, or worse? **Better**
Composition Theorems

Thm (post-processing) If \( M : X^n \to Y \) is \((\varepsilon, \delta)\)-DP,\[ f : Y \to Z \text{ is an arbitrary randomized function,} \]
then \( f \circ M : X^n \to Z \) is also \((\varepsilon, \delta)\)-DP.

Thm (group privacy) If \( M : X^n \to Y \) is \((\varepsilon, 0)\)-DP,\[ \text{then } M \text{ is } (k \cdot \varepsilon, 0)\)-DP for groups of size \( k \).

Thm (composition) If \( M_i : X^n \to Y \) is \((\varepsilon_i, \delta_i)\)-DP \( \forall i \in [k], \)
then \( M(D) := (M_1(D), \ldots, M_k(D)) \) is \((\sum_{i \in [k]} \varepsilon_i, \sum_{i \in [k]} \delta_i)\)-DP.
Privacy in ML

Each node in hidden layers: \textit{linear function} + \textit{activation function}

Data points \((\tilde{x}_i, y_i)\)
ML model: weights \(\tilde{w}\)
Loss function \(L_i(\tilde{w})\)

\text{Stochastic Gradient Descent (SGD)}:
- \(\tilde{w}\) initialized randomly
- Each iteration:
\[
\tilde{w} \leftarrow \tilde{w} - \eta \cdot \nabla L_i(\tilde{w})
\]
\[
\tilde{w} \leftarrow \tilde{w} - \frac{\eta}{B} \sum_{i \in [B]} \nabla L_i(\tilde{w})
\]
Privacy in ML

Server

⇒ ML model

· Does the model (updates) contain private information?

· Secure inference / training?

· Data deletion from trained model?