Alright, well they say save the best for the last but after hearing everyone else’s presentations, I think this will run contrary to that saying. Well, we’ve made it and the only thing in the way of ending this semester is our presentation, so I want to thank Prof. and all our classmates for holding your attention for a few minutes longer.

On behalf of myself, An, and Jodi, I’ll be presenting our term project on GDPR Compliant Public Blockchain using AI Smart Contracts. That was a mouthful, so I hope to share enough information so that everyone has an understanding of the problem, the solution, current research, our novel approach, and a workflow of our conceptual smart contract API.

<change to slide 2>

If the internet is accurate, we’re currently in the fourth industrial revolution led by innovations and emerging breakthroughs in robotics, artificial intelligence, nanotechnology, quantum computing, IoT, to name a few. And as much as all these will require electricity to power them, it’ll also include something that is just as important: Personal Data of Individuals.

As we have studied, learned, and heard this semester…security threats are pervasive, and attempts occur every second of each day. Adversaries are inventing smarter ways to gain unauthorized access to computers, networks, governments, and businesses – whether for personal gain or disruptive purposes. The protection of every individual’s personal data has been headlined due to data/security breaches at businesses such as Yahoo, Marriott, Adult Friend Finder, Target.

Thanks to Ananth and Quentin last week, we should all have exposure to GDPR – General Data Protection Regulation and Blockchain.

Our research focuses on providing a conceptual design with the goal of protecting user data while leveraging emerging technology breakthroughs satisfying GDPR while leveraging blockchain, AI, and Smart Contracts. Although GDPR only affects EU residents, businesses, or any foreign businesses holding EU resident’s personal data – US is already working a similar legislation called the American Data Dissemination Act.

<change to slide 3>

Let’s start with the PROBLEM. Protecting Personal Data is difficult and costly. GDPR could fine 20 million Euros or 4% of violator’s annual revenue. We believe Blockchain could be a solution with its security and decentralization features. After much research, we concluded (as well as many peers) that blockchain in its current form is not GDPR compliant as it violates Art. 17 “Right to be forgotten and functioning principle.”

<change to slide 4>

Our proposed solution is adding Artificial Intelligence and Smart Contracts to a public Blockchain. Let’s refer briefly to the diagram to get a high-level of our concept.

1. Personal Data is stored on the public blockchain. Each ledger/block can represent an individual’s personal data or different tiers of personal data
2. Local Storage are businesses, governments, entities getting copies of personal data
3. AI and Smart Contracts work in tantum
4. All this is decentralized on the network without requiring 3rd party intervention

<change to slide 5>

You’ve heard me refer to PUBLIC blockchain. I wanted to spend a minute explaining the various types of blockchain and what is the majority of current research on blockchain and GDPR compliant.

1. PUBLIC – Fully Decentralized and Secure. Everyone can read, write, and send transactions. Very much collaborative process.
2. PRIVATE – Not Decentralized. Writing permissions are centralized – usually within an organization or business. Owner essentially has exclusive right to make any changes and read rights could be open or limited.
3. HYBRID – Partially Decentralized. In this case a Public and Private blockchain are linked. Majority of current research on GDPR and Blockchain is centered around this type. Basically, store personal data on a private blockchain where the owner can make changes or deletes when requested while linking reference hashes on the public blockchain.

The main issue both private and hybrid blockchains marginalizes the security and decentralization features of blockchain technology. It does not solve the problem at hand but instead finds a work around. Our novel approach looks to be a complete GDPR compliant public blockchain solution.

<change to slide 6>

So let’s dig into our novel idea – combining Smart Contracts and Artificial Intelligence on a Public Blockchain giving individual’s full rights to their data, educating users on who has their data, and possibly creating a compensation system for both parties involved.

Smart Contracts are very much in the same vein as a traditional contract with one big difference, there is no 3rd party enforcing the terms of the contract. Instead, a Smart Contract is a computer program with conditions written in to trigger certain actions.

Artificial Intelligence is than added and parameters inserted provided into the Smart Contract along with each user’s selected conditions. An example of these parameters could be response variables from regressions on a requesting entity’s trustworthiness/risk factors – an index of some sort where a user can dictate only those having 80% or higher can have access to their information. Or AI could decide for the user which classification of entities are allowed to have access to various tiers of personal data.

Effectively, the end result is personal data is controlled fully by each individual while providing an audit trail of entities who have copies of the personal data.

<change to slide 7>

Let’s spend a moment walking through the Smart Contract Workflow:

1. Pre-defined contract: A Web or Mobile Application will provide a form for users to provide their personal information (i.e. full name, address, employment, marital status, income history, DL, SSN, Passport, Birth Date, etc…). User’s would than stratify their personal information into 3 tiers. Each Tier will have with its own contract conditions on who can read the information and/or actions that can be performed. Artificial Intelligence would provide various scores which than can be added to the conditions. Set values/compensation for each tier of information.
2. Once set, APIs would control the traffic of information between users and requesting entities. These events would be triggered based on the conditions determined by each user.
3. In order for the transaction to occur, both parties must have cryptowallets with balances to execute the requests – at which value is transferred between the parties.
4. Once confirmation is received that the action has been completed, the entities receives a copy of the user’s data and the user than gets compensated via a digital asset or in some cases, physical assets as well.

Entities themselves will also have smart contracts setting conditions on the users they want personal data access. Set values for actions such as personal information updates and/or deletion. In order for user’s to have full rights, entities must comply to requested actions. Fortunately, this is all automated and decentralized on the public blockchain so fraud or misuse can be found quickly – which would cancel the actions without the entities or user’s having to be notified.

A blockchain platforms with smart contracts could be Etheruem or a few others built of Etheruem’s ERC20 token. Cortex is another that is a decentralized AI platform that supports both SC and AI.

<change to slide 8>

In the coming years, we suspect more breakthroughs will occur in the field of blockchain and more use cases will lead to more adoption. It is certain the security and protection of personal data will continue to be a pressing matter. More innovation and novel ideas will be required to reach the goal of a fully decentralize method for user’s to have full control of their digital information.

Specifically, in our area of research – we do believe a public blockchain will in due time be a solution that is GDPR compliant that can automate the distribution, security, and enforcement of compensation for the next industrial revolution.

Thank you again for your time. This was an entire new field/topic for all three of us and learning more about it provided an excellent opportunity to round out our semester of security.

Any questions?