AMAN LADIA'S

Research Portfolio

In today's world where data is the new oil, privacy poses a formidable challenge to growth. I have spent the past four years trying to pioneer 'PrivTech': research that guarantees privacy as a fundamental right. The fourth paper is separate from this theme, focussing on a mechanical engineering solution.

1. ZeroWallet: Zero Knowledge Proofs Based Protocol to Secure Private Keys with Low-entropy Passwords

2. Privacy Centric Collaborative Machine Learning Model Training via Blockchain

3. Blockchain: A Privacy Centered Standard for Corporate Compliance

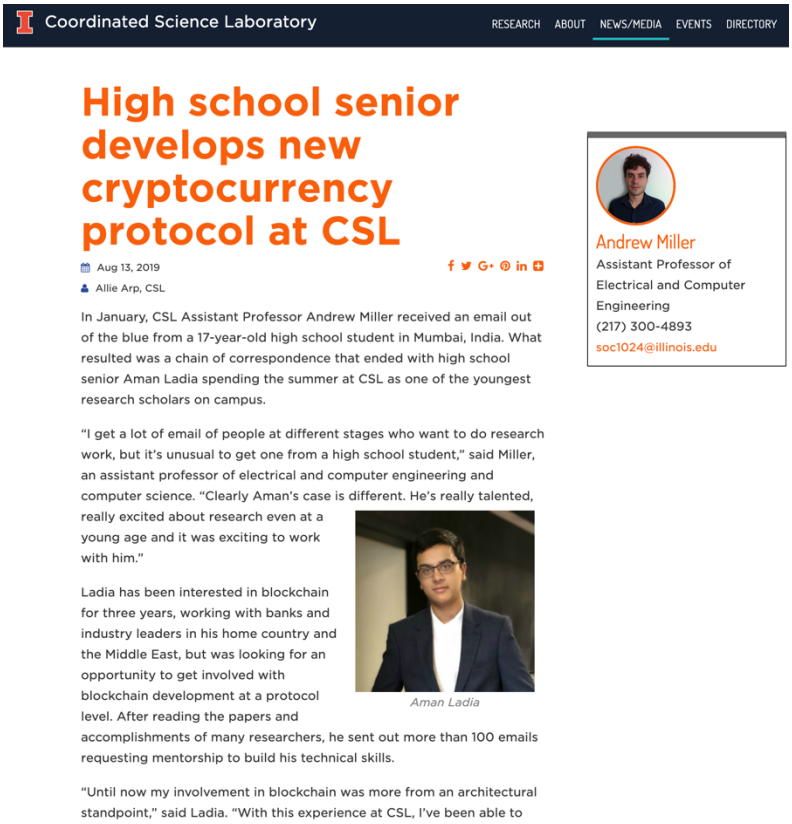
4. Mechanical Ramp Attachment for Wheelchairs to Climb Footpaths and Elevated Surfaces

ZeroWallet: Zero Knowledge Proofs Based Protocol to Secure Private Keys with Low-entropy Passwords

Introduction. ZeroWallet is a cryptographic protocol designed to provide the convenience of brain wallets with a security guarantee comparable to third party multi-sig setups. It provides a novel non-custodial method of deriving private keys from passwords whilst ensuring brute force resistance. ZeroWallet relies on an Oblivious Pseudo Random Function (OPRFs) that is derived from the OPAQUE password authenticated key exchange protocol to ensure that clients never see the server key (a salt) while the server never sees the client's passwords. Through an incorporated 2,3 threshold secret sharing scheme, the protocol also allows for private key recovery even in the absence of server interaction. ZeroWallet is implemented on Elliptic Curve Cryptography (ECC) and a fully functional public demo is available at https://app.zerowallet.me.

Key Words: password derived keys, multisig, oblivious transfer

The ZeroWallet protocol was developed by me with **Dr Andrew Miller, Asst. Professor of ECE** at University of Illinois, Urbana-Champaign (UIUC). The protocol is completely open source, with the code & documentation available at https://github.com/amsee01/ZeroWallet. The project page is http://zerowallet.me. ZeroWallet has now been **nominated for a ZCash Foundation Grant** and will likely be included as part of a ZCash Improvement Proposal (ZIP). See the coverage by UIUC at https://csl.illinois.edu/news/high-school-senior-develops-new-cryptocurrency-protocol-csl and the Initiative for Cryptocurrencies & Contracts (IC3) at https://www.initc3.org/blogs.html.



Coordinated Science Laboratory

RESEARCH ABOUT NEWS/MEDIA EVENTS DIRECTORY

High school senior develops new cryptocurrency protocol at CSL

Aug 13, 2019

Allie Arp, CSL

In January, CSL Assistant Professor Andrew Miller received an email out of the blue from a 17-year-old high school student in Mumbai, India. What resulted was a chain of correspondence that ended with high school senior Aman Ladia spending the summer at CSL as one of the youngest research scholars on campus.

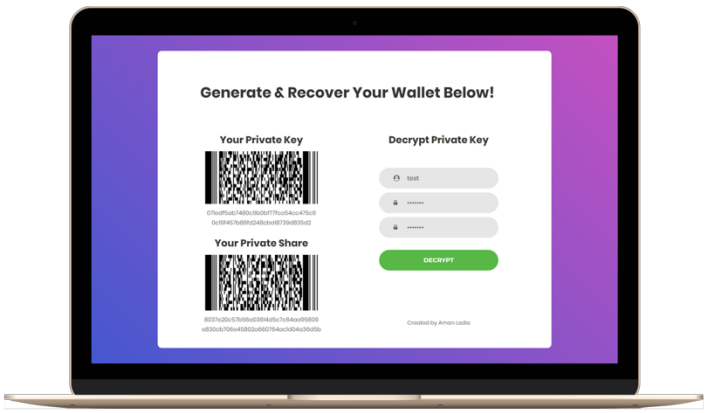
"I get a lot of email of people at different stages who want to do research work, but it's unusual to get one from a high school student," said Miller, an assistant professor of electrical and computer engineering and computer science. "Clearly Aman's case is different. He's really talented, really excited about research even at a young age and it was exciting to work with him."

Aman Ladia

Ladia has been interested in blockchain for three years, working with banks and industry leaders in his home country and the Middle East, but was looking for an opportunity to get involved with blockchain development at a protocol level. After reading the papers and accomplishments of many researchers, he sent out more than 100 emails requesting mentorship to build his technical skills.

"Until now my involvement in blockchain was more from an architectural standpoint," said Ladia. "With this experience at CSL, I've been able to

Andrew Miller
Assistant Professor of Electrical and Computer Engineering
(217) 300-4893
soc1024@illinois.edu

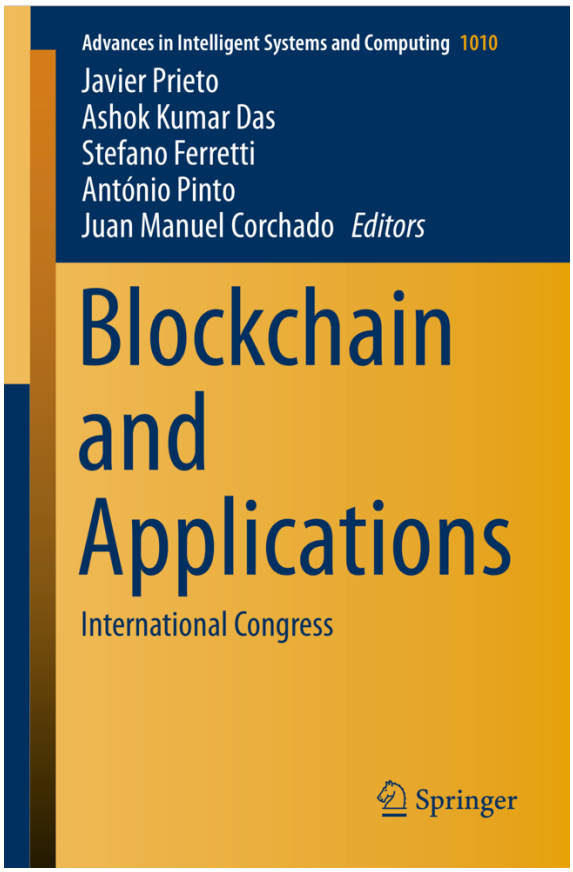


Privacy Centric Collaborative Machine Learning Model Training via Blockchain

Abstract. This paper tackles the issue of data siloing, where organisations are unable to share data with each other because of privacy concerns. Machine Learning models, which could benefit greatly from larger data sets shared between organisations, suffer in this era of data isolation. To solve this problem, a blockchain based implementation is proposed that allows training of machine learning models in a privacy compliant way. Instead of using blockchain in a typical database-style manner, the proposed solution uses blockchain as a means to handle joint ownership and joint control over a computer system known as the Training Machine. The Training Machine, set-up jointly by consortium members, serves as a secure, independent container that accepts data sets and an untrained model as inputs from different entities, trains the model internally, and outputs the trained model without revealing any data to other entities. Data is then deleted automatically. Blockchain ensures that this machine is not under the control of any one entity but is rather controlled transparently by all data-sharing parties. By placing sensitive information in an isolated system, and establishing blockchain based access control, the solution ensures that data is not accessible to any party other than the owner. The paper also shares use cases of this technology, along with a risk analysis and proof of concept.

Keywords: Private data sharing, Shared model training, Blockchain access control, Consortium data exchange, Deep learning training.

Paper Presented at **IEEE Cybernetics Conference in University of Salamanca, Spain**. Published as part of conference proceedings in **Springer's Advances in Intelligent Systems and Computing** series (AISC, volume 1010): https://doi.org/10.1007/978-3-030-23813-1_8



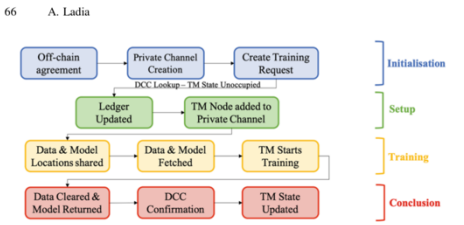


Fig. 2. Process for data sharing between *n* parties. This phase can be divided into four stages: (1) Initialisation, (2) Setup, (3) Training and (4) Conclusion

1. Entities A, B and C create a private channel
2. The ML model owner (entity C in this case) executes the `CreateTrainingRequest` smart contract on the DCC. The parameter specified is the name of the private channel created earlier. This contract performs a lookup of the DCC to check the state of the TM: whether it is occupied with an ongoing operation or not. If not, the request passes, and the ledger is updated to reflect the channel which the TM needs to join.
3. The TM joins the private channel. Entities A and B run the `AddData` smart contract on the private channel, which specifies the locations of the data to be fetched.
4. Finally, the `RunRequest` contract is called by the model owner, specifying the location of the model files, and the return location of the trained model. This signals the Ledger Bridge to start the training process.
5. The Bridge fetches the data and the untrained model from the locations specified. Note: both these locations are on the independent servers of entity A, B and C, and it is assumed that all entities have access control systems (possibly Public Key Infrastructure) in place that only allow GET requests from the Training Machine.
6. The Bridge runs the model training files on the data sets.
7. Once training has elapsed, the data sets are wiped by the Ledger Bridge, and upon successful deletion, a confirmation is posted on the DCC for transparent audit.
8. The trained ML model is returned to entity C. It is also deleted, and a confirmation is posted for open audit as before.
9. DCC is updated to indicate the TM is free for a new operation.

There is also a provision to allow entity C to gain direct access to check, update and maintain the training process. In order for such access to be granted, a proposal must be raised on the DCC, listing out the public key of the accessor, the period of access, and privileges needed. All members vote on the request; if it passes, the DCC state is updated. The Ledger Bridge creates a limited access user profile and adds entity C's cryptographic fingerprint to the SSH key list of the Training Machine for temporary

Blockchain: A Privacy Centered Standard for Corporate Compliance

Abstract. Recently, the right to privacy has become an important global issue, and laws are being enacted in different countries to ensure that citizens have control over how their data is stored and used. In this scenario, corporates face an increasing burden to comply with these laws, whilst ensuring that their business models and workflows are interrupted to as little a degree as possible. This paper presents blockchain as a potential technology that can help users keep their data under their own control and yet allow companies to responsibly access the data they need to function. It begins with an overview of blockchain as a technology and the properties that make it useful as a tool for privacy compliance. It then explores more niche fields like Zero Knowledge Proofs (ZKPs) and considers two industries where blockchain can be of benefit to consumers and corporates from a privacy standpoint.

Index Terms: Case Studies, Information flow controls, Security and Privacy Protection, Solution Reference Architectures

Research article manuscript submitted for publication in the IEEE IT Professional Magazine. Manuscript is available at http://bit.ly/PrivacyIEEE

Blockchain: A Privacy Centered Standard for Corporate Compliance

Aman Ladia

Abstract— Recently, the right to privacy has become an important global issue, and laws are being enacted in different countries to ensure that citizens have control over how their data is stored and used. In this scenario, corporates face an increasing burden to comply with these laws, whilst ensuring that their business models and workflows are interrupted to as little a degree as possible. This paper presents blockchain as a potential technology that can help users keep their data under their own control and yet allow companies to responsibly access the data they need to function. It begins with an overview of blockchain as a technology and the properties that make it useful as a tool for privacy compliance. It then explores more niche fields like Zero Knowledge Proofs (ZKPs) and considers two industries where blockchain can be of benefit to consumers and corporates from a privacy standpoint.

Index Terms— Case Studies, Information flow controls, Security and Privacy Protection, Solution Reference Architectures

1 The Relevance of Privacy Today

Over the last few years, privacy has evolved from merely a moral issue to a very real legal one. The argument for privacy has long been one of ethics–of corporates and governments having the intrinsic duty to protect consumer privacy. Unfortunately, ethics are difficult to justify in the court of law; legal frameworks for privacy were long due.

Today, privacy regulations have been enacted in nearly 80 different countries. The most prominent of these is the European Union's General Data Protection Regulation (GDPR), which despite its sceptics, has received applause from many. On a high-level, the GDPR aims to make companies accountable for the privacy of the users whose data they collect and store, whilst ensuring that consumers have the right to withdraw their consent for data collection as easily as they gave it in the first place [1]. Even in India, activism for privacy safeguards has led the Supreme Court to declare the Fundamental Right to Privacy a right at par with the Right to Life [2].

Evidently, privacy compliance has become a major factor of consideration for firms today. This article introduces blockchain as a potential technology that can aid in corporate privacy compliance.

2 Rethinking Databases

One of the fundamental technologies that corporates use to store user data is databases. Databases have been used incessantly since the late 1970s; while their capacity, features and complexity have certainly evolved, the underlying concept has remained much the same: a large table that stores 'records' for each individual.

It is undeniable that the security of databases has increased multifold over the years with the development of new data protection schemes and multi-stage safeguards. However, taking these measures one level forward requires us to rethink the basic architecture of databases and have accountability engrained into the base layer of data storage.

3 A Smarter Approach to Databases

To enforce the level of accountability required by present and future privacy regulations, safeguards need to exist such that users are always aware of the manner in which their data is being stored and used, and they have the power to revoke data access at any point of time with the surety that their data is indeed inaccessible.

Such a mechanism is implementable with blockchain. Blockchains, at their core, are distributed stores of information that use 'blocks' to record transactions between parties. For a transaction to go through, it must be validated by more than half of the blockchain nodes (network participants) and if successful, it is recorded on the blockchain.

Through this paper, it will be evident that there are two major ways in which blockchain can help enforce privacy regulations: first, by providing transparency in how data is handled, and second by providing methods that allow independent users to gain control over their data.

4 The Three Pillars of Blockchain

There are three main factors that differentiate blockchain from traditional, centralised databases:

1. Immutability: Blockchains are said to be immutable (not entirely true, but in a well designed blockchain solution, near immutability can be achieved). This means that any transaction recorded on a blockchain cannot be deleted or altered once it has been verified (confirmed). Therefore, accountability comes hand in glove with blockchain.
2. Distributed Ledger: Blockchains are designed to be distributed amongst hundreds, thousands or

• *Aman Ladia is with Liquid Protocol, B-1701, Chaitanya Towers, Prabhadevi, Mumbai, India – 400025. E-mail: aman@amanladia.com.*

Mechanical Ramp Attachment for Wheelchairs to Climb Footpaths and Elevated Surfaces

Abstract. This paper aims to tackle the problem of wheelchair bound personnel being unable to climb footpaths due to the absence of ramps on many pavements. The paper suggests a mechanical solution the problem that is simple yet effective in that it allows a wheelchair user to independently climb footpaths with minimal or no assistance. The design, which can be mounted onto any standard wheelchair, uses retractable control rods and an inbuilt ramp to lay an inclined plane in front of the wheelchair when needed, allowing the handicapped person to ascend or descend a step. This paper delineates the function and construction of each component of the proposed system and illustrates the same using both line diagrams and three dimensional computer generated models. It also investigates the various materials available for the construction of the device, whilst stating safety requirements and ensuring that the design adheres to them. Finally, it ends by describing the mode of operation of the device, and possibilities for future development of the design.

Keywords: Adaptable ramp, retractable plane, modular wheelchair

Paper published in International Journal of Mechanical Engineering & Technology (IJMET), Volume 10, Issue 06, June 2019, pp. 187-193, Article ID: IJMET_10_06_013. Paper open access and available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3451147

wheelchair unfriendly as it lacks even basic amenities like ramps for wheelchair users [2]. This reality exists not only in Mumbai, but in many towns and cities of the developing world.

This has a direct implication on the independence of wheelchair users. The handicapped are forced to either stay at home, or ask for the constant assistance of passers-by in order to climb or descend footpaths. Not only is this an inconvenience, but also a safety hazard as lifting a wheelchair several inches in order to push it up a footpath's edge can result in the wheelchair toppling and the handicapped person suffering injuries.

2. PROBLEM STATEMENT

Ideally, wheelchair users should be able to access footpaths and steps through permanent inclined planes. This would allow them to commute freely from one place to another without the assistance of others and the risk of injury. However, the absence of permanent ramps at footpaths means that this is not possible, and handicapped people feel all the more immobile.

Therefore, what is needed is a mechanism that allows wheelchairs to climb up footpaths in the absence of permanent ramps and without external help. At the same time, the designed system should be universally adaptable to accommodate the different form factors of wheelchairs available. This paper aims to delineate the construction and testing of such a system, built entirely using mechanical components and designed to be completely self-sufficient.

3. DESIGN

3.1. Analysis of wheelchair construction

Before designing the system according to the requirements mentioned in Section 2, it is imperative to understand the basic construction and operation mechanism of wheelchairs. Most wheelchairs have the same chassis. It consists of two large rear wheels mounted on a metal frame, with two smaller front castor wheels below a foot rest. Wheelchairs also typically have hand rims installed on the rear wheels, which allow the user to drive the chair without external help. Handles are also provided at the back of the chair in case an assistant is to help wheel the person. Fig. 1 indicates these components on a typical wheelchair [3].

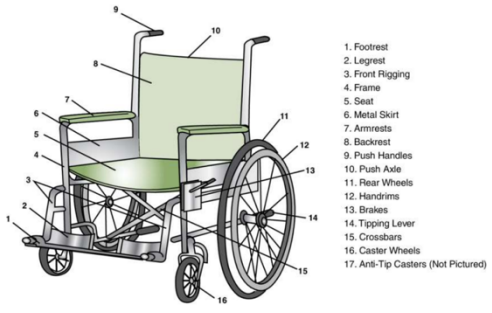


Figure 1 A typical hand driven wheelchair with annotated components

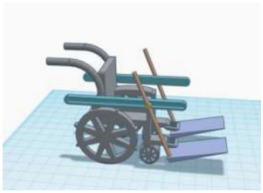


Figure 5 3D Computer Aided Design (CAD) Rendering of Wheelchair with Attachment

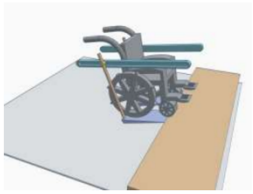


Figure 6 CAD Demonstration of Wheelchair climbing pavement

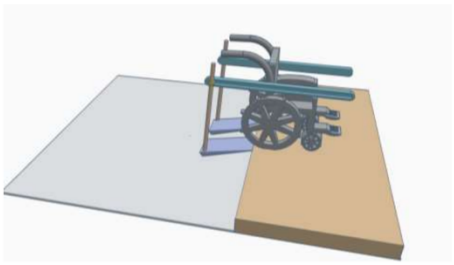


Figure 7 Final CAD rendering of wheelchair on top of pavement

5. CONCLUSION

This paper discussed the construction and operation of a lightweight, easy to use wheelchair attachment that can allow handicapped personnel to climb pavements without the assistance of an external helper. The system is built to be cheap, effective and modular such that it can be installed onto most manually operated wheelchairs.

The paper looked at the design of typical manual wheelchairs, and identified potential places where a mechanical attachment could be added to allow independent movement of a wheelchair on footpaths. Two locations were identified, and it was decided that the safest location would be along the armrests of the wheelchair. Following this, a basic line diagram was developed that illustrated the construction of the attachment and explained the various components of the proposed mechanism. To aid in the understanding of the modes of operation, a 3D model was also supplied.

To extend the discussion beyond the basic design of the wheelchair, three materials were investigated for suitability. After evaluating the trade-off between cost, density and tensile strength, 6061-T6 Aluminium Alloy was chosen as the material of choice. Furthermore, it was decided that the ramp would be carpeted with non-slip rubber in order to conform to safety