公立はこだて未来大学 2023 年度 システム情報科学実習
グループ報告書

Future University Hakodate 2023 Systems Information Science Practice
Group Report

プロジェクト名

暗号と数理とセキュリティ

Project Name

Crypto, a Mathematical Principle and Security

グループ名

楕円曲線暗号グループ

Group Name

Group ECC

プロジェクト番号/Project No.

17-B

プロジェクトリーダ/Project Leader

猪股莉記　Riki Inomata

グループリーダ/Group Leader

満保蒼月　Sogetsu Michiyasu

グループメンバ/Group Member

小林文太　Fumita Kobayashi

指導教員

白勢政明　川口聡

Advisor

Masaaki Shirase　Satoshi Kawaguchi

提出日

2024 年 1 月 17 日

Date of Submission

January 17, 2024

概要

本プロジェクトは, 暗号と数理に関する理解を深め, 暗号技術がもたらす強固なセキュリティを学ぶプロジェクトである. 現在, ブロックチェーン市場が拡大しつつあるが, ブロックチェーン技術の核は楕円曲線暗号を用いたデジタル署名である. そこで, 本グループでは, 楕円曲線暗号を学ぶことで, ブロックチェーンに対する理解を深め, 未来大生が身近に利用できるブロックチェーン技術を実装することを目標とする.

キーワード　楕円曲線暗号, デジタル署名, ブロックチェーン, 暗号資産

（※文責: 満保蒼月）

Abstract

This project is to deepen our understanding of cryptography and mathematics-, and to learn about the strong security that cryptography provides. Currently, the blockchain market is expanding, and the core of blockchain technology is digital signatures using elliptic curve cryptography. Therefore, the goal of this group is to deepen understanding of blockchain by learning elliptic curve cryptography and to implement blockchain technology that Future University students can use in their daily lives.

Keyword Elliptic Curve Cryptography, Electronic Signature, Blockchain, Crypto Currency

（※文責: 満保蒼月）

目次

第 1 章　背景

1.1　該当分野の現状と従来例

本節では、楕円曲線暗号にかかわるものとして、暗号、楕円曲線暗号、デジタル署名、ブロックチェーンについて説明し、現在存在する利用例についても紹介する。

現在用いられている暗号は、共通鍵暗号と公開鍵暗号の 2 種類に大別することができる。共通鍵暗号は、暗号化と復号に同一の鍵を用いる方式であり、公開鍵暗号は、公開鍵と秘密鍵という 2 種類の鍵を用いて暗号化と復号を行う方式である。

楕円曲線暗号は公開鍵暗号の中で主流と呼ばれるものの 1 つで、楕円曲線と呼ばれる曲線を用いた暗号である。公開鍵暗号の他の例としては素因数分解の困難性を用いた RSA 暗号が存在するが、RSA 暗号の安全性は、鍵の長さに強く依存している。現在では RSA 暗号の鍵長は 2048 ビットが推奨されることが多い。しかし、楕円曲線暗号は 256 ビットの鍵長で 3072 ビットの鍵長の RSA 暗号と同等の高い安全性を実現できる。鍵長が短ければ、暗号の計算を高速化が可能であり、また、鍵の保管に必要な容量も小さくなる。楕円曲線暗号の主な用途としては、SSH や SSL/TLS のような安全な通信プロトコルや、デジタル署名が挙げられる。

デジタル署名は、公開鍵暗号に類似した改ざん防止手法である。デジタル署名の大きな特徴は本人証明と、署名したメッセージの内容が改ざんされていないことの証明を同時に行うことができる点である。デジタル署名では、署名者の秘密鍵とメッセージを用いて署名を生成するので、他のメッセージに同じデジタル署名を用いることはできない。これは、紙の書類への署名や捺印では実現できないデジタル署名特有の利点である。楕円曲線暗号を用いたデジタル署名アルゴリズムの例としては ECDSA や BLS 署名が挙げられ、前者は Bitcoin、後者は Ethereum という暗号資産に利用されている。

ブロックチェーンは分散型のデジタル台帳と呼ばれる技術であり、ある一定の期間内の取引情報をまとめた台帳を 1 つのブロックとして、そのブロックをつなげたものである。ブロックチェーンの最大の特徴は改ざんが実質的に不可能ということである。これは、改ざんが一目瞭然かつ耐改ざん性があるということである。以上のようなブロックチェーンの安全性を保証する技術の一つがデジタル署名である。ブロックチェーンの活用例としては、Bitcoin や Ethereum といった暗号資産が挙げられる。ブロックチェーンは暗号資産への活用が進んでおり、ブロックチェーンと暗号資産が同一視されることもあるが、ブロックチェーンはデータの保管形態の 1 種でしかなく、暗号資産はあくまでもブロックチェーンを用いて実装されたものである。

（※文責: 満保蒼月）

1.2　現状における問題点

ブロックチェーンの問題点は、新たにブロックチェーンに参加するユーザーに専用のソフトウェアのダウンロードと、大容量のストレージを要求することである。大容量のストレージはブロックチェーンに記録されている過去から現在までの取引情報をダウンロードして保持するために要求される。例えば、Bitcoin では、Bitcoin Core と呼ばれるソフトウェアを公式に提供しているが、

このソフトウェアには過去の取引情報も含まれているため、ダウンロードには 350GB 以上のストレージが要求される [1]。また、このダウンロードには 1 週間以上の時間がかかる場合もある。もちろん、ブロックチェーン上での取引が続けば、それらの取引情報も記録する必要があるため、ブロックチェーンの取引に必要なストレージは今後も増え続けていくことがわかる。また、ソフトウエアのダウンロードといった行為は技術的な知識のない人々にとっては容易なことではなく、PC に関する基礎的な知識がない人はブロックチェーンに参加して取引を行うことは難しい。以上の理由から、ブロックチェーンは新規参入のための障壁が低いとは言えず、ブロックチェーン技術の普及を行うためには、これらの問題点を解決する必要がある。

そして、これらの問題点に加えて、暗号資産の抱える問題点として、人々の持つ暗号資産に対する漠然とした不安がある。日本においてこの漠然とした不安を生み出した要因の一つとして、暗号資産取引所「Coincheck(コインチェック)」が受けたハッキングによる暗号資産の流出が挙げられる。この事件は、Coincheck に対する不正アクセスが原因で発生したとされていて、この事件で流出した暗号資産自体の安全性はその原因ではない [2]。取引所の安全性と暗号資産自体がもつ安全性を切り分けて考える必要があることを、人々に啓蒙していく必要がある。

（※文責: 満保蒼月）

1.3 課題の概要

本グループの課題は、ユーザーすなわち人々にソフトウェアのダウンロードや大容量のストレージを要求することなく、ブロックチェーン上での取引を体験してもらうことである。疑似的な暗号資産を用いたブロックチェーン上での取引を体験することで、人々のブロックチェーン上での取引とブロックチェーン技術そのものに対する理解促進を図る。

（※文責: 満保蒼月）

第 2 章　到達目標

2.1　本プロジェクトにおける目的

本グループの目的はブロックチェーン技術とそれにかかわるマイニングなどの作業が体験できる Web アプリケーションを作成し人々に体験してもらうことで、ブロックチェーン技術を啓蒙することである。既存の暗号資産のようなブロックチェーンに新たに参加するために必要な、専用のソフトウェアの導入や大容量のストレージを要求しない Web 上で完結したアプリケーションを作成することで、人々が手軽にブロックチェーン技術を体験できるようになることを目指す。

（※文責: 満保蒼月）

2.2　通常の授業ではなく、プロジェクト学習で行う利点

通常の授業は前期または後期の半年弱で行われるが、楕円曲線暗号やブロックチェーンといった多くの知識を学ぶ必要がある場合には、半年弱の学習期間では足りないため、1 年を通して活動するプロジェクト学習が適している。また、通常の授業では先生が学生に対して一律で同じ授業を行うが、楕円曲線暗号とブロックチェーンについては学ぶことが多いため、役割を分担して学ぶことのできるプロジェクト学習が適している。

（※文責: 満保蒼月）

2.3　具体的な手順・課題設定

1. 基礎学習
   課題：この段階での課題は、有限体と楕円曲線について学び、さらにこれらの知識を用いて有限体上の楕円曲線について学ぶことである。楕円曲線暗号の詳細な仕組みを理解するためには、有限体上の楕円曲線の知識が必須となるためである。

2. 楕円曲線暗号とその応用に関する情報の収集
   課題：楕円曲線暗号が応用されているデジタル署名や通信プロトコルについて調べ、それらがどのように動作しているかを理解する。収集した情報をもとに、何を実装することを目的とするのかを定める。

3. ブロックチェーン技術に関する情報の収集
   課題：楕円曲線暗号を用いたデジタル署名が応用されているブロックチェーンについて調べる。ブロックチェーンに応用されているデジタル署名や、ブロックチェーン技術の具体的な応用例について調べることで、楕円曲線暗号とデジタル署名に対する理解を深める。

4. 製作物のアイデアの選定

課題：ブロックチェーンを用いた製作物としてどのようなものが考えられるかのアイデアをグループ内で出し合い、それが現実的なアイデアなのか、どのように製作するのかを話し合いながら検討する。

5. ブロックチェーンや暗号資産に関するさらなる調査
   課題：ブロックチェーンや暗号資産の仕組みに対する理解が不足しているため、さらに調査を進めることでその理解を深める。ブロックチェーンや暗号資産について詳しく調べることによって、制作物に関する新たなアイデアが思い浮かぶことも期待しながら行う。

6. ブロックチェーンと暗号資産のプログラミングによる実装
   課題：ここでは、ブロックチェーン全体を既存のライブラリを組み合わせて実装することと、Bitcoin のソースコードを参考にしながら、既存のライブラリを用いないで暗号資産の実装に挑戦する。最終的にはメンバー同士の製作した機能を組み合わせることで、既存のライブラリを用いずにブロックチェーンを実装することを目標とする。

7. 成果発表会で用いるスライドとポスターの作成
   課題：これまでの手順で得た知識や技術、それらを基に作り上げた成果物について聴衆にわかりやすく伝えられるようなスライドやポスターを作成する。スライドはできるだけ使う色の数と文字数を減らして、できるだけ平易な言葉で説明することを目標とする。ポスターでは、我々の学んだことをできるだけ正確に伝えることを目標とする。

（※文責: 満保蒼月）

2.4 課題の割り当て

基礎学習では、グループ全員が楕円曲線暗号の基礎を理解するために、同じ学習を行った。また、楕円曲線暗号についての情報収集では、グループ全員が情報ライブラリやインターネットで暗号や楕円曲線暗号にかかわる情報を調べた。

ブロックチェーンにかかわる情報収集を情報ライブラリやインターネットで行った。ブロックチェーンは比較的新しい技術であることから、日本語だけでなく英語での情報収集も必要であると考えた。グループの人数が 2 人であることに鑑みて、グループ全員での情報収集を行った。その後、暗号資産で最も有名な BitCoin に焦点を当て、BitCoin で使用されている電子署名アルゴリズムである ECDSA についても全員で理解をした。ECDSA について理解をした後は、暗号資産を実装できるかを判断するために満保蒼月は BitCoin の具体的なソースコードを調べ、暗号資産以外の制作物につながるアイデアを得るため小林文太はブロックチェーン技術の全体像についてさらに調べ、理解を深めた。

情報収集の担当分野と各メンバーの趣向に合わせて、ブロックチェーンの全体を既存のライブラリなどを用いて実装することを小林文太が担当し、楕円曲線暗号を用いたデジタル署名を、既存のライブラリをできるだけ用いることなく実装することを満保蒼月が担当した。各自の担当作業後に、ライブラリなしで実装したデジタル署名とブロックチェーンの全体を組み合わせることによって独自のブロックチェーンを実装することを目指した。

（※文責: 満保蒼月）

第 3 章　課題解決のプロセスの概要

2.2 節で具体化した各小課題の解決のプロセスの概要を、各々記述する。

1. 基礎学習
   解決過程：公立はこだて未来大学で 1 年生後期に開講される情報数学の教科書と、担当教員の推薦に基づく楕円曲線に関する基礎の本を基に、有限体と楕円曲線について学習した。

2. 楕円曲線暗号とその暗号資産への応用に関する情報の収集
   解決過程：Python での BitCoin のプログラミングについて学べる書籍とインターネットを活用して、ECDH と ECDSA、そして BitCoin について学んだ。

3. ブロックチェーン技術に関する情報の収集
   解決過程；ブロックチェーンに関する情報収集は主に情報ライブラリーで関連書籍を検索することから始めた。複数の関連書籍が見つかったので、グループメンバーが各々別の書籍を借りて読み、それぞれの情報を共有することで、学びを深めた。

4. 製作物のアイデアの選定
   解決過程：現状のブロックチェーンの応用例である暗号資産やサプライチェーンマネジメントなどについて主にインターネットを活用して調べた。一般の人々にはブロックチェーンと暗号資産はほぼ同じものであると認識されていることから、その誤解を解いたうえでブロックチェーン技術の啓蒙を行うには暗号資産に関する製品を作る必要があると私たちは考えた。しかし、実際に使われている通貨と対応させた暗号資産を扱うのは簡単ではないため、実際に使われている通貨とは関係ない疑似的な暗号資産を実装することが望ましいという結論に達した。

5. ブロックチェーンや暗号資産に関するさらなる調査
   解決過程：暗号資産の応用例や暗号資産の実装例について調べることで、どのような手法でブロックチェーン、そして独自の暗号資産を実装するべきかを理解した。既存のライブラリ、例えばデジタル署名のライブラリなどを用いることで、簡単なブロックチェーンを実装することは難しくないことが分かったため、ライブラリを用いずにデジタル署名を実装することと、ブロックチェーンの全体を実装することを切り分けて考えることで独自の暗号資産を実装するに至るのではないかという考えに至った。

6. ブロックチェーンと暗号資産のプログラミングによる実装
   解決過程：ブロックチェーンの全体を実装することについては、クラウド上に疑似的なブロックチェーンを構築することで、取引やブロックが可視化するようにした。クラウド上のブロックチェーンについては研究があまり進んでいないこともあり、様々な文献を参考にしながら実装をした。デジタル署名のライブラリを用いない実装は、主に [3] と [4] を参考にした。ライブラリを用いないデジタル署名の具体例について学んだ後、その具体例を応用し

てブロックチェーンにはほとんど用いられていないが有望なデジタル署名を自らの手で実装した。

7. 成果発表会で用いるスライドとポスターの作成
   解決過程：スライドについては、掲載したい文章をすべて書いてから、必要ない要素を削ってようやくすることによって、洗練された文章を作成した。その後、背景、目的、結果という流れを失わないように視覚的な効果も意識してスライドの作成を行った。ポスターについてもスライドと同様に掲載したいことをすべて書いてから、必要のない要素を削減することによって洗練された文章を作り上げた。このとき、専門的な言葉を排除しすぎないことで、誤解のない文章の作成を行った。また、スライドとポスターのどちらも、担当教員のフィードバックを受けてそれを反映することによってより良いものとした。

（※文責: 満保蒼月）

第 4 章　課題解決のプロセスの詳細

4.1　学習内容

4.1.1　デジタル署名

情報セキュリティにおいて、デジタル署名は以下の三つの主な目的を果たす。

- **認証**：署名はメッセージが送信者によって実際に送信されたことを証明し、身元の改ざんを防ぐのに役立つ。
- **完全性**：署名はメッセージが送信中に変更されていないことを確認する。ドキュメントやメッセージの内容がデジタル署名が適用された後に変更された場合、署名は無効になる。
- **否認防止**：署名は送信者がメッセージを送信したことを否定することを防ぐ。なぜなら、署名を作成するための固有の秘密キーは送信者だけが持っているからだ。

では、これはどのようにブロックチェーン技術と関連しているのだろうか。ブロックチェーン技術は、セキュアな取引のためにデジタル署名に依存している。例えば、一人の人から別の人へビットコインを送るなどしてブロックチェーンで取引が作成されるとき、、それは送信者の秘密キーで署名される。これがデジタル署名であり、それは取引の詳細と一緒にブロックに含まれる。

ブロックチェーンネットワークの他の参加者は送信者の公開キーを使用して署名を検証する。署名が検証されれば、取引が本物であり、改ざんされていないことが確認される。確認されたら、取引（ブロック）は取引の連鎖（ブロックチェーン）に追加される。

デジタル署名の概要

- **秘密鍵**：この鍵は、所有者が厳重に秘密にするもので、デジタル署名の作成に使用される。文書やメッセージなどのデータにこの鍵を適用することで、所有者は固有の署名を生成できる。作成過程は複雑な計算を伴うが、基本的には、データを短く、ハッシュ化し、そしてこのハッシュ値を秘密鍵で署名を生成する。
- **公開鍵**：この鍵はすべての人に公開されていて、デジタル署名の検証に使用される。デジタル署名が付されたデータを受け取った人々は、公開鍵を用いて署名を元のハッシュ値に復号する。次に、彼らは送信者と同じ方法で受け取ったデータをハッシュ値に変換する。もし二つのハッシュ値が一致すれば、それはデータが署名された後で変更されていないこと、すなわちその完全性を証明することとなる。

（※文責: 小林文太）

4.1.2　楕円曲線を用いたデジタル署名

楕円曲線を用いたデジタル署名は、既存のデジタル署名に楕円曲線を用いたものがよく見られる。この例としては ECDSA、EC-Schnorr が挙げられる。楕円曲線を用いたデジタル署名は、楕

円曲線暗号と同様に短い鍵長で既存のデジタル署名に匹敵する安全性を提供する。鍵長が短くなると、同じような安全性を持つ鍵長の長い暗号と比較すると計算が高速に行える可能性が高いことも利点である。

以下では、ECDSA と EC-Schnorr について簡単に説明する。

ECDSA

ECDSA は、DSA と呼ばれるデジタル署名方式に楕円曲線を用いたデジタル署名であり、BitCoin の実装に用いられているデジタル署名である。ECDSA は高い安全性を持つことで知られている。しかし、ECDSA では、ECDSA に用いる有限体上の楕円曲線の位数を n とすると、署名 $\sigma(r,s)$ が正当な署名ならば $\sigma(r,n-s)$ も正当な署名と判定されてしまう脆弱性がある。しかし、この脆弱性は、常に $s < n/2$ (もしくは $s > n/2$) となるように s を決定すれば解決することができるため、大きな問題とは言えない。

EC-Schnorr

EC-Schnorr は Schnorr 署名と呼ばれる効率的で安全な署名とされているデジタル署名に楕円曲線を用いたデジタル署名である。EC-Schnorr は ECDSA のような脆弱性を持たず、また、鍵を線形和で扱うことができる。これは、複数のデジタル署名をまとめて処理することができるということである。ブロックチェーンにおいては、複数の送信者が同一の受け取り先に送信する場合、送信者たちは共同でデータに署名でき、署名済のデータは送信者の公開鍵の和で検証可能となる [5]。このことから、複数の送信者がかかわる取引においても、それぞれの送信者が独立に署名をするよりも、効率的に取引を行うことができるとわかる。

（※文責: 満保蒼月）

4.2　各人の課題の概要とプロジェクト内における位置づけ

満保蒼月の担当課題は以下のとおりである。

5 月　楕円曲線暗号と有限体の基礎について学ぶ。プロジェクト内の輪読で、有限体と有限体上での演算について説明する。

6 月　楕円曲線暗号の具体例と、楕円曲線暗号の活用事例の情報収集。Python を用いた BitCoin のプログラミングについて学ぶ。

7 月　楕円曲線と有限体について数学的な知識が足りない人に向けて説明できるようにする。中間発表に用いるポスターやスライド資料を作成。中間報告書の作成も行う。

8 月　楕円曲線と有限体の知識の復習とブロックチェーン技術のライブラリを用いない実装について学ぶ。

9 月　楕円曲線暗号、その中でもデジタル署名についてさらに深く学ぶ。楕円曲線上の点をプログラミングでどのように扱うのか理解する。

10 月　既存のデジタル署名である ECDSA の実装例について学ぶ。この実装例を基にして EC-Schnorr の実装を行う。また、トランザクション、シリアライズについても学ぶ。

11 月　成果発表会に向けたスライドとポスターの作成を行う。グループメンバーの担当するスライドについても監修を行う。スライドとポスターについては背景や目的などの部分を主に担当する。

12 月　成果発表会に向けた発表練習を行う。発表練習ではグループメンバーへのフィードバックも行う。成果発表会での発表を行う。成果発表会後は、最終報告書に着手する。最終報告書の分担の振り分けについても担当する。

1 月　担当教員からのフィードバックを基に、最終報告書を修正し完成させる。

小林文太の担当課題は以下のとおりである。

5 月　有限体の概念に再び取り組み、特に剰余に焦点を当てて、有限体上の楕円曲線を完全に理解するための基礎を固める。

6 月　楕円曲線が暗号技術にどのように応用されているかについて情報を収集する。

7 月　ECDSA がブロックチェーンのアルゴリズムでどのように実装されているかを調査する。また、中間発表のためのポスターやパワーポイントのスライドを作成する作業にも従事する。

8 月　仮想通貨の基本システムに関する研究を行い、大学内での暗号資産システムの効果的な統合に焦点を当てた。ブロックチェーン取引の安全性に関わる暗号化手法を理解することに注力。

9 月　Azure を活用したクラウドとブロックチェーンの統合の可能性を研究。ブロックチェーンのスケーラビリティ向上と効率化を目指し、学術環境向けのクラウドベースのブロックチェーンシステムの概念モデルを開発。

10 月　クラウドベースのブロックチェーン環境でのクライアントサイドマイニングに関する研究に注力。JavaScript を用いたマイニングソリューションの開発により、効率的かつ完全性を保持するマイニングプロセスの最適化を図る。

11 月　理論から実践へと移行し、アプリケーションの設計から開発、テスト、デプロイまでを一手に担当。エラーハンドリングとデバッグにおいても、一元管理による効率的な対応を実現。

12 月　最終発表に向けたスライド作成と練習に専念。プロジェクトの技術的側面を簡潔に伝えるスライドの作成を通じて、プロジェクトの深い理解を示す。

1 月　プロジェクトの包括的な報告書作成に着手。クラウドコンピューティングとブロックチェーン技術を組み合わせたキャンパス内での暗号資産ウェブアプリケーション開発の成功を文書化し、Azure 上での実施による透明で分散化された不変のブロックチェーンシステムの提供を強調。

（※文責: 小林文太）

4.3　担当課題解決過程の詳細

4.3.1　満保蒼月

5 月　有限体と楕円曲線の基礎について学ぶために、一年次の情報数学の教科書と、担当教員の推薦する楕円曲線の入門書を用いた。また、学んだ内容をまとめ、プロジェクト内での輪読で発表を行って自身の理解を共有した。また、楕円曲線暗号がブロックチェーンに用いられていることからグループの目標をブロックチェーンにかかわるものにすることを提案した。

6 月　BitCoin が C++ や Python でプログラミングできることを知り、グループメンバー全員が知識のある Python を用いた BitCoin のプログラミングを学び、電子署名のプログラミングについて理解した。また、楕円曲線暗号について調べる中で、BitCoin で用いられている ECDSA だけでなく EdDSA や Ed25519 などのアルゴリズムについても知った。これらと

並行して、中間発表とグループ間の発表に向けた準備を行った。

7 月 中間発表に向けて、スライドやポスターの作成を行った。このとき、数学的知識が少ない人にも楕円曲線や楕円曲線暗号の性質を分かりやすく伝えるために、できるだけ図や簡単な例を用いた説明をできるように準備を行った。また、中間発表でのフィードバックから、課題の設定や今後の予定があまり具体的ではなく、見通しの甘さが露わになったため、課題やその解決方法の再設定が必要であると認識し、グループメンバーと意見を交換した。

8 月 5 月に学んだ内容を軽く復習し、楕円曲線と有限体に関する基礎的な知識を確固たるものとした。また、ブロックチェーンに関連する書籍を読むことで、既存のライブラリをできるだけ用いずにデジタル署名を実装するにはオブジェクト指向プログラミングが適していることを理解した。

9 月 はじめに、デジタル署名の大まかな仕組みとその利点を理解した。その後、楕円曲線暗号が関わっているデジタル署名の具体例について学び、その仕組みを理解した。それと並行して、オブジェクト指向プログラミングを用いることで有限体上の点と楕円曲線上の点をそれぞれクラスで表し、楕円曲線上の点の演算についても定義できるようにした。

10 月 楕円曲線暗号が関わっているデジタル署名の 1 例である ECDSA の実装例について学んだ。ECDSA の実装例について学ぶ中で、デジタル署名についての理解が深まり、この知識と経験を応用して EC-Schnorr を実装し、そのテストを行った。EC-Schnorr の実装においては、BitCoin にも用いられている secp256k1 という有限体上の楕円曲線を用いることで、実用的な EC-Schnorrn の実装を行った。デジタル署名が実装できたので、その後はブロックチェーンにおいてデジタル署名とのかかわりがあるトランザクションとシリアライズの 2 つについて学んだ。また、独自の楕円曲線を用いることはできないかと考え、PARI/GP を用いて有用な楕円曲線を探したが、大きな位数を持った有限体上の楕円曲線を探すことは容易ではなく断念した。

11 月 成果発表会に向けたスライドとポスターの作成を行い、その大部分を担った。次の 3 点を意識してスライドを作成することで、非常に見やすいスライドを作成した。1 点目は、スライドは背景、目的、結果の順に作成することを意識することである。2 点目は、できるだけスライドの 1 ページ当たりの文字数を減らすことである。これは、まずスライドではなく、スライドに記載したいことを文章としてまとめた後、その文章を削って必要最低限の情報まで削ることによって洗練された文言に書き換えることで。3 点目はスライドに用いる色も 3 色までにすることである。また、ポスターを作成する際には、スライドを作成した際に使用した文章を参考にして、端的に楕円曲線やデジタル署名について説明する文章を構成した。このとき、スライドは誤解を恐れずに必要最低限の情報を用いて専門用語を説明する形で作成したが、ポスターは短い文章で正確に専門用語を説明することを意識して作成した。

12 月 1 週目は、スライドをよりよいものにすることと、発表練習に用いた。発表練習を行う前には、Google ドキュメントの音声入力機能を用いて大まかな発表原稿を作成することで、発表時間の見積もりを行うことでスライドや発表内容の調整に活かした。発表練習を行い、担当教員と他グループからのフィードバックをもらい、さらに発表内容とスライドの調整を行った。成果発表会後は、提出物の作成に着手し、報告書の執筆の分担や内容についてグループメンバーへの指示を行った。

1 月 報告書等の提出物を完成させるために、1 年間で学んだことや成果物について見直した。

（※文責: 満保蒼月）

4.3.2 小林文太

5 月 有限体を視覚的に理解するために、Python のライブラリ”matplotlib”を活用した。その後、プロジェクトメンバーと共に、一年次の情報数学の教科書の中の有限体に関する特定の部分について理解を共有した。

6 月 楕円曲線暗号には、Elliptic Curve Diffie-Hellman（ECDH）やデジタル署名に主に使われる ECDSA など、さまざまな種類があることを発見した。ECDH の仕組みについては、中間発表で発表することに決めた。ECDH の簡潔さは、楕円曲線に慣れていない人でもアルゴリズムを視覚的に理解することを可能にする。

7 月 この期間の多くは、間近に迫った発表の準備に費やされた。それでもなお、ECDH と ECDSA と深く絡み合っているブロックチェーン技術についての調査に時間を割いた。この尽力により、我々のグループはこのプロジェクトの具体的な目標を設定することができた：誰でも使えるブロックチェーンをテーマに、ブロックチェーン技術を使ったサービスを開発するというものだ。”中間発表”でのフィードバックは、声の調節や説明の明確さなど、我々の発表技術の改善点を示してくれた。これらの洞察は、12 月の最終発表に向けて間違いなく有益であるだろう。

8 月 8 月には、暗号資産の基本的なシステムに関する徹底的な研究を行った。これには、さまざまなブロックチェーン構造の探求が含まれ、特に大学内で使える暗号資産システムへの効果的な統合方法に焦点を当てた。研究の重要な部分は、ブロックチェーン取引を安全にするための暗号化手法の理解に捧げられた。

9 月 9 月の研究は、特に Azure の機能を活用しながら、クラウドコンピューティングとブロックチェーン技術の統合の複雑さを解き明かすことに向けられた。この期間は、この統合を通じてブロックチェーンのスケーラビリティと効率を高める方法の詳細な分析によって特徴づけられた。学術環境に特化した、クラウド技術によるブロックチェーンシステムの概念的なモデルを作成することに努めた。

10 月 10 月には、クラウドベースのブロックチェーン環境内でのクライアントサイドマイニングの概念を進展させることに注力した。クライアントデバイスで効率的なマイニングプロセスを実現するための計算上の課題と潜在的な解決策に関する徹底的な研究を行った。この月の大部分は、クラウドインフラストラクチャとの統合が可能な JavaScript ベースのマイニングソリューションの探求に費やされ、システムの効率と完全性を保ちながらマイニングプロセスを最適化することを目指した。

11 月 11 月には、プロジェクトは理論的研究から実用的な応用へと移行した。バックエンドとフロントエンドのアプリケーションの設計、開発、テスト、デプロイを全て自分で担当した。エラーやバグに対処する際に、開発のすべての側面を自分自身で管理することが効率的であった。JavaScript に依存するクラウド環境でのクライアントサイドマイニングの実装は当初難しい課題だったが、これを成功裏に克服した。この成果は、複雑な技術的課題をナビゲートし解決する能力を示す重要なマイルストーンとなった。

12 月 12 月はプロジェクトの最終発表の準備に専念した。これには、プロジェクトの本質を簡潔に捉えた詳細なスライドを作成する作業が含まれた。この作業は、プロジェクトの技術的な側面を深く理解し、これらの複雑さをアクセスしやすい方法で伝える能力を必要とした。

1 月 最後に、1 月はプロジェクトに関する包括的な報告書の作成に焦点を当てた。この報告書は、

初期の研究段階から最終的な実装に至るまでのプロジェクトの全ての側面を包含していた。報告書は、クラウドコンピューティングとブロックチェーン技術を統合して、キャンパスで使用できる革新的な暗号資産ウェブアプリケーションを作成したプロジェクトの成功を証明するものである。報告書は、Microsoft Azure 上でホストされたこのウェブサービスが、クラウド上の透明で分散化された、不変のブロックチェーンシステムを提供することを強調した。

（※文責: 小林文太）

4.4 担当課題と他の課題の連携内容

4.4.1 満保蒼月

前期は、全員が同じ課題に取り組むという形でグループ活動を進めたため、ほかの課題との連携はあまり見られなかった。後期では、ライブラリなしでデジタル署名を実装するなかで、ブロックチェーンの全体像の知識を学ぶことができた。また、スライドやポスターの作成を通して、わかりやすい文章の内容と構成について学ぶことができたため、報告書の作成でそれを生かすことができた。

（※文責: 満保蒼月）

4.4.2 小林文太

このプロジェクトにおいて、私はアプリ開発プロセス全体を担当した。これは、最初の要件定義から開発、実装、デバッグ、テストの最終段階に至るまでの幅広い責任を含んでいる。私の任務は、アプリケーションのバックエンドとフロントエンドの両方に及び、プロジェクト全体に一貫性と統合性をもたらすことであった。

設計担当として、私はアプリケーションのアーキテクチャを綿密に設計した。このプロセスには、クラウドコンピューティングとブロックチェーン技術の統合というプロジェクトのビジョンに合致した、ユーザーのニーズとシステム要件の詳細な分析が含まれていた。スケーラブルでセキュアなフレームワークを構築することに重点を置き、これによりクラウド環境内のブロックチェーン操作の複雑さに対応できるようにした。

開発フェーズでは、多岐にわたるプログラミング言語とテクノロジーを駆使して複雑な機能をコーディングした。特に Microsoft Azure でのクラウドサービスとのシームレスな統合を図りながら、ブロックチェーン取引のための複雑なアルゴリズムを実装した。

テストとデバッグは、私の責任の重要な部分であった。特にクラウド技術とブロックチェーンを統合するという革新的な性質上、システムがクラウド環境で無過失に機能することを保証する上で多くの課題に直面した。クライアントサイドマイニングは、JavaScript に依存するため、当初は大きな障壁となったが、進んだ JavaScript ベースのマイニング機能を Web アプリケーションに組み込むことで、これらの課題を効果的に克服した。これによりアプリケーションのパフォーマンスが向上し、ユーザー体験も豊かになった。

プロジェクト全体を通して、初期の要件と期待に応えることに集中した。技術的な複雑さをナビ

ゲートし、革新的な解決策を見出す私の能力は、プロジェクトの成功において重要な役割を果たした。その結果、追加のソフトウェアをダウンロードすることなく、ユーザーがアクセスできる透明で分散化された不変のブロックチェーンシステムを提供するアプリケーションが生まれた。

このプロジェクトでの私の役割は、技術的な開発にとどまらず、アプリケーションが学術基準に沿い、大学の教育目的に貢献することも含まれていた。ブロックチェーン技術を解き明かし、学生や教員にアクセス可能にするアプリケーションを作成することにより、私は大学の技術面だけでなく教育面にも大きく貢献したと信じている。

（※文責: 小林文太）

第 5 章　結果

5.1　プロジェクトの結果

このプロジェクトは、ブラウザを通じて直接アクセスできるユーザーフレンドリーなブロックチェーンベースの仮想通貨システムの開発を中心に展開した。主な目標は、ブロックチェーン技術をより多くの人々に理解しやすくすることであった。開発チームは、ブロックチェーン技術を駆使した仮想通貨システムとの直接的なやり取りを可能にする Web ベースのアプリケーションを作成することに集中した。このアプローチにより、ブロックチェーン技術へのアクセス障壁を大幅に下げた。

プロジェクトの重要な部分は、JavaScript を使用してマイニング機能を再現することだった。これにより、クラウド内でユーザーのコンピュータの計算能力を活用し、中央集権的な処理能力に依存せずに重要なブロックチェーン操作を行うことができた。この方法は、ブロックチェーン取引の検証を実際に示すだけでなく、その分散型の特性も強調した。

さらに、プロジェクトでは、複数の API サーバーを使用してクラウド内でブロックチェーンノードを模倣することを含んでいた。この構成により、多数の取引とブロックチェーン操作を同時に処理できる堅牢でスケーラブルなインフラストラクチャが実現された。サーバーは仮想通貨システムのバックボーンを形成し、効率的に機能させた。

アプリケーションの開発には、Django と FastAPI が用いられた。Django はユーザーフレンドリーなフロントエンドインターフェイスを構築するために使用され、FastAPI はバックエンドとして機能し、暗号化、デジタル署名、新しいブロックの作成、トランザクション、チェーンとトランザクションの検証などの重要な操作を扱った。システムのセキュリティと整合性を保つために、FastAPI アプリは Django アプリからのリクエストを通じてのみアクセス可能に設定され、ネットワークセキュリティグループやファイアウォールなどの厳格なセキュリティ対策が施された。

また、仮想通貨システムの開発中に、EC-Schnorr というブロックチェーンアプリケーションに適したデジタル署名スキームの有用性を発見した。これにより、暗号鍵の効率的なストレージと組み合わせた使用が可能となる。我々は、外部ライブラリに最小限依存しながら、Python で EC-Schnorr を実装した。EC-Schnorr システムは結果的に我々のシステムに組み込まれていないが、そのブロックチェーンのセキュリティと効率性に対する潜在的な利点は明らかであり、今後の強化に対して有望であると言えるだろう。

機能面では、Django アプリケーションは、ブロックチェーンシステムとのユーザーインタラクションを容易にするように細心の注意を払って設計された。ユーザーは、受取人のユーザー名、送金額、取引の説明を入力することで、他のユーザーに仮想通貨を送ることができた。システムの信頼性を高めるため、ユーザーが自分の残高を超えて送金することを防ぐ安全対策が実装された。

また、プール内のトランザクションが検証されてチェーンに追加されるまでの注意メッセージが表示されるようにした。この機能はユーザー体験を向上させるだけでなく、取引プロセスの透明性をもたらした。クラウドベースのブロックチェーンシステムにおけるマイニング機能の実装は、プロジェクトの重要な側面であった。JavaScript を活用してクライアントサイドでのマイニングを可能にし、計算処理はホストの計算リソースではなく、クライアントのウェブブラウザで行われ

た。このアプローチは資源利用の効率化だけでなく、アプリケーションに対話的で教育的な要素をもたらした。

アプリケーションはまた、ユーザーが現在のブロックとトランザクションプールを視覚的に理解できるように設計された。ブロック番号、取引時間、送信者と受信者の情報、取引額、説明、署名などの詳細が分かりやすいテーブル形式で提示された。さらに、ユーザーは自分の秘密鍵と公開鍵を閲覧できることで、システムの透明性とセキュリティが強化された。

総じて、このプロジェクトの結果として、アクセシビリティ、セキュリティ、ユーザーフレンドリー、教育的価値に焦点を当てた詳細で革新的なアプローチを含んでいた。我々の努力は、複雑なブロックチェーン技術のメカニズムを簡素化し、Web ベースのプラットフォームを通じてアクセスしやすくすることで、より広い層にブロックチェーン理解を促進する重要な進歩を示した。

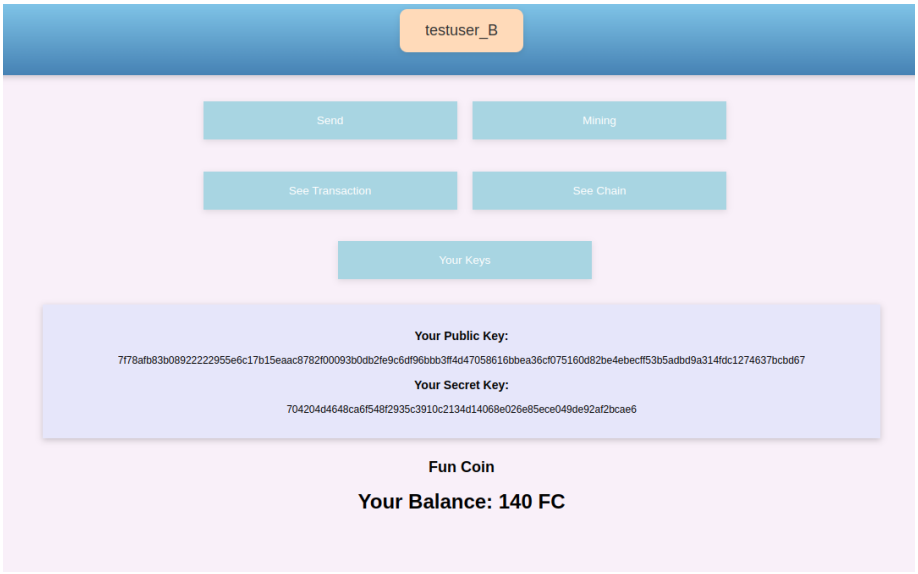

図 5.1　作成した We アプリのホーム画面

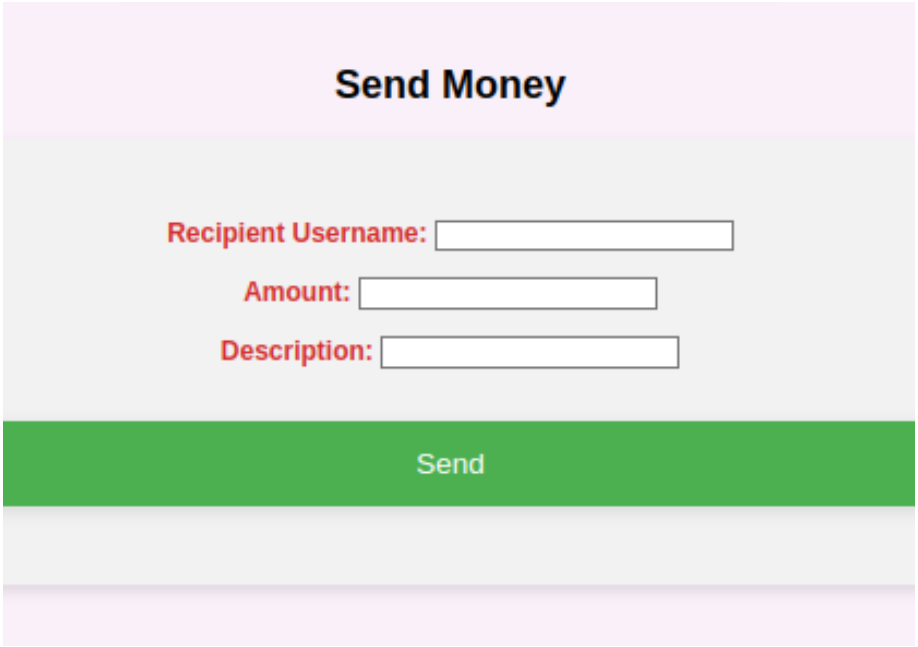

図 5.2　暗号資産の送金機能用フォーム

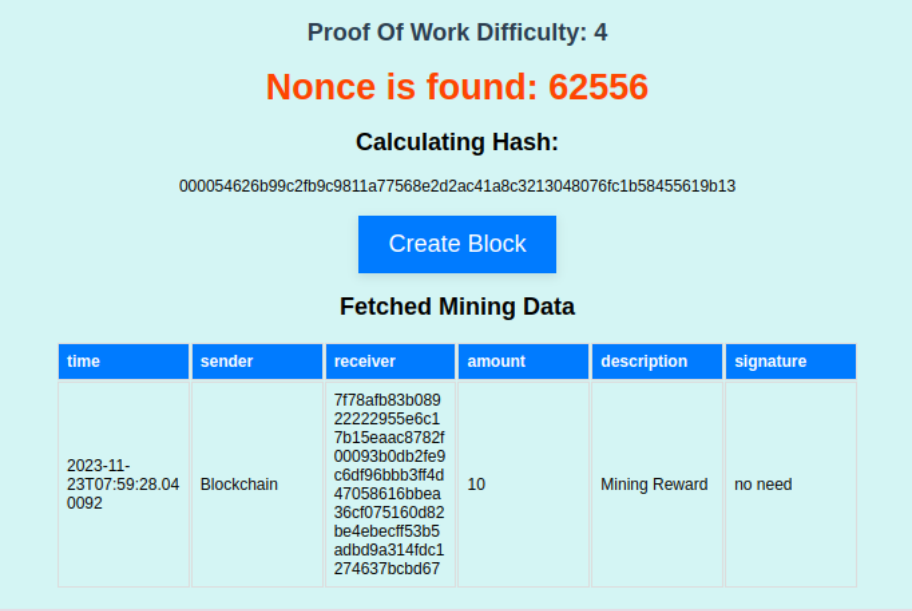

図 5.3　JavaScript 上で Nonce の値を計算するマイニング機能

（※文責: 小林文太）

5.2　成果の評価

プロジェクトの全体的な結果と問題解決の観点に焦点を当てると、クラウドベースの環境でブロックチェーン技術の効果的な応用と、それがユーザー体験に与えた影響が明らかになる。

まず、プロジェクトはブロックチェーン技術をより広い範囲の聴衆にアクセス可能かつ理解しやすくするという初期の問題に成功裏に対処した。ウェブベースの仮想通貨システムの開発により、ソフトウェアのダウンロードの必要性を排除し、ユーザーがブロックチェーン技術との相互作用を大幅に単純化した。このアプローチは、ブロックチェーンをよりアクセスしやすくするだけでなく、その仕組みを知らないユーザーに技術を解明する教育ツールとしても機能した。

プロジェクトの重要な特徴は、JavaScript を使用したクライアントサイドのマイニングの統合であった。これにより、ユーザーはウェブブラウザから直接ブロックチェーンネットワークに積極的に参加し、トランザクションを検証することができた。この革新的なアプローチは、ブロックチェーンの分散型の性質を実証するだけでなく、ユーザーに技術の操作に関する実践的な体験を提供し、彼らの理解を深めた。

さらに、プロジェクトの成果には、クラウド内でのブロックチェーンノードの成功したシミュレーションが含まれていた。この側面は、ブロックチェーン技術の現実世界での応用を再現する上で重要であり、その拡張性と堅牢性を示した。複数の API サーバーを使用してブロック情報を管理することで、システムが大量のトランザクションを処理できるようにし、任意のブロックチェーンネットワークにとって基本的な要件を確保した。

セキュリティはプロジェクトにおいて最優先の懸念事項だった。Django および FastAPI アプリケーションを同じ Azure バーチャルマシン上にデプロイし、FastAPI アプリへのアクセスを制限することにより、システムの完全性を保証した。このセットアップは、バックエンドを不正アクセスから保護し、ブロックチェーンシステム全体の安全性を強化した。

プロジェクトの結果は、初期の仮説と密接に一致している。追加のソフトウェアダウンロードを

必要としないで、没入感のある対話的なブロックチェーン体験を提供するシステムの能力は、私たちのアプローチを検証した。ユーザーは、トランザクションやマイニングプロセスを透明かつユーザーフレンドリーな方法で理解できるようになった。

しかしながら、さらなる改善の余地が残っている。より良いナビゲーションのためのユーザーインターフェースを強化し、追加のブロックチェーン機能を組み込むことで、ユーザー体験をさらに豊かにすることができる。また、ブロックチェーン技術の進化する性質に適応し、システムのセキュリティと効率を維持するために、継続的なテストと開発が必要である。

結論として、プロジェクトの成果は、ユーザーフレンドリーで安全かつ教育的な方法でのブロックチェーン技術の成功した実装を示している。これらの成果は、ブロックチェーン技術を解明し、より広い聴衆にアクセス可能にするというプロジェクトの主要な目標を達成したことを示している。

（※文責: 小林文太）

5.3 担当分担課題の評価

5.3.1 満保蒼月

1. **有限体と楕円曲線についての学習**
   有限体と楕円曲線についての学習では、主体的に行動し、細かな情報まで調べつくしたため輪読でも非常に良い評価を得た。また、中間発表でも、輪読での発表の経験が役に立ち、聴衆にわかりやすいように説明できた。有限体と楕円曲線について学んだ後に楕円曲線暗号について調べた際には、有限体と楕円曲線の基礎をしっかりと抑えていたおかげで理解が早かった。

2. **Python でプログラミングされた BitCoin の学習**
   有限体と楕円曲線から体系的に Python でプログラミングしていくことを学んだため、BitCoin で使われている ECDSA がどのようなコードで書かれているのかを正確に理解するに至った。後期では、トランザクションの処理やマークルツリーといったブロックチェーンを実装するうえで必要な概念をさらに学んでいく必要がある。また、Python を用いて記述された BitCoin は Python という言語の性質により、実用的な計算速度を提供することができないため、後期に行うアプリケーションの実装では開発言語を変える必要があることがわかった。

3. **既存のライブラリを用いないデジタル署名の実装**
   BitCoin の実装を学ぶ中で、既存のライブラリを用いない ECDSA の実装について理解した。これを応用して、EC-Schnorr を既存のライブラリをあまり用いることなく実装することに成功した。EC-Schnorr では ECDSA に存在するデメリットを克服したうえで、鍵を複数まとめて管理することができるという利点も持ち合わせているため、今後のブロックチェーン開発においても大いに役立つであろう。今回は Python で実装したが、より高速で計算ができる C++ で実装することが今後の課題となるだろう。

4. **スライド、ポスターの作成**

自らの担当したスライドのページに関しては担当教員だけでなく、他のプロジェクトに参加している人からも非常に良いというフィードバックを受けたため、楕円曲線暗号やブロックチェーンといった難しい内容を非常にわかりやすく伝えられるものが作成できたといえる。成果物の詳細を理解するうえで必要な知識をわかりやすく伝えられるようになったことで、発表がより円滑に行えた。また、スライドやポスター全体の内容について監修することで、自らが担当したページとほかのメンバーが担当したページで説明に食い違いが生まれないようにした。

（※文責: 満保蒼月）

5.3.2 小林文太

1. **楕円曲線暗号に関する基礎知識の習得**
   楕円曲線暗号の基礎知識を成功裏に習得した。情報数学およびシステム数学 I の講義で学んだ理論を応用し、有限体上の楕円曲線とその暗号技術での役割を理解した。暗号強度の維持と暗号セキュリティの評価に関するさらなる研究が必要である。

2. **ブロックチェーン技術における楕円曲線暗号の応用**
   特にビットコインにおいて、楕円曲線暗号がブロックチェーン技術のセキュリティを確保する上で重要な役割を果たしていることを学んだ。トランザクションの検証やアドレス生成におけるその使用を探求し、他の暗号技術との統合や新しい暗号技術がブロックチェーンに与える影響に関する理解のギャップを特定した。

3. **問題設定と目標の定義**
   プロジェクトの主な目的を明確に定義し、楕円曲線暗号を使用してブロックチェーン技術のセキュリティと効率を高めることに焦点を当てた。初期の目標は野心的であったが、実現可能なものに修正した。技術選択と具体的な実装戦略についてさらなる検討の必要性を議論した。

4. **システム開発と実装**
   システム開発と実装のすべての側面を個人的に担当した。楕円曲線暗号をブロックチェーン運用に効果的に統合するシステムの設計に焦点を当てた。複雑な暗号プロセスを単純化するユーザーフレンドリーなインターフェースの開発における課題に取り組んだ。プロジェクトに適合する暗号アルゴリズムと技術を評価した。

5. **将来の方向性と改善**
   暗号技術とブロックチェーン技術の進化に適応するために継続的な研究開発が必要であると特定した。システムのセキュリティと運用効率を高めるために先進的な暗号ソリューションを探求することを提案した。システムを洗練させ、利用性の問題に対処するために包括的なテストとユーザーフィードバックセッションを実施することを提案した。

6. **スケーラビリティとパフォーマンスの向上**
   成長する取引数を効率的に処理できるようにブロックチェーンシステムのスケーラビリティを向上させる戦略を探求した。トランザクション処理時間を短縮し、システム全体の応答性を向上させる方法に焦点を当てた。

7. **堅牢なセキュリティフレームワークの開発**
   システムの包括的なセキュリティフレームワークを構築するために努力を注いだ。ブロックチェーン技術の潜在的な脆弱性に対処し、データ完全性を確保するための複数層のセキュリティプロトコルを実装した。

（※文責: 小林文太）

第 6 章　今後の課題と展望

今後の展望としては、EC-Shcnorr を本プロジェクトで実装したブロックチェーンに組み込むことが挙げられる。これにより、一人で複数の秘密鍵や公開鍵を利用することがあっても、鍵を線形和でまとめて用いることができる。また、ECDSA にはある条件を満たす 2 つの署名が同一の正しい署名として認識されてしまう脆弱性が存在するが、EC-Schnorr にはその脆弱性が存在しないため従来のブロックチェーンよりも優れた安全性を持ったブロックチェーンを実装できる可能性がある。

（※文責: 満保蒼月）

付録 A　新規習得技術

前期は、BitCoin のコードを読む中でオブジェクト指向プログラミングを習得し、楕円曲線と有限体上の楕円曲線のグラフを matplotlib を用いて描画できるようになった。また、一部のソースコードの共有のために Git と GitHub を習得した。ブロックチェーン技術を体験できる Web アプリケーションを作成するために、Microsoft Azure、Django、FastAPI についても学んだ。

付録 B　活用した講義

- **情報数学**
  情報数学で説明された有限体の概念の話が、楕円曲線暗号で使う有限体錠の楕円曲線を理解する上で非常に役に立った。

- **システム数学 I , 応用数学 I**
  以下に記す式は、楕円曲線上の点の加算やそのスカラー倍を計算するために用いる公式である。この公式を理解するために偏微分が必要不可欠であったため、偏微分の概念を時間をかけて学べた非常に有意義な講義だった。

$$\begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 = -y_1 + \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \end{cases}$$

- **情報代数と符号理論**
  情報数学のときよりも更に深く、有限体やその拡大体の構成法と性質を学べる授業だった。楕円曲線上の無限遠点を理解するのに非常に役に立った。

- **複雑系科学演習**
  この講義では gnuplot を用いた作図の方法について学んだ。この技術を活かして、gnuplot で楕円曲線のプロットを行った画像を作成し、ポスターに掲載した。

付録 C　相互評価

満保蒼月

小林文太：彼は楕円曲線暗号について積極的に学んでいた。また、ビットコインをプログラミングする本を学習していた。そして EC-Schnorr 署名のプログラムの作成をした。後期に入ってからの最終発表の準備では、当初は役割分担の割当等がスムーズに進まなかったが、最終的に成果物の開発と、発表用のスライドやポスター作成等で分担した結果、最終発表まで余裕を持って終えることができた。発表用ポスターとスライドは彼の功績であり、非常に時間をかけて編集していたこともあり、発表用のスライドとポスターは非常にわかりやすいものになっていた。

小林文太

満保蒼月：前期においては、彼はブロックチェーンと ECDH,ECDSA などの楕円曲線暗号を用いたアルゴリズムについて意欲的に学んでいた。物事の理解が早いので、こちらの意図をすぐに汲み取ってくれることもあり、活動しやすかったように思うが、連絡や指示が通っていないことがあったので確認をお互いにできるようにしたい。後期では、彼はブロックチェーンについて意欲的に学び、プロジェクト活動外で得た知識も生かしながらブロックチェーンをクラウド上で実装することに挑戦した。成果発表会までに成果物を完成させたことは素晴らしいことである。スライドや発表方法については改善の余地が見込まれたが、十分な発表が行われていたように思う。

付録 D　その他製作物

参考文献

[1] Bitcoin.org, ”Bitcoin Core のダウンロード”, https://bitcoin.org/ja/download (参照 2023/12/22)

[2] Coincheck, ”暗号資産 NEM の不正送金に関する質問”, https://coincheck.com/ja/info/faq_nem (参照 2023/12/22)

[3] Jimmy Song 著, 星野靖子訳 (2020) ”プログラミング・ビットコイン：ゼロからビットコインをプログラムする方法”, オライリー・ジャパン

[4] 山崎重一郎, 安土茂亨, 金子雄介, 長田繁幸 (2021) ”ブロックチェーン技術概論：理論と実践”, 講談社

[5] Blockchain Biz ”「シュノア署名」ビットコインのセキュリティー、効率、プライバシーを改善する署名”, https://gaiax-blockchain.com/schnorr (参照 2024/1/10)