東北大学
ブロックチェーンセミナー

株式会社Neo Breakthrough
山科 優希

2023/3/2

講師紹介

株式会社Neo Breakthrough
Blockchain Lab Director
山科 優希

【略歴】

山形東高校探究科卒業（2021.3）

＞東北大学工学部電気情報物理工学科入学（2021.4）

＞同大学中退（2021.8）

＞株式会社Neo Breakthrough入社（2021.9）

＞Blockchain Lab設立（2021.10）

本日のスケジュール

13:00 | 13:10 | 13:50 | 14:30 | 15:10 | 17:30

Bitcoin Prehistory

Bitcoin以前の
暗号技術の歴史を
振り返ります。

Bitcoin

Bitcoinを学びます。
Whitepaperから始まり、
Bitcoin Blockchainの
仕組みについて。

Ethereum

Ethereumを学びます。
Whitepaperから始まり、
Account / Smart Contract
を解説します。
DeFiやERCについても
触れます。

Hands-on

remixを用いてERC20/721の
発行を体験します。
thirdwebを用いて
NFTマーケットプレイスを
開発します。

Bitcoin Prehistory

1976年

Diffie-Hellman key exchange

~DH鍵共有~

論文”New Directions in Cryptography”

内で提唱された

『公開鍵暗号の駆け出し』となる技術。

共通鍵暗号方式による鍵配送を

セキュアに行うための理論。

2人が示したのはあくまでも原理のみであり、

具体的関数の存在性については示されていない。

1977年

RSA Cryptosystem

~RSA暗号~

Diffie/Hellmanの示した原理を満足する
理想的な関数の存在を証明。
存在を示したRivest/Shamir/Adlemanの3名の名前
に由来してRSA暗号となった。
素因数分解問題の困難性によって、
暗号の安全性が担保されている。

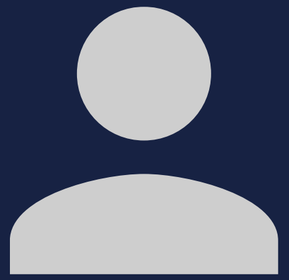
仕組み

Step1

①十分大きな素数p,qを用意して積をとる。n=pq
②gcd((p-1)(q-1) , k_1)=1なる整数k_1をとる。
③k_1k_2 ≡ 1 (mod (p-1)(q-1))なる整数k_2をとる。
（k_2は1≦k_2≦(p-1)(q-1)-1の範囲で
一意的に定まる。）

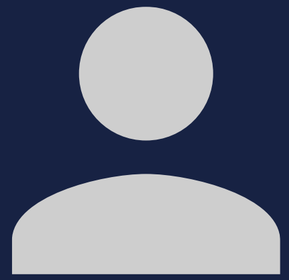
Step2

m：メッセージ
（mはn未満の正整数）
$m^{k_1} \equiv C \pmod{n}$
Cを暗号文とする。



送信者

暗号文：C



受信者

公開鍵（n , k_1)
秘密鍵（k_2）

Step3

$C^{k_2} \equiv x \pmod{n}$
上式を計算するとx = mとなり、
メッセージの解読に成功！

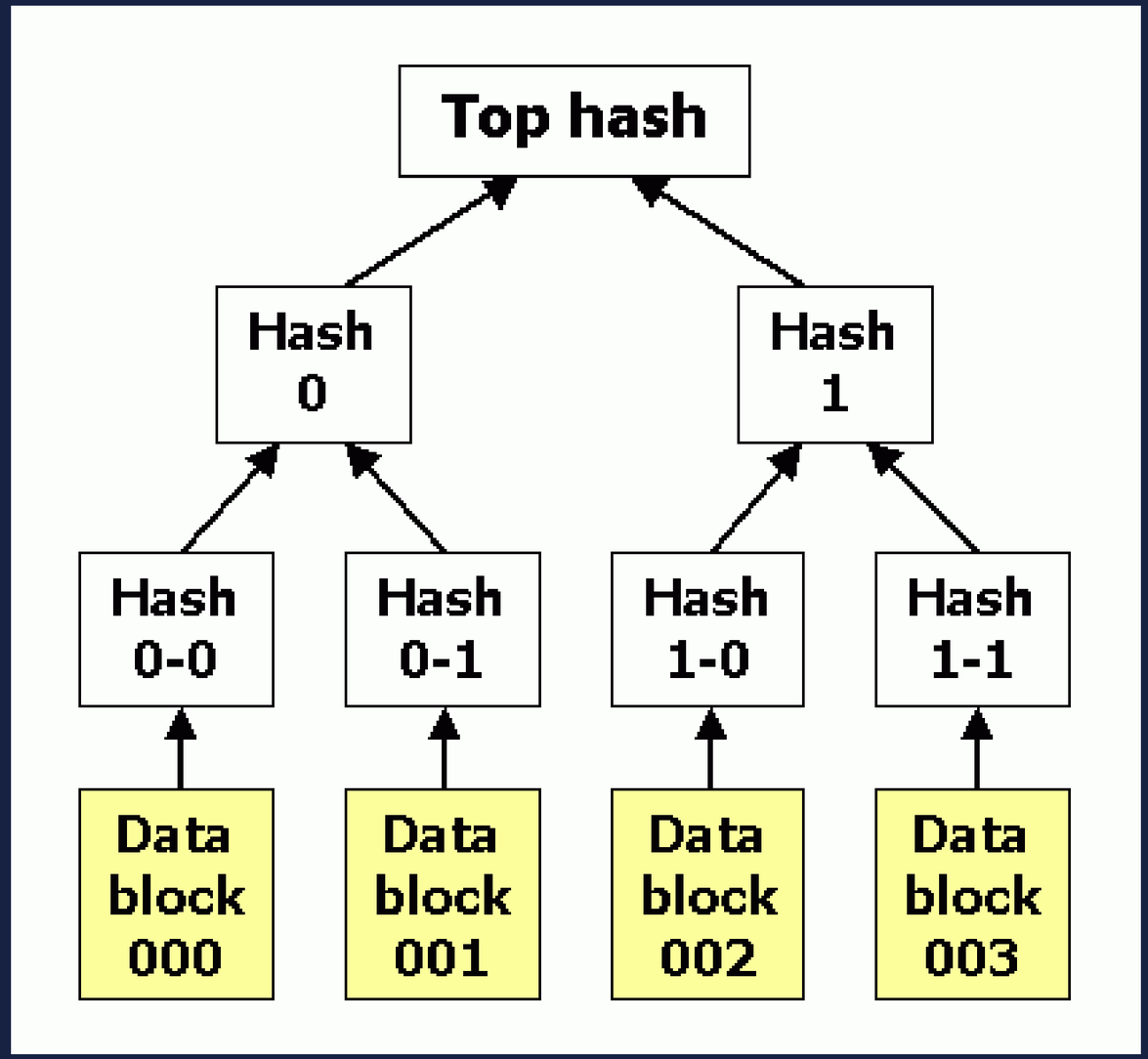
1979年

Merkle Tree

~マークル木~

Ralph Merkleによって発明された、大きなデータを要約して格納するツリー構造の一種。
ハッシュチェーンのうち、二分木によるツリー構造を組成するものを示す。
ハッシュを利用していることから、ハッシュ木と呼ばれることもある。

仕組み



出典：https://ja.wikipedia.org/wiki/ハッシュ木

1983年

Blind Signatures for Untraceable Payments

~ブラインド署名~

デジタル署名の一種。
『署名する人』と『署名するメッセージの作成者』が異なる場合に用いられる。
応用具体例として、メッセージ送信者のプライバシーが必要な匿名投票システムなど。

1985年

Elliptic Curve Cryptography

~楕円曲線暗号~

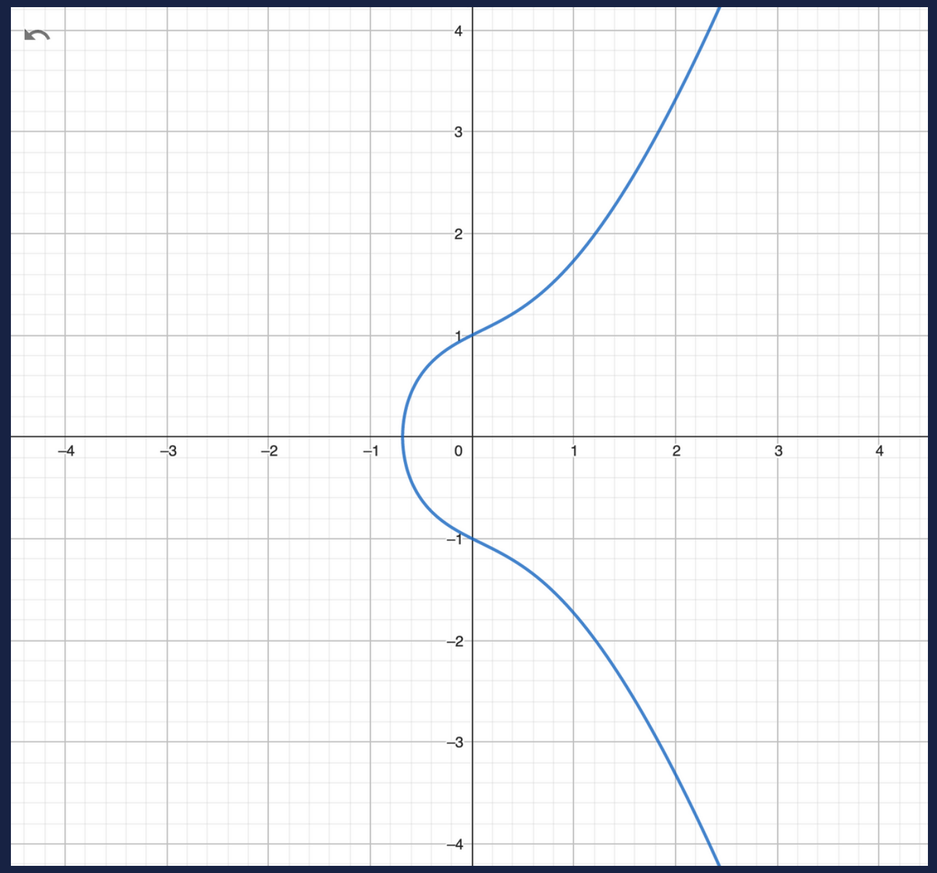
楕円曲線を利用した暗号方式の総称。

楕円曲線上の離散対数問題（EC-DLP）の困難性が暗号の安全性を担保している。

RSA暗号よりも短い鍵で処理速度も速い状態で同レベルの安全性を保つことができる。

一部のEC-DLPに対しては多項式時間アルゴリズムが見つかっている。（危険）

楕円曲線とは



楕円曲線は y^2 = x^3 + ax + b を満たす（x , y)の

集合に無限遠点O = (∞ , ∞)を加えたもの。

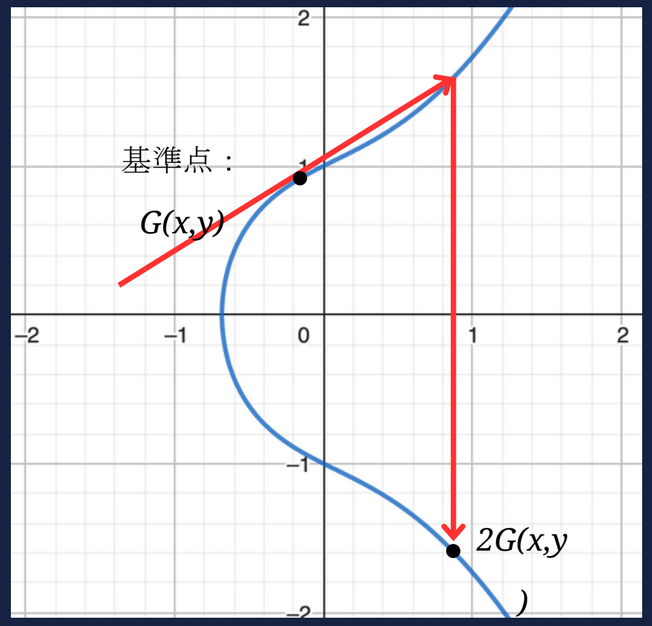
a,bは$4a^3 + 27b^3 \neq 0$を満たしている。

左グラフではa = 1 , b = 1と設定している。

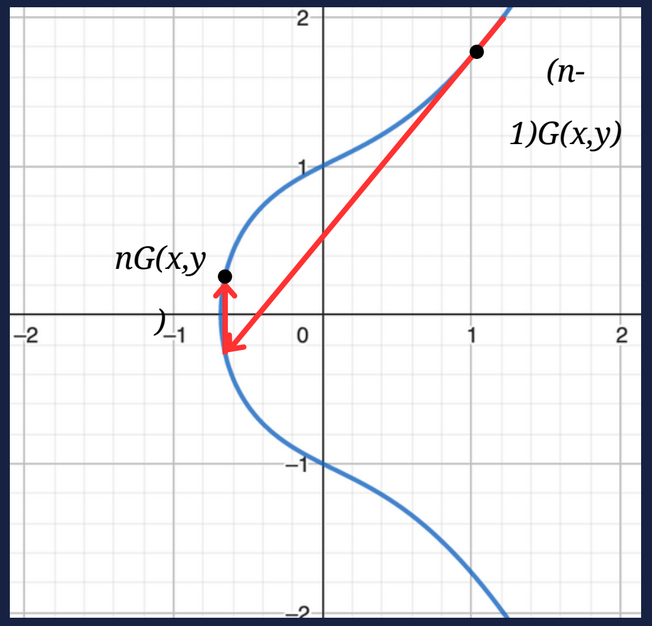
楕円曲線暗号では素数pを法とした

$y^2 \equiv x^3 + ax + b \pmod{p}$が使われる。

仕組み



n回繰り返す



公開鍵 nG

秘密鍵 n

1985年

FLP Impossibility

~耐障害分散合意の不可能性~

4月にFischer/Lynch/Pattersonによって発表された論文"Impossibility of Distributed Consensus with One Faulty Process"において提唱。
可用性のある非同期分散システムにおいて、
有限時間内で分散合意を達成できるアルゴリズムが存在しない。

1991年

Time-stamp "How to Time-stamp a digital document"

~電子時刻印~

HaberとStornettaによって提唱された。
ドキュメントをハッシュ化し、リンキングさせることによってドキュメントの存在と前後関係を示した。
信頼できるタイムスタンプサービスが存在することで成立。

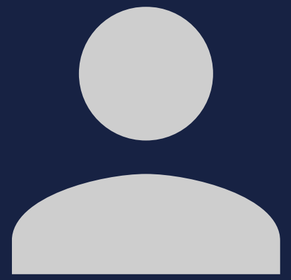
仕組み

ハッシュ化

AC124C34
EB344B1A
BD6D728A
37BA4C5D

タイムスタンプサービス

ハッシュの送信



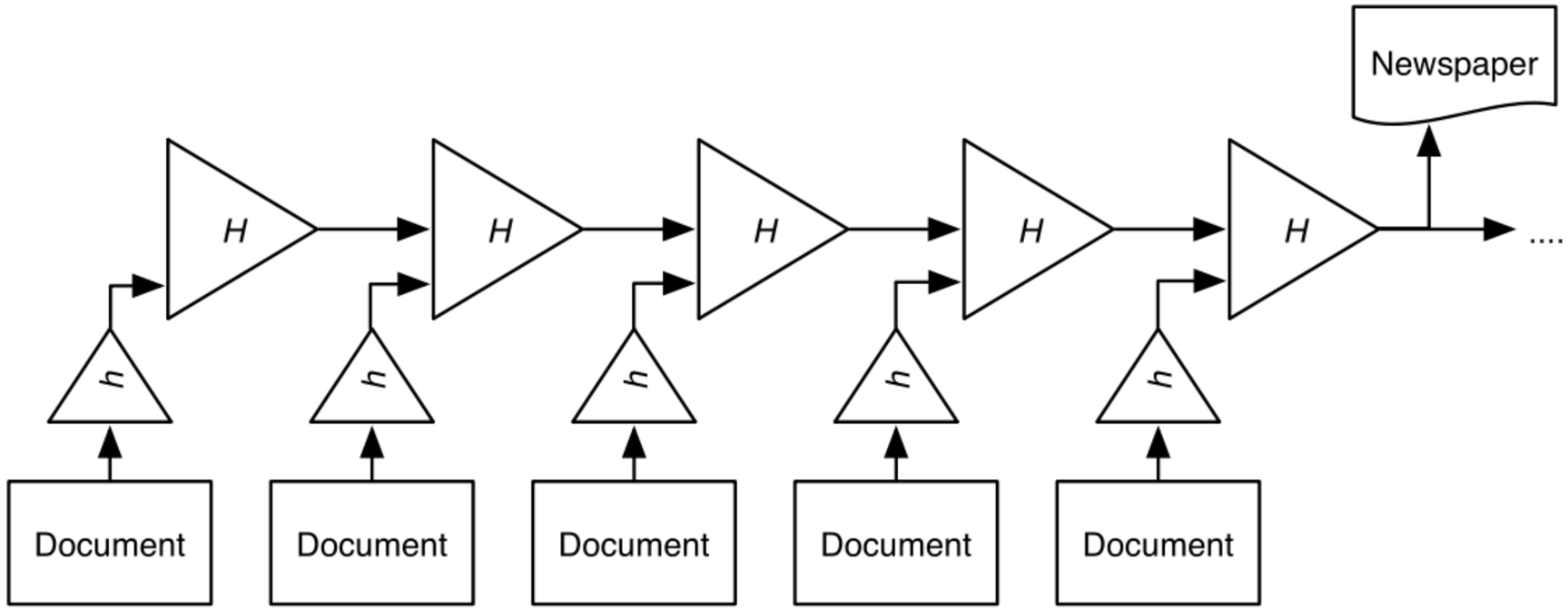
ハッシュ＋タイムスタンプ

AC124C34
EB344B1A
BD6D728A
37BA4C5D

＋

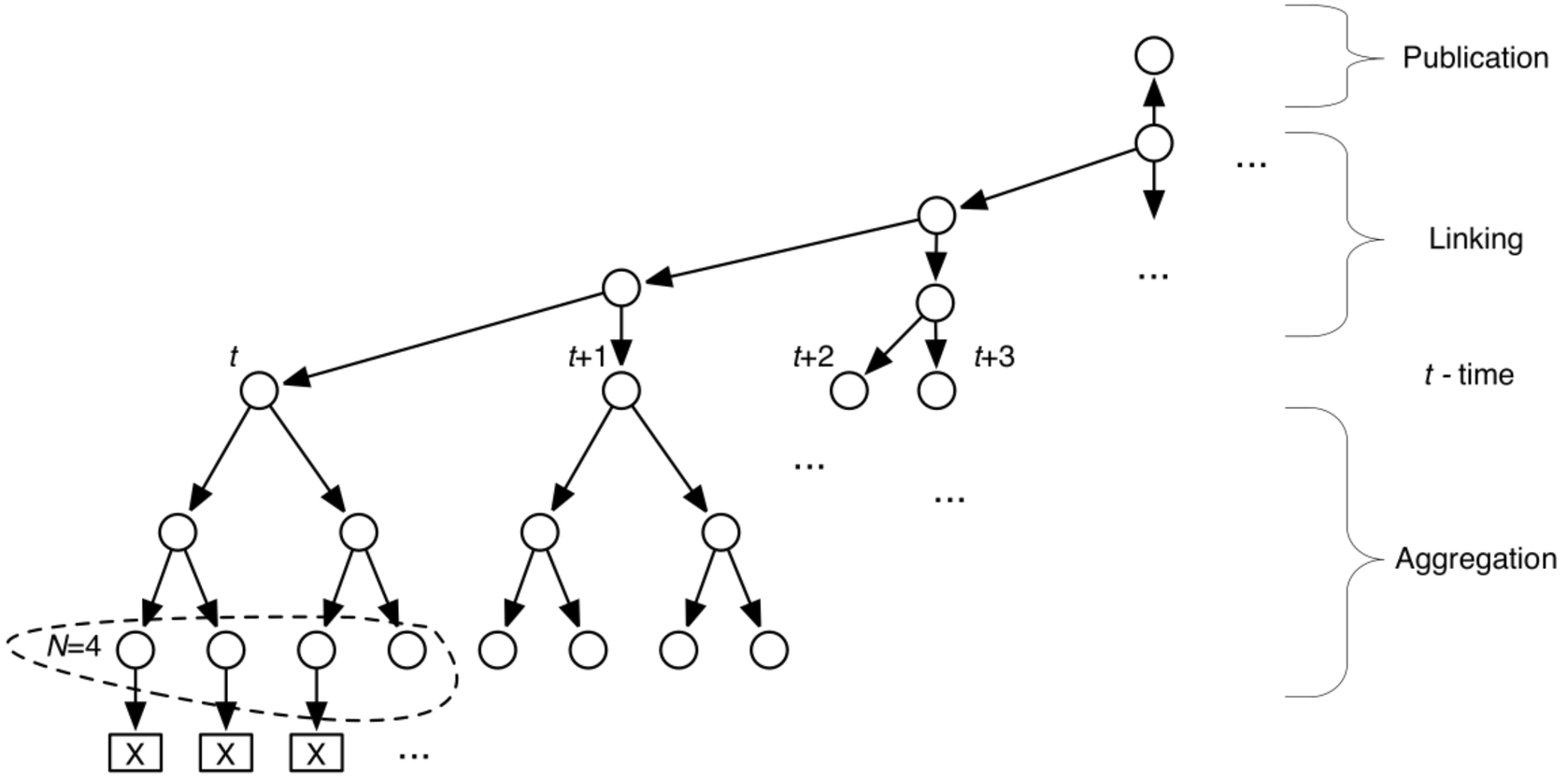
デジタル署名

Harber-Stornetta Linking



出典：https://en.wikipedia.org/wiki/Linked_timestamping

Linking with Merkle tree



出典：https://en.wikipedia.org/wiki/Linked_timestamping

1992年

”The Crypto Anarchist Manifesto”

~クリプトアナーキスト宣言~

Timothy C Mayによる暗号無政府主義宣言。
88年に提唱され、92年にサイファーパンク運動設立総会にて読み上げられた。
完全匿名・完全自由言論・完全自由市場を確固たるものとし、暗号無政府主義の基盤を固めた。

1997年

”Formalizing and Securing Relationships on Public Networks”

~公開ネットワーク上の
　関係の形式化と安全化~

法学者であり暗号学者でもあるNick Szaboによって論文が発表され、『スマートコントラクト』という言葉を初めて提唱した。

Nick Szaboは自動的であり暗号学的に安全なデジタル市場を構想し、スマートコントラクトを取引やビジネス機能が仲介者なしに信頼できる形で実行されるものとしていた。

1997年

Hashcash

~ハッシュキャッシュ~

Hashcashは1997年にAdam Backによって提唱された
Proof-of-Workのシステム。
電子メールのスパムやサービス拒否攻撃を制限するために
使用される。
送信のためにコストとしてCPUを消費（ハッシュ値生成）
することによって、コストを指標に送信元が信頼できるか
どうかを検証することができる。

1998年

BitGold

~ビットゴールド~

Nick Szaboが分散型デジタル通貨の仕組みとして設計した。
実装されることはなかったが、『Bitcoinアーキテクチャの直接的な先駆け』と呼ばれている。
Szaboは『金の安全性と信頼性の特徴』を、サイバースペースで忠実に実現しようとしていた。

1999年

Napster “Modern P2P”

~ナップスター~

P2P技術を用いた（主に音楽を共有することを目的とした）ファイル共有システム。
米Napster Inc.によって運営された。
アカウントを中央サーバーで管理し、所有者から直接ダウンロードする方式でファイル共有をP2Pネットワーク上で行う*”Hybrid P2P”*であった。

2002年

Winny

~ウィニー~

元東京大学大学院情報理工学系研究科助手の金子勇によって開発された、P2P技術を応用したファイル共有ソフト。
自身の接続しているPCをファイル転送の中継点として使うため、実際のファイルが保存されているPCがどこであるかを知ることができない。
Winnyはピュア型P2Pであり、利用開始時に中央サーバーからアクセス権を受け取り、ネットワークに参加する。

2003年

BitTorrent

~ビットトレント~

P2P技術を利用したファイル転送用プロトコルのこと。
従来のインターネットに反して『人気のあるソフトであればあるほどダウンロード速度が速くなる』という点が特徴であり、この点がNapsterと異なる。

2004年

Reusable Proof-of-Work

~再利用可能なPOW~

Nick Szaboの理論に基づいてHal Finneyが発明したデジタル通貨の原型とされるもの。
RPOWはプロトタイプ以上にはならなかったが、
もし普及していたら巨大なネットワークに対応することになっていたと言われている。
高度なセキュリティモデル下での構築を条件として、二重支払い問題を解決した。