Blockchain for Medical Consultation

Jackson Shea

Param Desai

What is Blockchain?

- Blockchain consists of multiple blocks chained together each of which contain transactional data, a hashcode, and a previous hash [1].

- A public key in a decentralized network is used to encrypt digital signatures and is also passed onto the others in the network.[9]

- This means that the private key decrypts the hashcode, verifying the previous block's hashcode.[9]

- After that process of the public key being handed off and decrypted by the private key, then the process repeats to anyone in that network.[9]

Ledgers in Blockchain

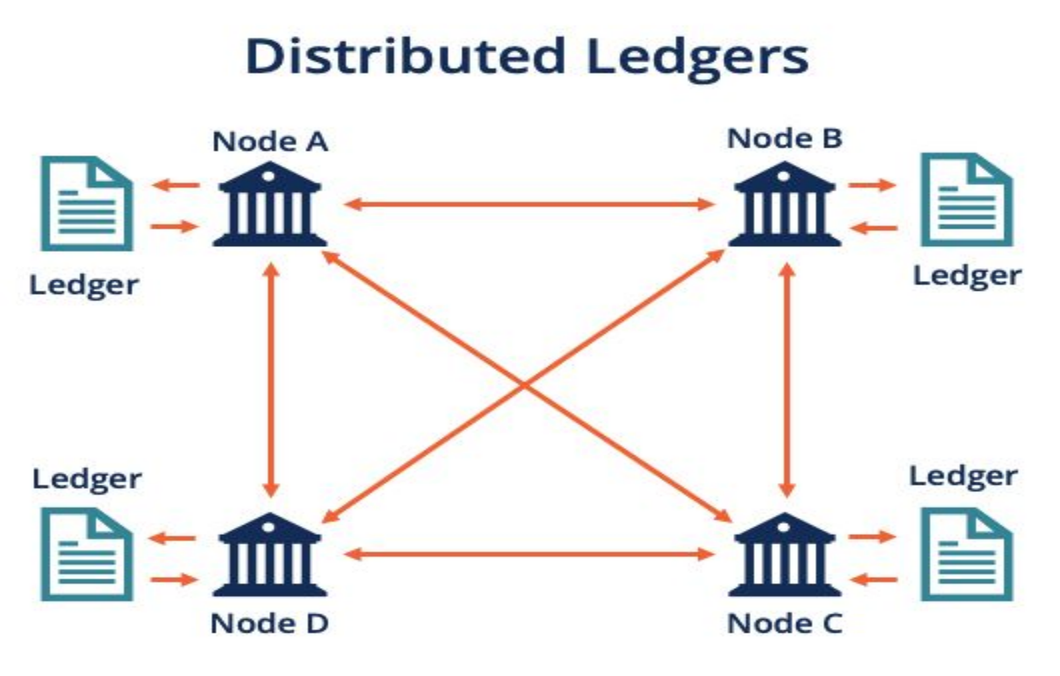
- Blockchain is a distributed ledger[2].

- **Ledgers**: A ledger is a type of record keeping databases where financial transactions between multiple parties are recorded.

- There are two types of Ledgers

  1. Centralized Ledgers

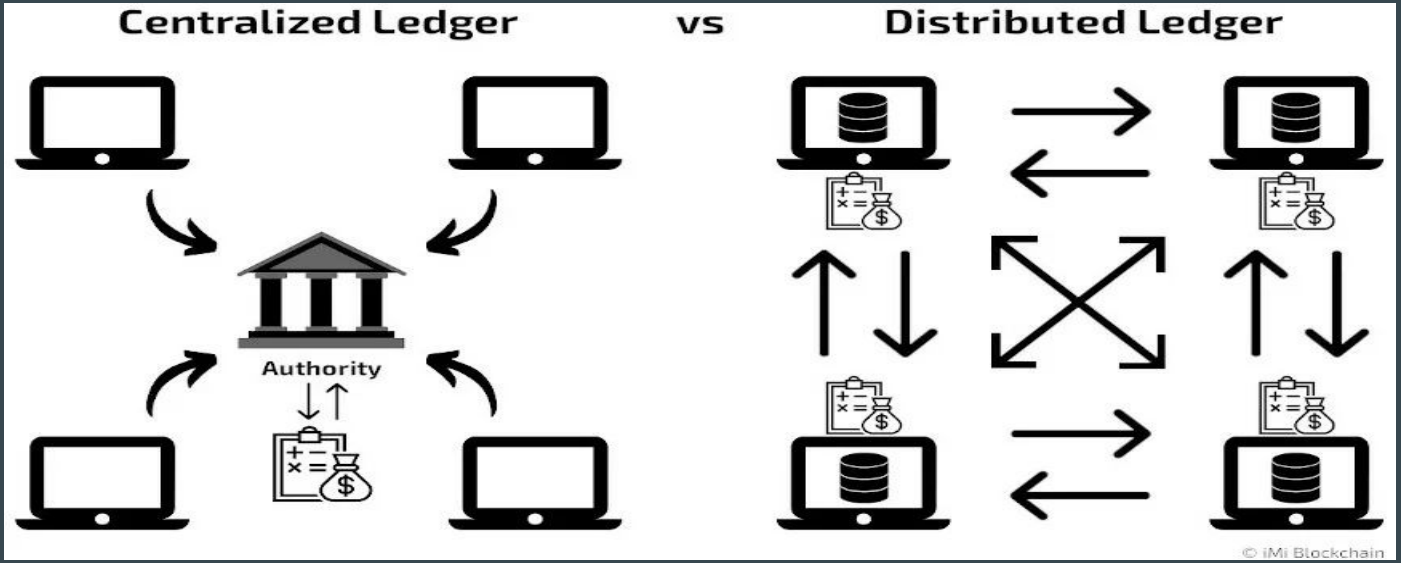
  2. Distributed Ledger



Fig[1]: Distributed Ledgers
Source:[18]

Centralized Ledgers

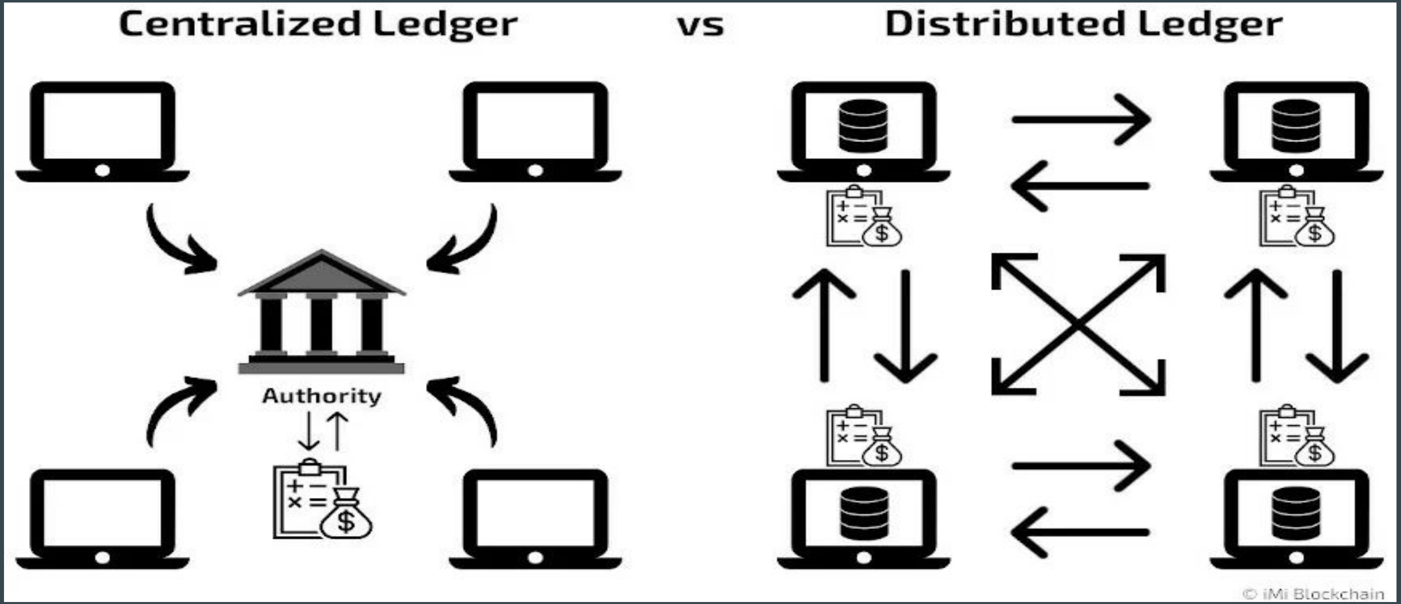
- In Centralized Ledgers transactions and terms of transactions controlled by a central authority.



Fig[2]:Centralized Ledger vs Distributed Ledger
Source:[17]

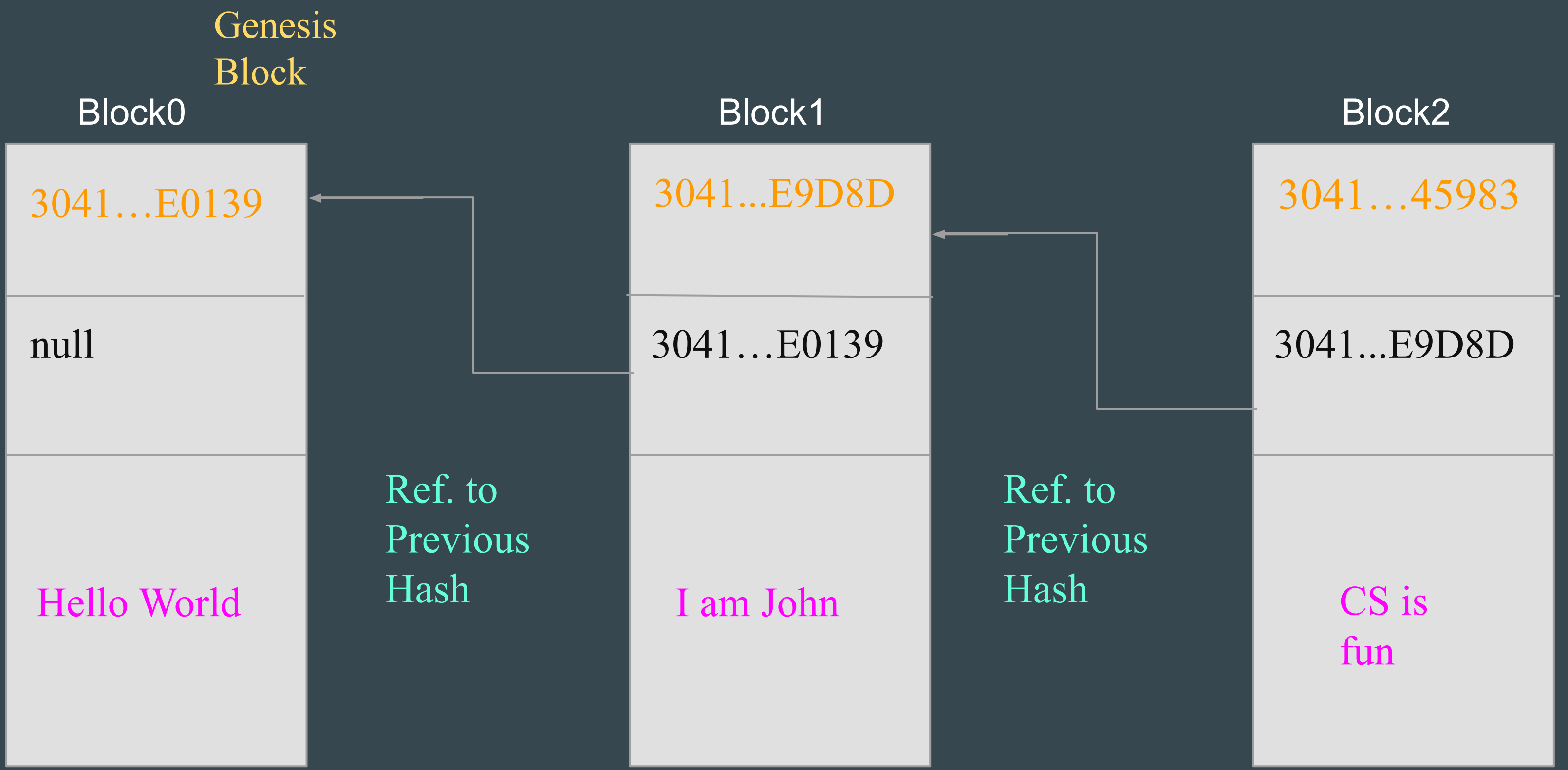
Distributed Ledgers

- In Distributed Ledgers, transactions and terms set up by parties without any intermediary.



Fig[2]:Centralized Ledger vs Distributed Ledger
Source:[17]

How does Blockchain work?



Genesis Block

Block0

3041…E0139

null

Hello World

Ref. to Previous Hash

Block1

3041...E9D8D

3041…E0139

I am John

Ref. to Previous Hash

Block2

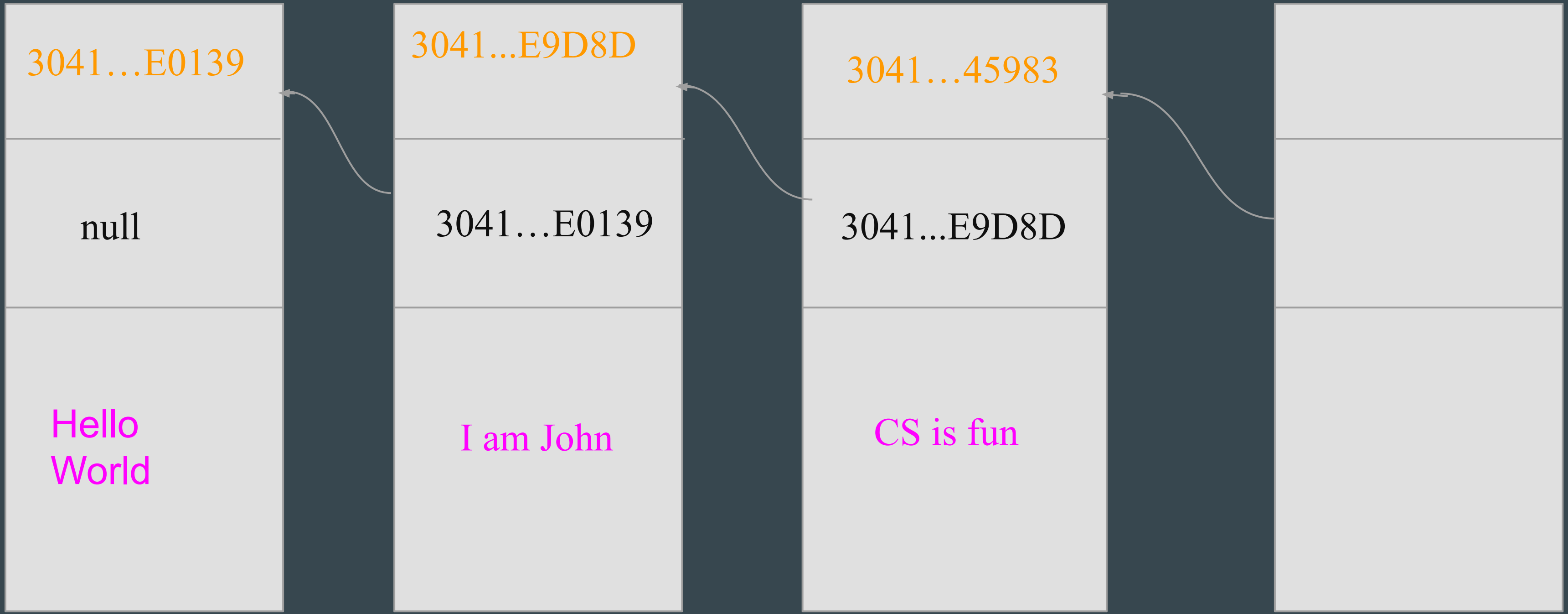
3041…45983

3041...E9D8D

CS is fun

How does blockchain work?

If we were to chain a fourth block what would be the contents of it?



3041…E0139

null

Hello World

3041...E9D8D

3041…E0139

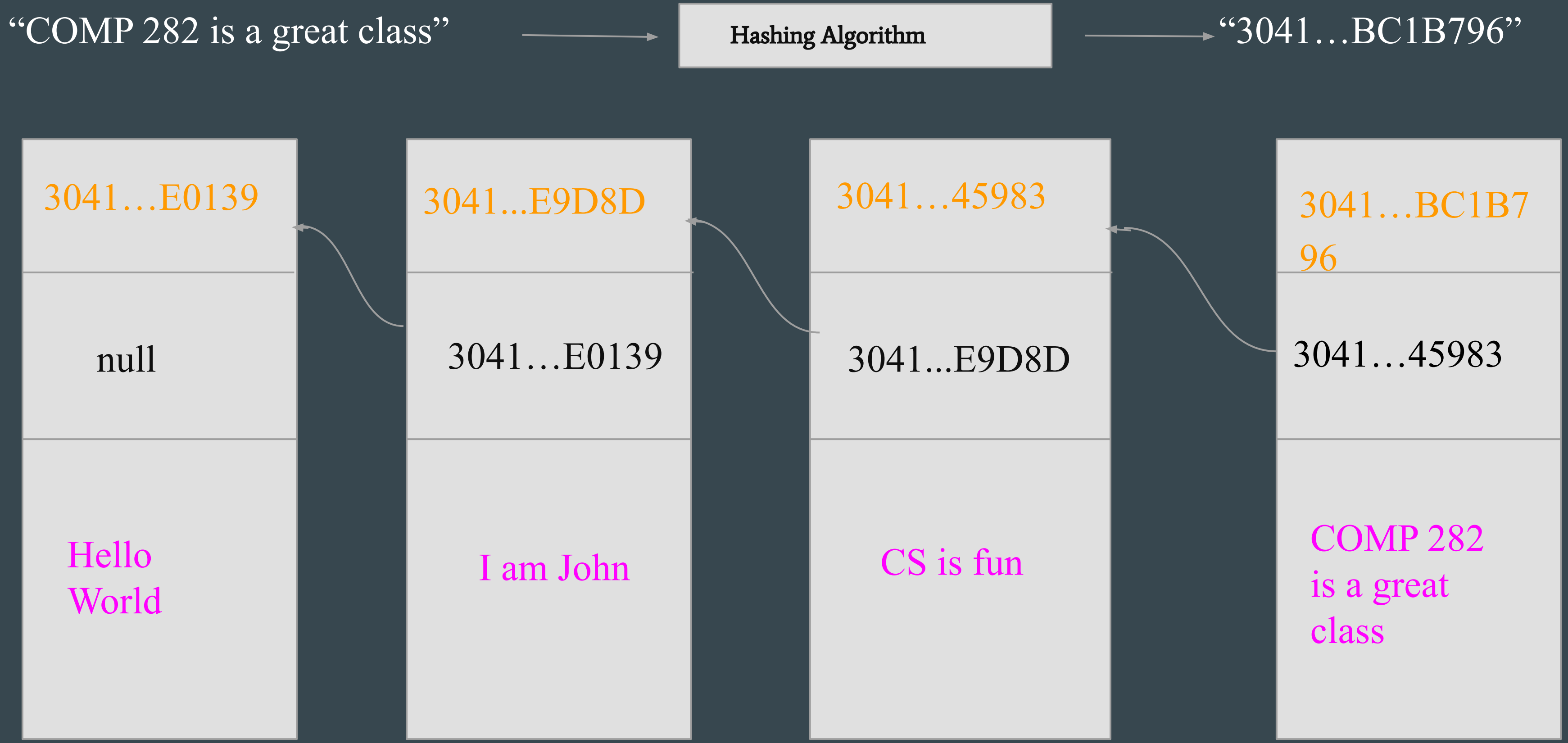
I am John

3041…45983

3041...E9D8D

CS is fun

Numerical Example Cont.



“COMP 282 is a great class” → Hashing Algorithm → “3041…BC1B796”

3041…E0139

null

Hello World

3041...E9D8D

3041…E0139

I am John

3041…45983

3041...E9D8D

CS is fun

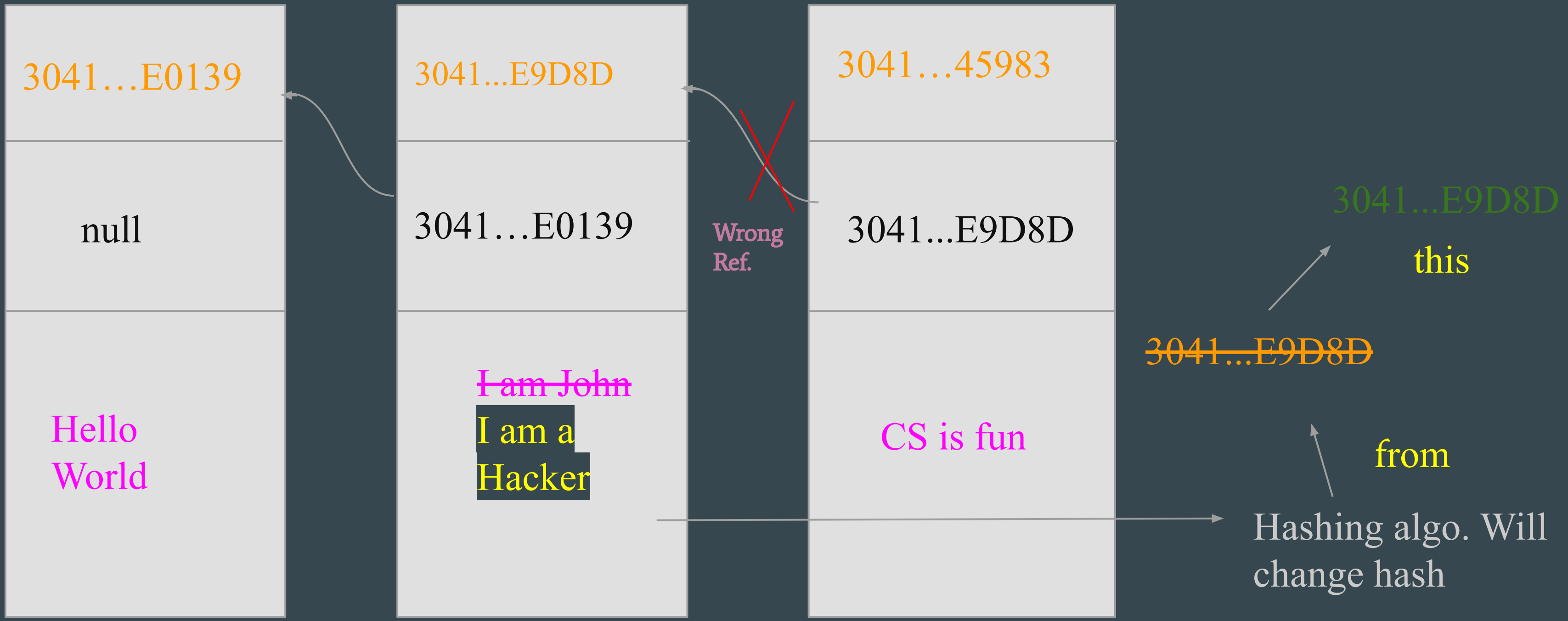
3041…BC1B796

3041…45983

COMP 282 is a great class

Special Property of Blockchain

-If a block is brute-forced and the hacker changes the data then the hashing algorithm will change the hash and the block is separate from the chain.



Pseudo Code for Implementation of Blocks

```
Block(messageArray){
        PreviousHash is null // this is genesis(first) block
        Data is equals to messageArray
        BlockHash: calculateHash(null,messageArray)
}
Block(PreviousHash,messageArray){
        this->PreviousHash is equals to PreviousHash
        Data is equals to messageArray
        BlockHash: calculateHash(PreviousHash,messageArray)
}
```

Constructor for Genesis Block

Previous Hash is null, hence not used in encryption

Constructor for a regular block with a prev. hash

Chaining the Blocks

```
Blockchain = []

function addBlock(PreviousHash,messageArray){

        Block = {

                Data:messageArray,

                previousHash: PreviousHash,

                Hash: calculateHash(PreviousHash,messageArray)

// calculating hash using ECDSA and SHA256

}

blockchain.add(Block)

}
```

Increasing Cybersecurity Breaches on Healthcare Industry

- The Department of Health and Human Services uncovered a staggering breach, with over 385 million patient records compromised [1].

- The FBI's has said that cyberattacks targeting healthcare databases have increased immensely [1].

Graph of total people affected every year from 2010-2022

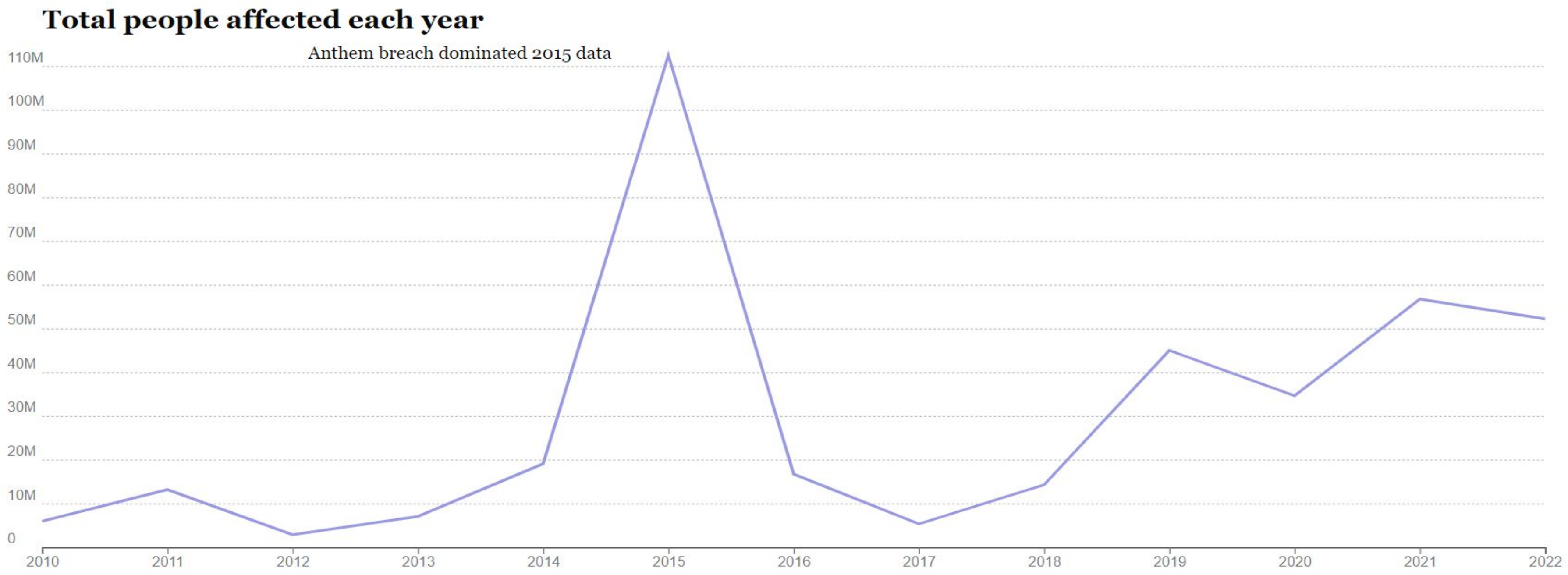
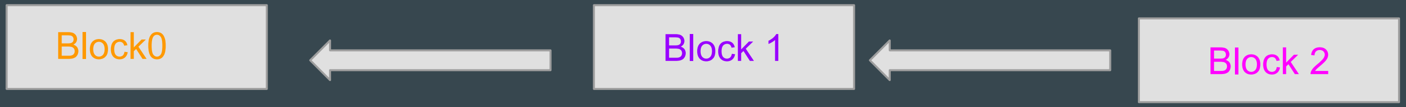


Figure 3: Total people affected each year. X-axis: years Y-axis:People compromised
Source: [1]

Is there a solution for this problem ?

- Blockchain can be used to make a secure platform.



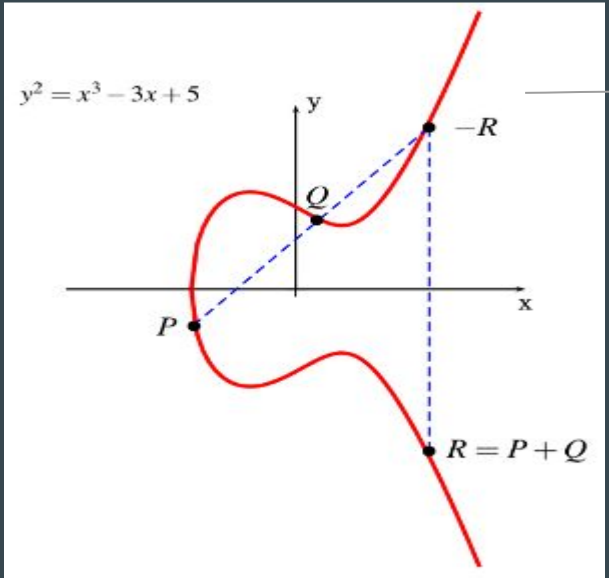
Reference to previous hash

- It uses enhanced encryption algorithms which makes it almost impossible to brute force.

- We will be using an **Elliptical Curve Digital Signature Algorithm**(one of the best encryption algorithms) to validate our blocks.[5]

Hashing: Elliptical Curve Digital Signature Algorithm(ECDSA)

- We are using ECDSA Algorithm to generate 256 bits long hash.
- ECDSA uses Elliptical Curves to generate two large prime numbers.



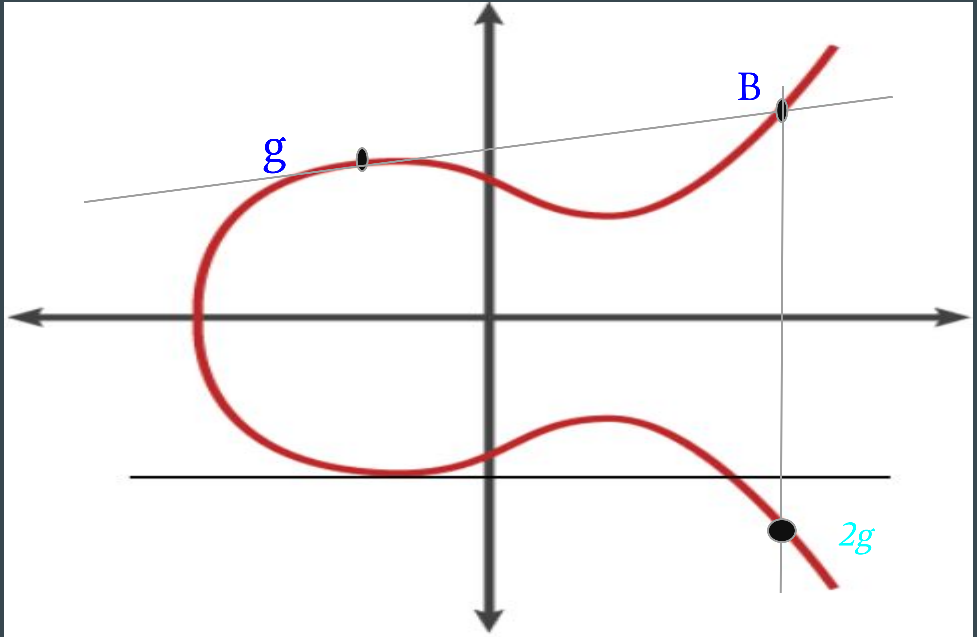
secp256r1

ECDSA cont.

Let’s take an example:

Assume *g* is a large prime number

- we plot g on the curve
  - draw tangent to point *g*
  - then plot the reflection of that point on the curve and call it *2g*
  - these points are unique and this method is called **Two Point sum**



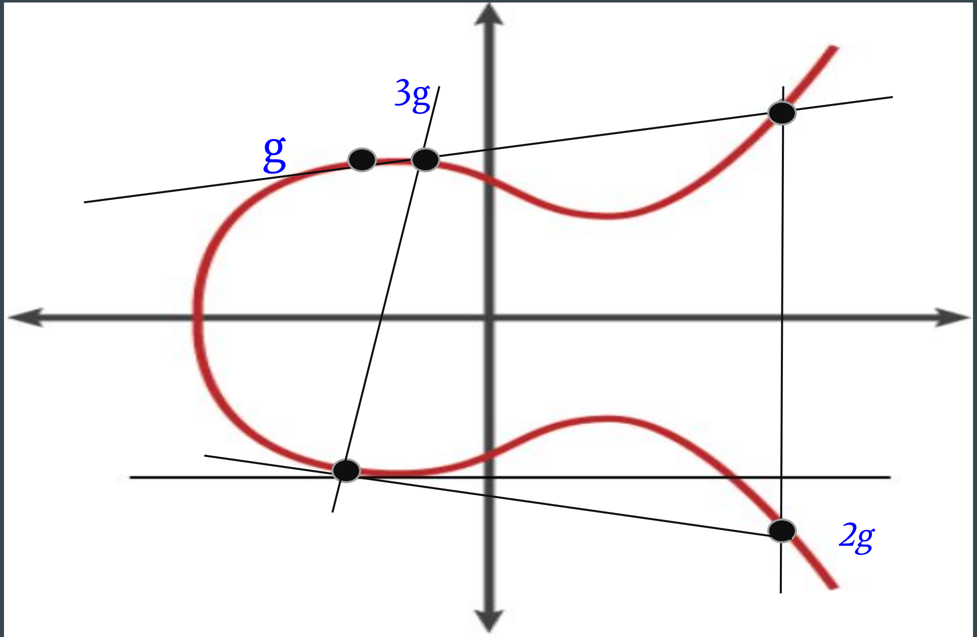
Fig[4]: Elliptical Curve Adapted from:[18]

ECDSA cont.

Let’s take an example:

Assume *g* is a large prime number

- we plot g on the curve



-then plot the reflection of that point on the curve and call it

-these points are unique and this method is called **Two Point sum**

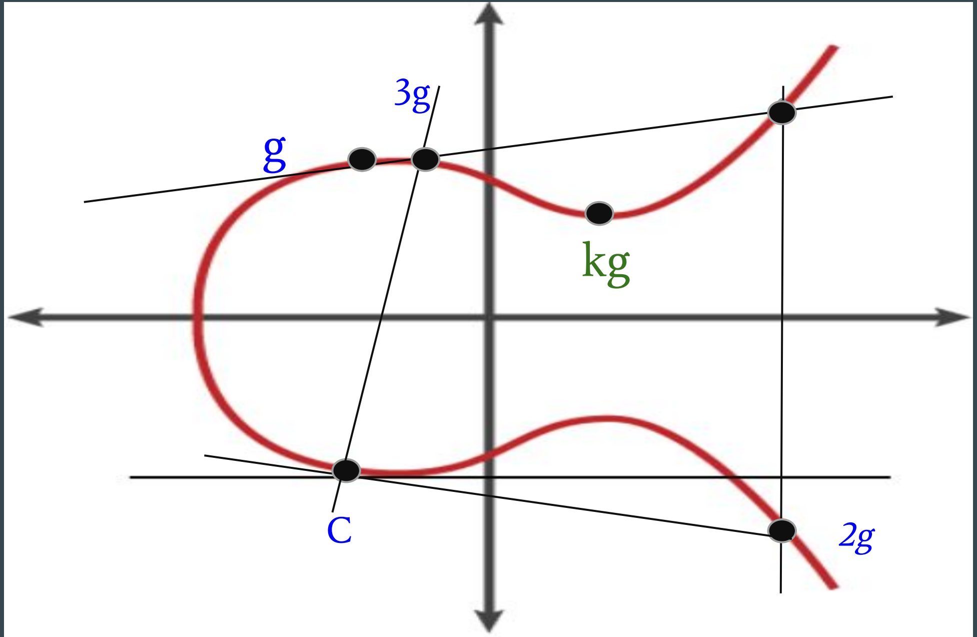
-the location of *3g* is pretty random

Fig[4]: Elliptical Curve Adapted from:[18]

ECDSA cont.

Let’s take an example:

Assume g is a large prime number



-how many time do you add g to get kg
- it is almost impossible to tell if k is large enough
- so in this case k is our private key

Fig[4]: Elliptical Curve
Adapted from:[18]

Dataset

- This is dataset is based on a paper published in the National Library of Medicine: A dataset of simulated patient-physician medical interviews with a focus on respiratory cases

- The Dataset was made by the students and researchers of Western University and Waterloo University in Canada.

- The Dataset has 287 recorded conversations between Doctors and Patients

- We will specifically be using CAR0001.txt file to secure our dataset

ECDSA: generating key pair pseudo code

- To calculate the hash we use Elliptical Curve Digital Signature Algorithm(ECDSA), which is use by the following methods

```
// Generate key pair consisting of private and public key
        Function genkeypair(dataArray, Previoushash){
//Create a combined data string for key pair generation
        combinedData equals to combinedata(dataArray,Previoushash)
// Generate a key pair using ECDSA
        keyPair equals to generateECDSAkeypair(combinedData)
        return keyPair
}
```

ECDSA: signature pseudo code

```
// Sign a message
        Function sign(messages, privatekey){
// Create an ECDSA signature for a set of messages using a private key
        signature equals createECDSASignature(messages, privatekey)
        return signature
        }
```

ECDSA: verification pseudo code

```
// Verify a Signature Using a Public Key
    Function verify(messages, signature, publicKey){
// Verify the authenticity of a signature for a set of messages using a public key
    isVerified equals verifyECDSASignature(messages, signature, publicKey)
    return isVerified
// returns true or false
    }
```

ECDSA: Converting to Hex pseudo code

```
// Convert Bytes to Hexadecimal String
    Function bytesToHex(bytes){
// Convert a sequence of bytes to a hexadecimal string
    hexadecimalString equals convertBytesToHexadecimalString(bytes)
    return hexadecimalString
    }
```

Our github repo:
https://github.com/paramdesai321/BlockchainforMedicalConsultation

Time complexity = O(N) + O(M x N) where (M x N) represents the hash function algorithm and M = size of the message to hash.[6] O(N) represents modular multiplication and modular inverse complexity.[6]

ECDSA Results

```
Block #:0
Block Hash:
304102010030130607 2A8648CE3D020106082A8648CE3D030107042730250201010420A98
52EE0F53C6CA119258A0D34FB9D9604FB2BAE1A0E3D15A2EF93FBABADB54
Previous Hash: null
Data:
D: What brought you in today?
D: OK, before we start, could you remind me of your gender and age?
D: OK, and so when did this chest pain start?
D: OK, and where is this pain located?
D: OK, and, so how long has it been going on for then if it started last night?
Block Verification: true
```

ECDSA Results Cont.

```
Block #:1
Block Hash:
3041020100301306072A8648CE3D020106082A8648CE3D03010704273025020101042
0BCE76CCCA346D9A2B0505921D94C4CD7A167F65F30E0101E677701563CA93A3B
Previous Hash:
3041020100301306072A8648CE3D020106082A8648CE3D03010704273025020101042
0A98352EE0F53C6CA119258A0D34FB9D9604FB2BAE1A0E3D15A2EF93FBABADB
54
Data:
P: Sure, I'm I'm just having a lot of chest pain and and so I thought I should get it checked
out.
P: Sure 39, I'm a male.
P: It started last night, but it's becoming sharper.
P: It's located on the left side of my chest.
P: So I guess it would be a couple of hours now, maybe like 8.
Block Verification: true
```

ECDSA Results Cont.

```
Block #:2
Block Hash:
3041020100301306072A8648CE3D020106082A8648CE3D03010704273025020101042
0C18411B67AD49345E52C395629EE125FCB70A05F6DB10CFE74CB947C955BA446
Previous Hash:
3041020100301306072A8648CE3D020106082A8648CE3D03010704273025020101042
0BCE76CCCA346D9A2B0505921D94C4CD7A167F65F30E0101E677701563CA93A3B
Data:
D: OK. Has it been constant throughout that time, or uh, or changing?
D: OK, and how would you describe the pain? People will use words sometimes like
sharp, burning, achy.
D: Sharp OK. Uh, anything that you have done tried since last night that's made the pain
better?
D: OK, so do you find laying down makes the pain worse?
D: OK, do you find that the pain is radiating anywhere?
Block Verification: true
```

ECDSA Results Cont.

```
Block #:3
Block Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420
4602E90B7266CEC2C6336C91486457E8EB4E0DE8EB488FE27F96EE97CB7511D8
Previous Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420
C18411B67AD49345E52C395629EE125FCB70A05F6DB10CFE74CB947C955BA446
Data:
P: I would say it's been pretty constant, yeah.
P: I'd say it's pretty sharp, yeah.
P: Um not laying down helps.
P: Yes, definitely.
P: No.
Block Verification: true
```

ECDSA Results Cont.

Block #:4
Block Hash:
304102010030130607 2A8648CE3D020106082A8648CE3D030107042730250201010420 6A1DF72BFE09FA0FC9BA40092EEDE23047E7E00A6BE8ED1DDD1387717B7DBE5D
Previous Hash:
304102010030130607 2A8648CE3D020106082A8648CE3D030107042730250201010420 4602E90B7266CEC2C6336C91486457E8EB4E0DE8EB488FE27F96EE97CB7511D8
Data:
D: OK, and is there anything else that makes the pain worse besides laying down?
D: OK, so not like taking a deep breath or anything like that?
D: OK. And when the pain started, could you tell me uh, could you think of anything that you were doing at the time?
D: OK, so you didn't feel like you hurt yourself when you were doing that?
D: OK, and in regards to how severe the pain is on a scale of 1 to 10, 10 being the worst pain you've ever felt, how severe would you say the pain is?
Block Verification: true

ECDSA Results Cont.

```
Block #:5
Block Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420005115072
0FAC84631BF3F6D8D4DC9FEA06F5CC8D61408103349C128F66B25B9
Previous Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420577A802C
0AE811E5251F3C81C7B30370F935D826BAD6C8DEAC0D114FD1DE02A3
Data:
P: Not that I've noticed, no.
P: Maybe taking a deep breath. Yeah.
P: I mean, I was moving some furniture around, but, that I've done that before.
P: No.
P: I'd say it's like a seven or eight. It's pretty bad.
Block Verification: true
```

Contributions

- There are many contributions to healthcare and blockchain, but the problem is that these networks are not highly secured.

- The possibilities of hacking into a blockchain secured network with ECDSA is incredibly low.

- ECDSA has been used a couple times within research, but we will also be implementing smart contracts to help us complete the algorithm.

Contributions Cont.

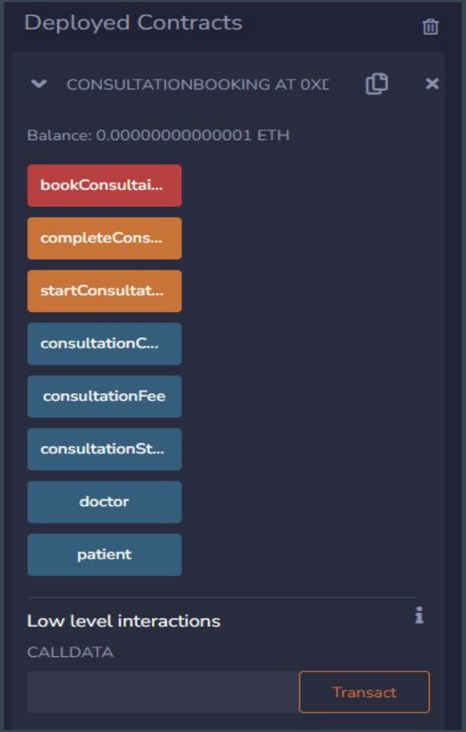
- Smart contracts are important to blockchain because it helps two parties secure transactional data directly without a third party.

- We believe that the contracts will help doctors and patients be more secure because there are only two parties.

- We hope that our contribution using ECDSA and smart contracts will help further the security of healthcare industries with zero to no penetration in the network!

Contributions Cont.

- Smart Contracts are programs in blockchain that are run when certain conditions are met.
- The speciality of smart contracts are they completely Decentralized i.e they do not need third parties
- We are using them for patients to book consultations and transaction related that


Deployed Contracts

CONSULTATIONBOOKING AT 0XD

Balance: 0.00000000000001 ETH

Comparisons and Conclusions

RSA (Rivest Shamir Adleman)

- Rsa is the algorithm we decided to compare with ECDSA.

- Rsa is a cryptographic number system that uses large prime number factorization. [13]

- It is extremely hard to crack due to the complexity of finding extremely large prime numbers.

RSA Pseudo code

```
// Key Generation
(public_key, private_key) = generateKeyPair()

// public_key is (n, e), private_key is (n, d)
// Encryption

ciphertext = encrypt(public_key, plaintext)

// Decryption

plaintext = decrypt(private_key, ciphertext)
```

Time Complexity = O(K*log(N))
Where K is the number of iterations and N is the prime number

RSA Pseudo Code Cont.

```
// Key Pair Generation

function generateKeyPair():
    p = generatePrimeNumber()                // Generate a prime number p
    q = generatePrimeNumber()                // Generate a prime number q
    n = p * q                                // Compute n as the product of p and q
    phi = (p - 1) * (q - 1)                  // Calculate φ(n)
    e = chooseEncryptionExponent(phi)                  // Choose an encryption exponent e
    d = calculateDecryptionExponent(e, phi)   // Calculate the decryption exponent d
    return (public_key(n,e), private_key(n, d))
```

RSA Results

```
Block #0
Previous Hash:null
Original message: P: Sure, I'm I'm just having a lot of chest pain and and so I thought I should get it
checked out.
Hash:
342509343913861845163315311327797263442711035439571332882034740862726593135394761З
8230599727441888383714491247334829447249230683027604614954201982499531526271163481
0910408227673343093004362145262791138407346172539891992897672446291535587100467359
8227652716990748672927149864061243565329679931876736513207528444131469543098906245
9783890733260902277336544023987897019476096030631568397040111246771290399176263394
5874774669191059725821024421643560993953870041618317274068448840117534468127748065
6648775807550331737771756226197678538492149160220368633384540234752306799657376806
835622899081787693386261519398125922202871
Decrypted message: P: Sure, I'm I'm just having a lot of chest pain and and so I thought I should get it
checked out.
```

RSA Results Cont.

Block #1
Original message: P: Sure 39, I'm a male.
Hash:
87269268051272860719414371595813699325075336997347839928394087090650534883348016199062355583774481121750110402345077726852024871131561967055151328276480147409650280566527248258995288329784903599814023705925477947965229958958508594937053796724803502587045522690347701237509606697296943585039525417118538522893161010513030800788932397427881881252243962466967939533773961263505293344061971358221875907072464479186432530484920473501014819587107593844383162140028224425020106506348660987050163078373266707007847187508795037203663571441049983958026744194707724944933228330060874097397863357898831267025701426378458060931 67

Previous
Hash:342509343913861845163315311327797263442711035439571332882034740862726593135394761382305997274418883837144912473348294472492306830276046149542019824995315262711634810910408227673343093004362145262791138407346172539891992897672446291535587100467359822765271699074867292714986406124356532967993187673651320752844413146954309890624597838907332609022773365440239878970194760960306315683970401112467712903991762633945874774669191059725821024421643560993953870041618317274068448840117534468127748065664877580755033173777175622619767853849214916022036863338454023475230679965737680683562289908178769338626151939812592220287 1

RSA Results Cont.

Block #2

Original message: P: It started last night, but it's becoming sharper.

Hash:
3922818352893269312104169478875934733167947511512444714273146300279045802628125566999086641182930677309537631338843276508348357311009643077141759808347758477994080610591982317110874856323373248635942654153578885852278688071700588962155443795439467595504528082755397567925379843514928584083594954247106289141622323636094327636262801491871459076620265261431192114216996958680758559324825375332078495585959316133544625042654749351242277680349979187834848366477854548832408932422185133963393818790857294952433780861012499429066591895518559791061329099780196489994579125630913644579275697455858865529993358550718749560349

Previous Hash:
4628075502224030347848043723228153138374029722660552936830919340203881214401364034942375313958705056290884434759800912858327693502174655931670331165874878654541106194904149649433175004252831059356380272339495614374072939905622434748755453024966230477252810209592376598308766975291349720561999887082952958845816163400318612800118480483566245517631464609812815708674960976183971733151378552744736679057614378399751004682522026336832937600926881783645726100310007046872873317988860033229791759059032611980130879923166332306060953932665425978484725959852954618504355525296341729136215900008395161722405587924129962562162

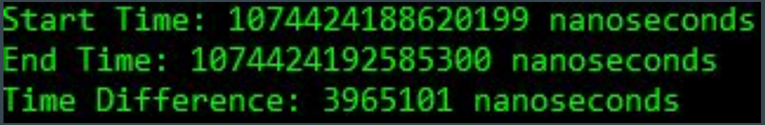
ECDSA vs RSA results comparison

ECDSA

Block #:0
Block Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420A983
52EE0F53C6CA119258A0D34FB9D9604FB2BAE1A0E3D15A2EF93FBABADB54
Previous Hash: null
Data:
D: What brought you in today?
D: OK, before we start, could you remind me of your gender and age?
D: OK, and so when did this chest pain start?
D: OK, and where is this pain located?
D: OK, and, so how long has it been going on for then if it started last night?
Block Verification: true

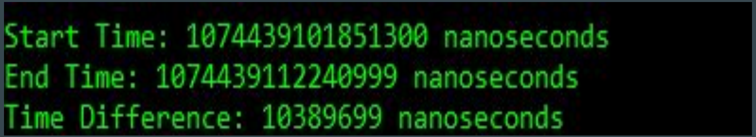
256 bits

Block #:1
Block Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420BCE
76CCCA346D9A2B0505921D94C4CD7A167F65F30E0101E677701563CA93A3B
Previous Hash:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420A983
52EE0F53C6CA119258A0D34FB9D9604FB2BAE1A0E3D15A2EF93FBABADB54
Data:
P: Sure, I'm I'm just having a lot of chest pain and and so I thought I should get it checked out.
P: Sure 39, I'm a male.
P: It started last night, but it's becoming sharper.
P: It's located on the left side of my chest.
P: So I guess it would be a couple of hours now, maybe like 8.
Block Verification: true



```
Start Time: 1074424188620199 nanoseconds
End Time: 1074424192585300 nanoseconds
Time Difference: 3965101 nanoseconds
```

RSA



```
Start Time: 1074439101851300 nanoseconds
End Time: 1074439112240999 nanoseconds
Time Difference: 10389699 nanoseconds
```

Block #0
Previous Hash:null
Original message: P: Sure, I'm I'm just having a lot of chest pain and and so I thought I should get it checked out.
Hash:
3425093439138618451633153113277972634427110354395713328820347408627265931353947613823059972744188838371449124733482944724923068302760461495420198249953152627116348109104082276733430930043621452627911384073461725398919928976724462915355871004673598227652716990748672927149864061243565329679931876736513207528444131469543098906245978389073326090227733654402398789701947609603063156839704011124677129039917626339458747746691910597258210244216435609939538700416183172740684488401175344681277480656648775807550331737771756226197678538492149160220368633384540234752306799657376806835622899081787693386261519398125922202871

Decrypted message: P: Sure, I'm I'm just having a lot of chest pain and and so I thought I should get it checked out.

Block #1
Original message: P: Sure 39, I'm a male.

2048 bits

Hash:
8726926805127286071941437159581369932507533699734783992839408709065053488334801619906235558377448112175011040234507772685202487113156196705515132827648014740965028056652724825899528832978490359981402370592547794796522995895850859493705379672480350258704552269034770123750960669729694358503952541711853852289316101051303080078893239742788188125224396246696793953377396126350529334406197135822187590707246447918643253048492047350101481958710759384438316214002822442502010650634866098705016307837326670700784718750879503720366357144104998395802674419470772494493322833006087409739786335789883126702570142637845806093167

Previous
Hash:3425093439138618451633153113277972634427110354395713328820347408627265931353947613823059972744188838371449124733482944724923068302760461495420198249953152627116348109104082276733430930043621452627911384073461725398919928976724462915355871004673598227652716990748672927149864061243565329679931876736513207528444131469543098906245978389073326090227733654402398789701947609603063156839704011124677129039917626339458747746691910597258210244216435609939538700416183172740684488401175344681277480656648775807550331737771756226197678538492149160220368633384540234752306799657376806835622899081787693386261519398125922202871

Decrypted message: P: Sure 39, I'm a male.

ECDSA vs RSA

Pros

- ECDSA results have hexadecimal hash codes
- ECDSA also has a smaller bit hashcode
- Time complexity for ECDSA is O(N)+ O(M x N) [6]

  (M = size of the message to hash)

Cons

- It is not universally compatible with all clients and servers
- Key management within ECDSA is harder to manage to ensure secure elliptic curve hashes
- ECDSA has a higher complexity in implementing its algorithm due to the strict mathematics going into elliptic curves

Limitations

- Privacy and data security with ECDSA is very impactful, but sometimes data can be really secure to the point where the data is immutable.

- As the blockchain network with ECDSA increases and adds more patients, then the scalability of the network becomes a problem increasing the amount of blocks and data added into the network.

- A specific limitation we hit with this project are Proof of work and smart contracts.

- Use of Proof of Work within our blockchain system is impractical because of smaller peer-to-peer network.

- Smart contracts have difficult implementation methods when dealing with java code, which means that a different interface is needed to make the java code compatible with those contracts(Web3j).

Future Work

- Specifically we wanted to add blockchain solidity contracts to activate functions within the network.

- This would make it easier to authenticate new users/patients into the networks and gives access to that network.

- This has been used in past research and has proven that blockchain within a medical network can be secure with the right implementation of a efficient hashing algorithm[4][6][8] .

References Slide

[1] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *2018 International Conference on Information Networking (ICOIN), Jan. 10-12, 2018, Chiang Mai, Thailand.* [Online] Available: IEEE Xplore, https://ieeexplore.ieee.org/abstract/document/8343163?casa_token=ukvIJEJc41MAAAAA:jbAanQJhyCe4U2U95l6lpVcAh-C3LmX86T7Tb0n-K6ozOXS_SZPzIJA7ywNMNPPleS08KIL6NQ

[2] S. Liss and J. Ye Han "Hacking healthcare: With 385M patient records exposed, cybersecurity experts sound alarm on breach surge," *Healthcare Dive*. Mar. 09, 2023. [Online]. https://www.healthcaredive.com/news/cybersecurity-hacking-healthcare-breaches/643821/#:~:text=The%20number%20of%20breaches%20reported [Accessed: Oct. 10, 2023]

[3] V. Gupta, "A Brief History of Blockchain," *Harvard Business Review*, Apr. 05, 2017. [Online]. https://hbr.org/2017/02/a-brief-history-of-blockchain [Accessed:Oct. 10, 2023]

[4] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain," in *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Oct. 27-30, 2015, Osaka, Japan*. [Online] Available: IEEE Xplore, https://ieeexplore.ieee.org/abstract/document/7398721?casa_token=Hr7MgxJrOGwAAAAA:PeoYTJAayKPCZaejKwdymSOJHlnYDrHIGBsgRBTfLq4fX0C8R7Z1esiYAmZblK6leVoimUZg

[5] A. Andi, C. Juliandy, R. Robert, and O. Pribadi, "Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain," *CommIT (Communication and Information Technology) Journal*, vol. 16, no. 1, pp. 87–96, Mar. 2022. https://doi.org/10.21512/commit.v16i1.7958.

[6] J. Petit, "Analysis of ECDSA Authentication Processing in VANETs," 2009 3rd International Conference on New Technologies, Mobility and Security, Cairo, Egypt, 2009, pp. 1-5, doi: 10.1109/NTMS.2009.5384696.

References Slide Cont.

[7] A. T. Sherman, F. Javani, H. Zhang and E. Golaszewski, "On the Origins and Variations of Blockchain Technologies," *IEEE Security & Privacy,* vol. 17, no. 1, pp. 72-77, Mar. 2019. [Online] Available: IEEE Xplore, https://ieeexplore.ieee.org/document/8674176

[8] T. Kuo, H. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications”, *Journal of the American Medical Informatics Association*, vol. 24, no. 6, p. 1211–1220, Nov. 2017. [Online]. Available: Oxford Academic, https://doi.org/10.1093/jamia/ocx068

[9] D. Puthal, N. Malik, S. P. Mohanty, et al, "The Blockchain as a Decentralized Security Framework [Future Directions]," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, p. 18-21, Mar. 2018, doi: 10.1109/MCE.2017.2776459

[10] Computerphile, Nottingham, U.K. *Secret Key Exchange (Diffie-Hellman) - Computerphile.* (Dec. 15, 2017). Accessed: Oct. 19, 2023. [Online Video]. Available: https://youtu.be/NmM9HA2MQGI?si=JdZCGv6dPIY_M5mf

[11] L. Hartikka, “naivechain,” *github.com/lhartikk/naivechain,* main.js, Oct. 9, 2016. [Online]. Available: https://github.com/lhartikk/naivechain/blob/master/main.js#L108. [Accessed: Oct. 19, 2023]

[12] C. W. Smith, F. Fareez, T. Parikh, et al, “Collection of simulated medical exams”. figshare, Jun. 8, 2022 [Online]. Available: https://springernature.figshare.com/articles/dataset/Collection_of_simulated_medical_exams/16550013/1. [Accessed: Oct. 9, 2023]

[13] S. M. Bamakan, A. Motavali, and A. Babaei Bondarti, “A survey of Blockchain Consensus Algorithms Performance Evaluation Criteria,” *Expert Systems with Applications*, v ol. 154, p. 113385, 2020. doi:10.1016/j.eswa.2020.113385

[14] X. Zhou and X. Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption," in Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216

[15] F. M. Benčić and I. Podnar Žarko, "Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph," 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2018, pp. 1569-1570, doi: 10.1109/ICDCS.2018.00171.

[16] R. Minni, K. Sultania, S. Mishra and D. R. Vincent, "An algorithm to enhance security in RSA," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 2013, pp. 1-4, doi: 10.1109/ICCCNT.2013.6726517.

Reference Slides Cont.

[17] G. Benjamin,”Distributed Ledger Technology”,BLOCKCHAIN VS DISTRIBUTED LEDGER TECHNOLOGY, IMi Blockchain, Oct 11, 2023. Available:https://imiblockchain.com/blockchain-vs-distributed-ledger-technology/ [Accessed: Nov 14, 2023].

[18] “Introduction to ECC”, Sept. 2023, *Roll your own Crypto.*[Online] Available:https://onyb.gitbook.io/roll-your-own-crypto/introduction. [Accessed: Nov 14, 2023]

[19] “Distributed Ledgers”, *Corporate Finance Institute.*[Online] Available:https://corporatefinanceinstitute.com/resources/cryptocurrency/distributed-ledgers/ [Accessed: Nov. 16, 2023]