Bitcoin & Cryptocurrency

Priya R L

Department of Computer Engineering, VESIT, Mumbai

Agenda

- Course Overview
- Why there is a hype in Blockchain?
- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is Blockchain ?
- P2P Network in Blockchain - Challenges & Solutions

University of Mumbai Blockchain											
Year & Sem	Course Code and Course Title	Teaching Scheme Hours / Week			Examination Scheme and Marks						Credit Scheme
		Theory	Seminar / Tutorial	Pract	Internal Assessment		End Sem Exam	Term Work	Oral/ Pract	Total	Credits
					Mid Term	Continuous Assessment					
TE Sem V	HBCC501: Bitcoin and Crypto currency	04	--	--	20	20	60	--	--	100	04
	Total	**04**	**-**	**--**	**100**			**-**	**-**	**100**	**04**
Total Credits = 04											

Sr. No.	Course Objectives
The course aims:	
1	To get acquainted with the concept of Block and Blockchain.
2	To learn the concepts of consensus and mining in Blockchain.
3	To get familiar with the bitcoin currency and its history.
4	To understand and apply the concepts of keys, wallets and transactions in the Bitcoin Network.
5	To acquire the knowledge of Bitcoin network, nodes and their roles.
6	To analyze the applications& case studies of Blockchain.

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Describe the basic concept of Block chain.	L1,L2
2	Associate knowledge of consensus and mining in Block chain.	L1,L2
3	Summarize the bit coin crypto currency at an abstract level.	L1,L2
4	Apply the concepts of keys, wallets and transactions in the Bit coin network.	L3
5	Interpret the knowledge of Bit coin network, nodes and their roles.	L1,L2
6	Illustrate the applications of Block chain and analyze case studies.	L3

HBCC501 : Blockchain Development - Assessment (100 Marks)

Direct Assessment

- End Semester Exam (Full syllabus, Duration : 2 hours) : **60 Marks**
- Internal Assessment : **40 Marks**
  - Mid Term Test (50% syllabus, Duration : 1 hour) - **20 marks**
  - Continuous Assessment - **20 marks**

Indirect Assessment (Extra Assignment - Case Study) - 25 Marks

Rubrics considered for Continuous Assessment from Syllabus :

1. ** Certificate course NPTEL/ Coursera/Udemy/any MOOC - 10 marks
2. Wins in the event/competition/hackathon - 10 marks
7. **** Participation in event / workshop / talk / competition** - **5 marks**
8. **Multiple Choice Questions (Quiz)** - **5 marks**
9. **** Case study, Presentation, group discussion** - **10 marks**
10. Question paper solution (Slow Learners) - 10 marks
11. Multiple Choice Questions (Quiz) (Slow Learners) - 5 marks
12. ** Literature review of papers/journals - 5 marks
13. Library related work (Slow Learners) - 5 marks

** Conditions Apply - Refer Syllabus

Text Books:

1. "Mastering Bitcoin, PROGRAMMING THE OPEN BLOCKCHAIN", 2nd Edition by Andreas M. Antonopoulos, June 2017, O'Reilly Media, Inc. ISBN: 9781491954386.
2. "Blockchain Applications: A Hands-On Approach", by ArshdeepBahga, Vijay Madisetti, Paperback – 31 January 2017.
3. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", July 19, 2016, by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press.

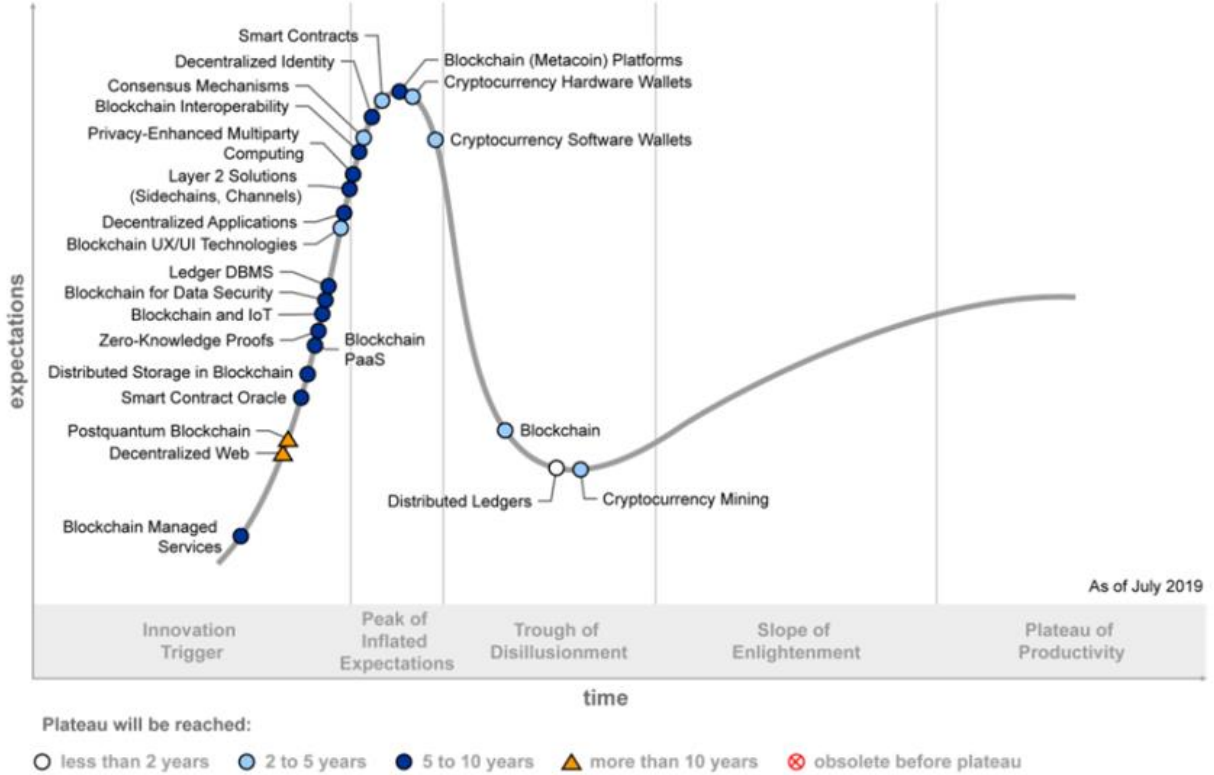
Reference Books:

1. "Mastering Blockchain", by Imran Bashir, Third Edition, Packt Publishing
2. "Mastering Ethereum: Building Smart Contracts and Dapps Paperback" byAndreas Antonopoulos, Gavin Wood, Publisher(s): O'Reilly Media
3. "Blockchain revolution: how the technology behind bitcoin is changing money, business and the world $ don tapscott and alex tapscot, portfolio penguin, 856157449

Agenda

- Course Overview
- Why there is a hype in Blockchain?
- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is Blockchain ?
- P2P Network in Blockchain - Challenges & Solutions

Why there is a hype in Blockchain?



Courtesy : https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/blockchain-hypecycle-oct-3-2019-2.png

Agenda

- Course Overview
- Why there is a hype in Blockchain?
- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is Blockchain ?
- P2P Network in Blockchain - Challenges & Solutions

Why to Learn Blockchain ?

Current Scenario

- Internet is owned by Technical Giants
- Huge Transaction fees by 3rd Parties
- Time to complete Transactions..
- Ownership for Content Creators
- Lack of Transparency

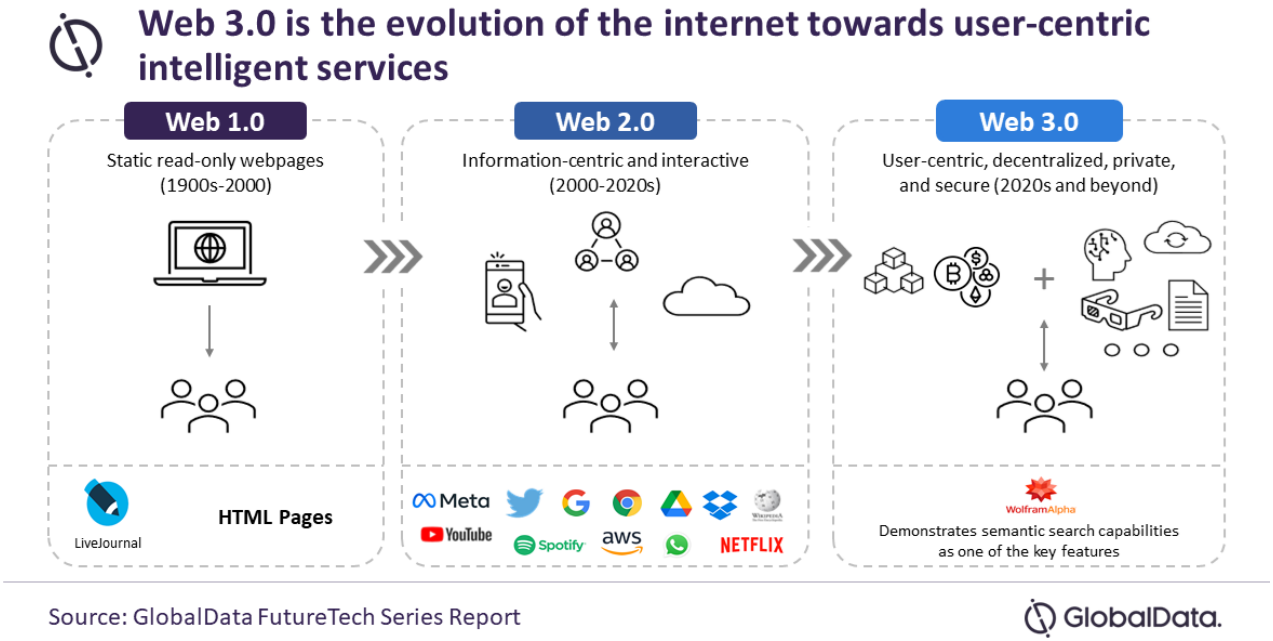
Blockchain Offers …

- Decentralized with P2P Network
- Trust in a Trustless Network
- Immutable
- Security through Cryptography
- Transparency

Agenda

- Course Overview
- Why there is a hype in Blockchain?
- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is Blockchain ?
- P2P Network in Blockchain - Challenges & Solutions

What is Web 3.0?



Courtesy : https://www.globaldata.com/wp-content/uploads/2022/03/220302_Web3.0_7and9_1.png

Agenda

- Course Overview
- Why there is a hype in Blockchain?
- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is Blockchain with an Example Scenario
- P2P Network in Blockchain - Challenges & Solutions

What is Blockchain ?

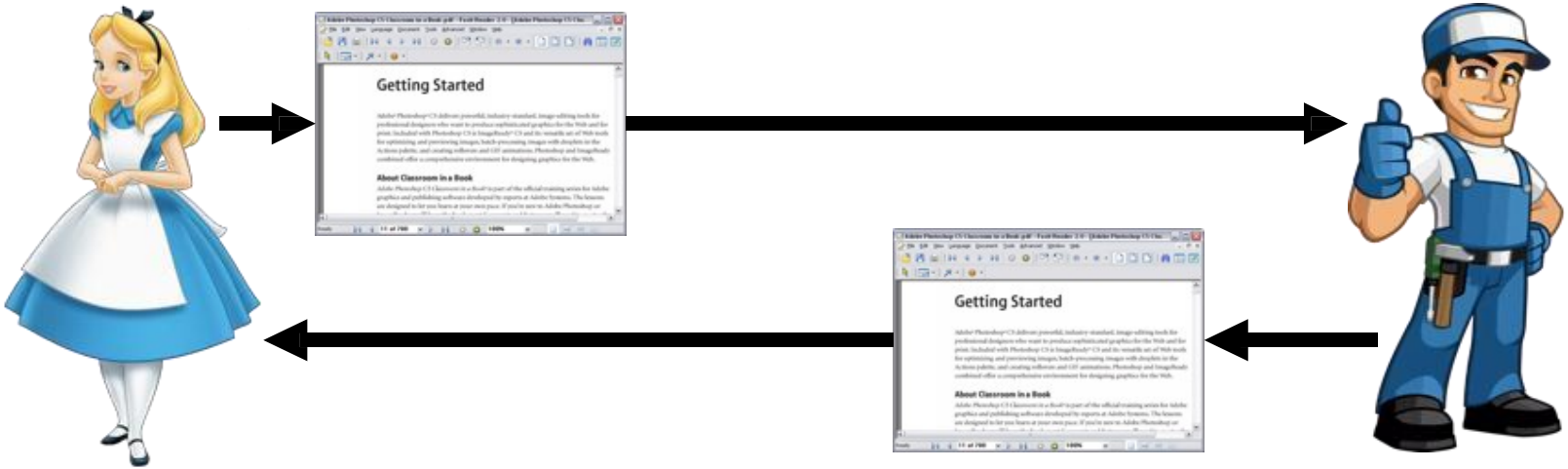
- A Blockchain is “an **open**, **distributed ledger** that can record transactions between two parties **efficiently** and in a **verifiable** and **permanent** way” (Iansiti, Lakhani 2017)

- The keywords: **Open** (accessible to all), **Distributed or Decentralized** (no single party control), **efficient** (fast and scalable), **verifiable** (everyone can check the validity of information), **permanent** (the information is persistent)

Courtesy : https://nptel.ac.in/courses/106105184

Example Scenario

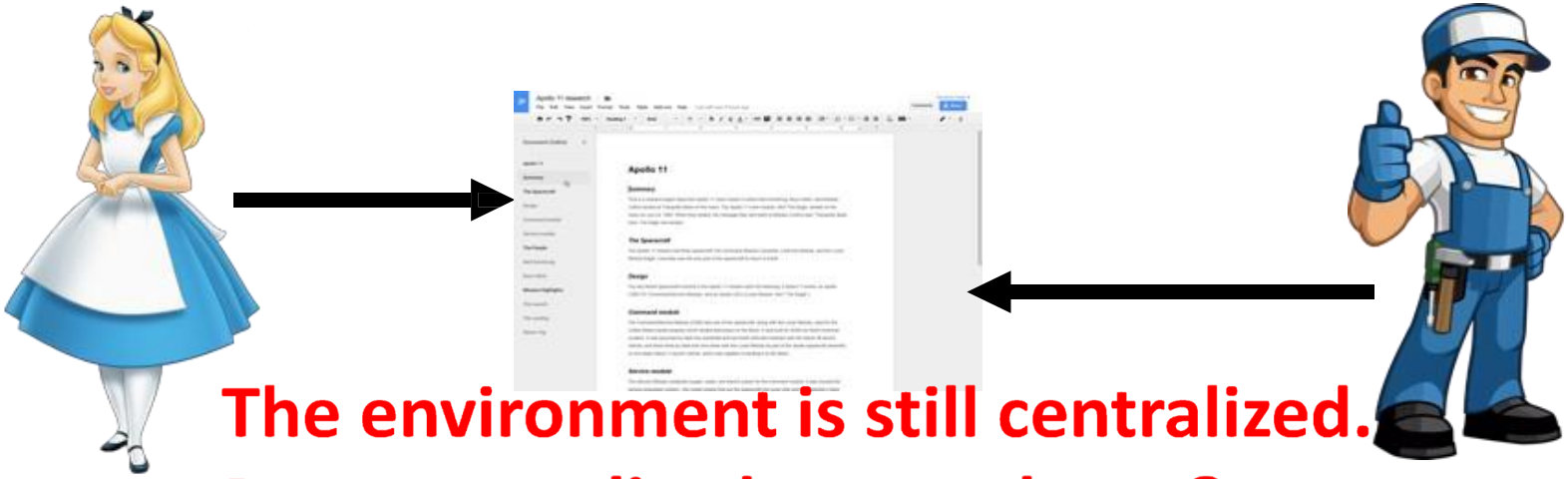
- Traditional way of sharing documents



Courtesy : https://nptel.ac.in/courses/106105184

Example Scenario

- Shared Google doc – both the users can edit simultaneously



The environment is still centralized.

Does centralized system harm?

Courtesy : https://nptel.ac.in/courses/106105184

Example Scenario

Problems with a Centralized System

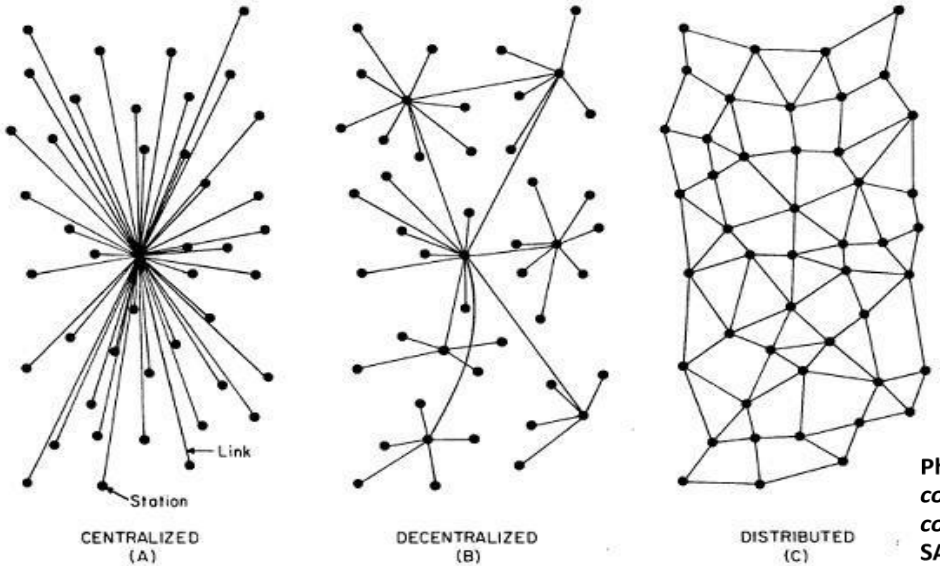
A single point of failure

- If you do not have sufficient bandwidth to load Google doc, you'll not be able to edit
- What if the server crashes?

Courtesy : https://nptel.ac.in/courses/106105184

Example Scenario

Centralized vs Decentralized vs Distributed



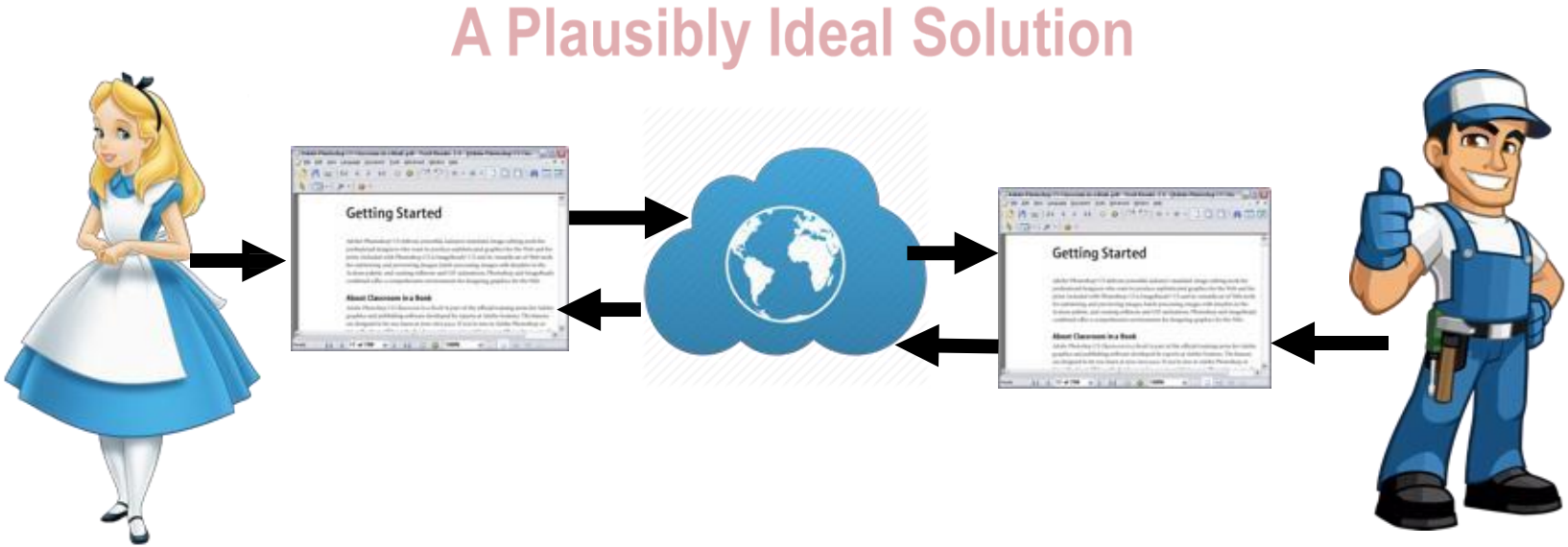
Complete reliance on single point (centralized) is not safe

- **Decentralized: Multiple points of coordination**
- **Distributed: Everyone collectively execute the job**

Photo courtesy: Baran, Paul. *On distributed communications: I. Introduction to distributed communications networks.* No. RM3420PR. RAND CORP SANTA MONICA CALIF, 1964.

Courtesy : https://nptel.ac.in/courses/106105184

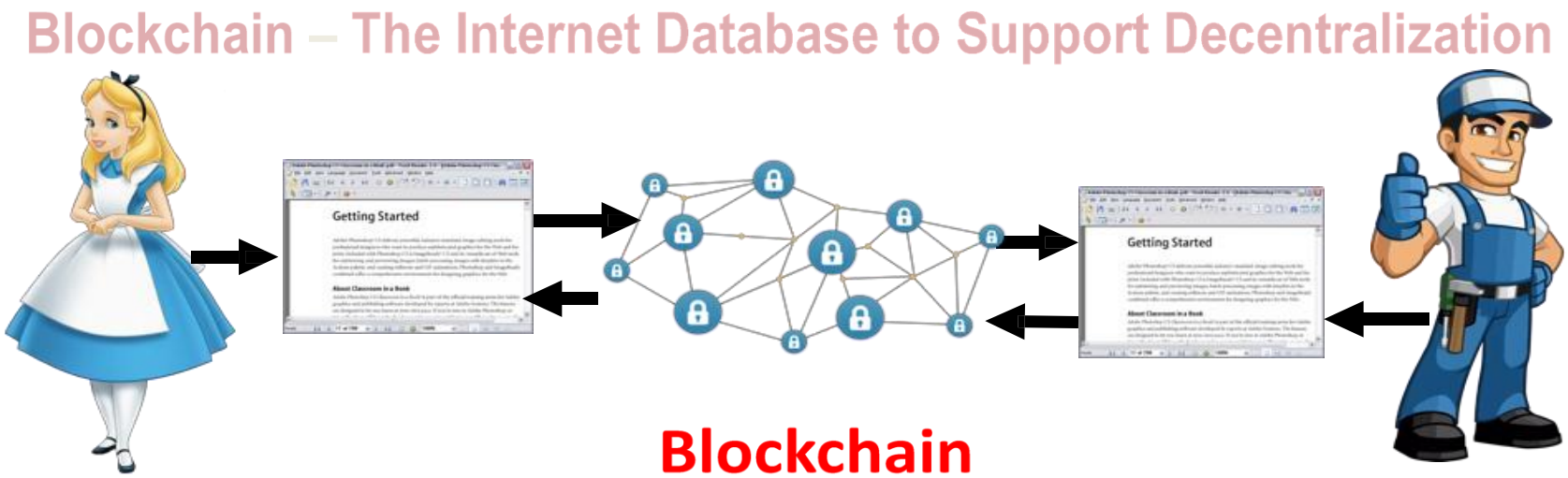
Example Scenario



Everyone edits on their local copy of the document – the Internet takes care of ensuring consistency

Courtesy : https://nptel.ac.in/courses/106105184

Example Scenario



A decentralized database with strong consistency support

Courtesy : https://nptel.ac.in/courses/106105184

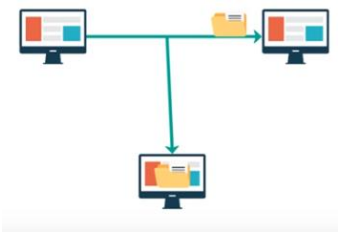
Agenda

- Course Overview
- Why there is a hype in Blockchain?
- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is Blockchain? With an example Scenario
- P2P Network in Blockchain - Challenges & Solutions

P2P Network in Blockchain

Challenges

1. **Confidentiality**
2. **Integrity**
3. **Non-repudiation**
4. **Authentication**



Solution

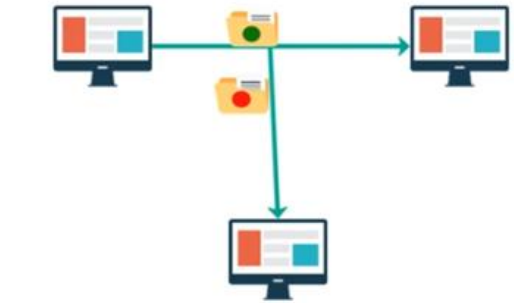
- **Cryptography**

Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

P2P Network in Blockchain

Challenges

1. **Confidentiality**
2. **Integrity**
3. **Non-repudiation**
4. **Authentication**

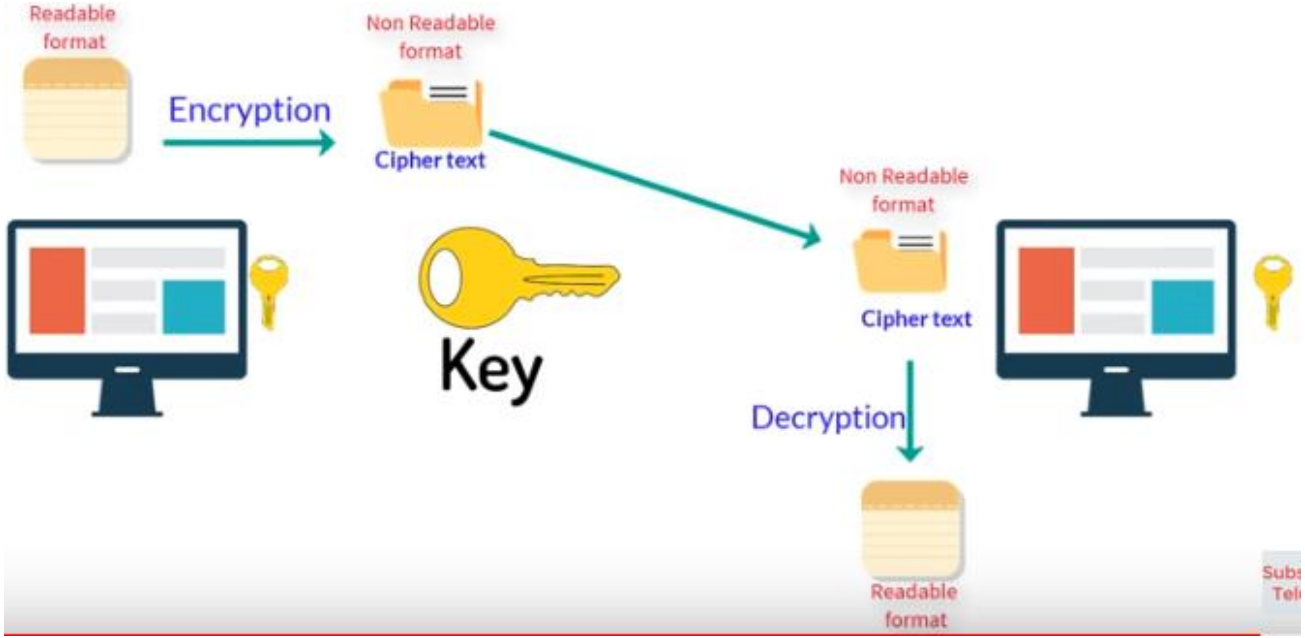


Solution

- **Cryptography**

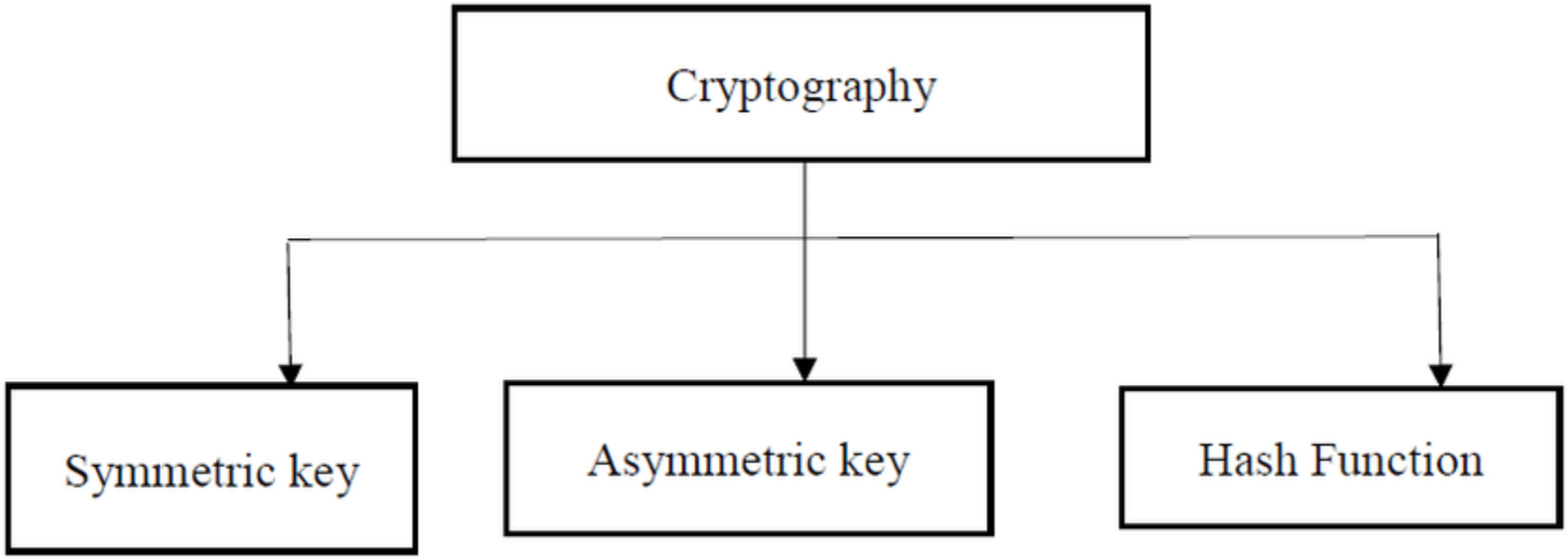
Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

P2P Network in Blockchain → Cryptography

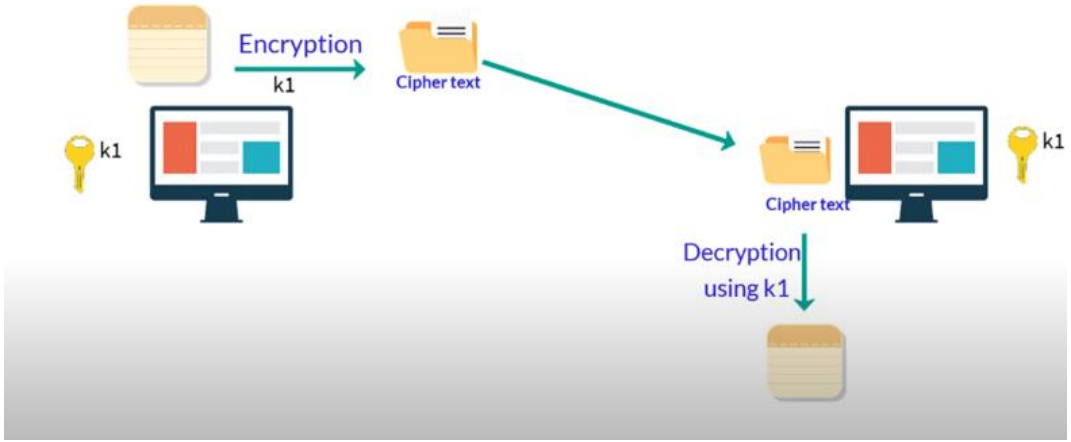


Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Cryptography - Types



Symmetric Key Cryptography

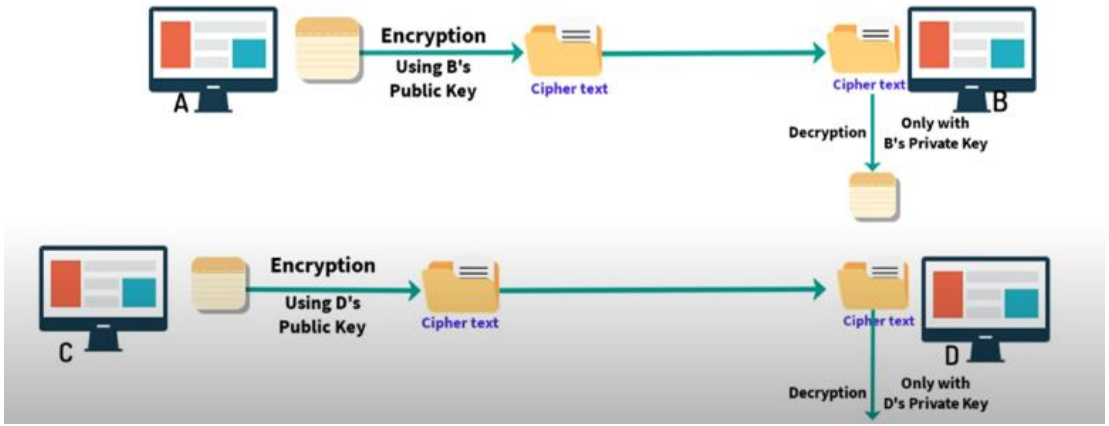


Challenges

- **Key must be secure**
- **Need for Frequent Key changes**
- **Key Distribution Problem**
- **# Communication pairs**

Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Public Key or Asymmetric Key Cryptography



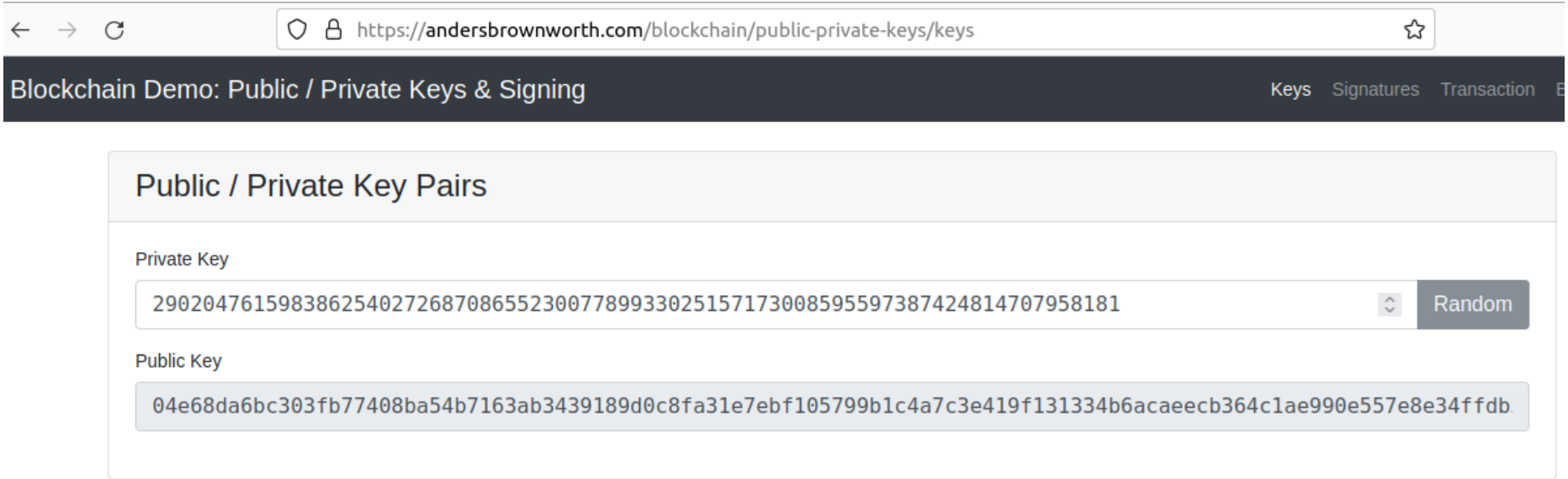
Challenges

- **Require a pair of keys**
- **Expensive to generate**
- **Not efficient for long messages**
- **Require High Computational Power**

Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Asymmetric Key Generation - Demo

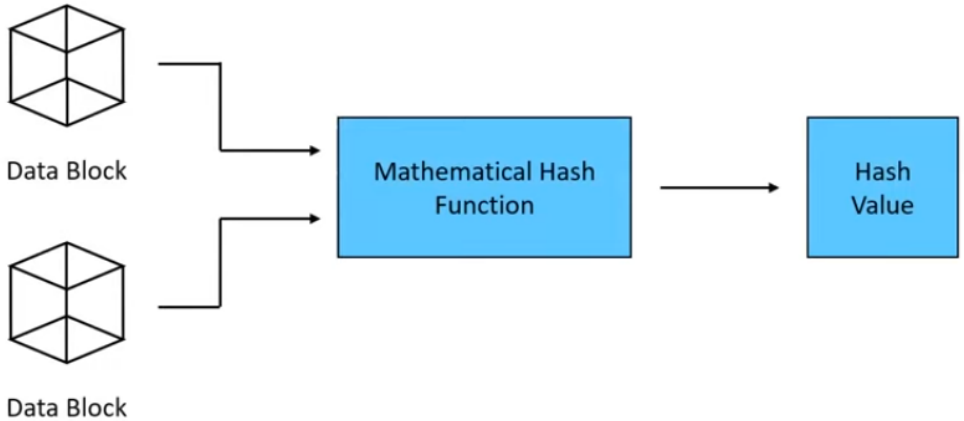
Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/keys



Cryptographic Hash Functions

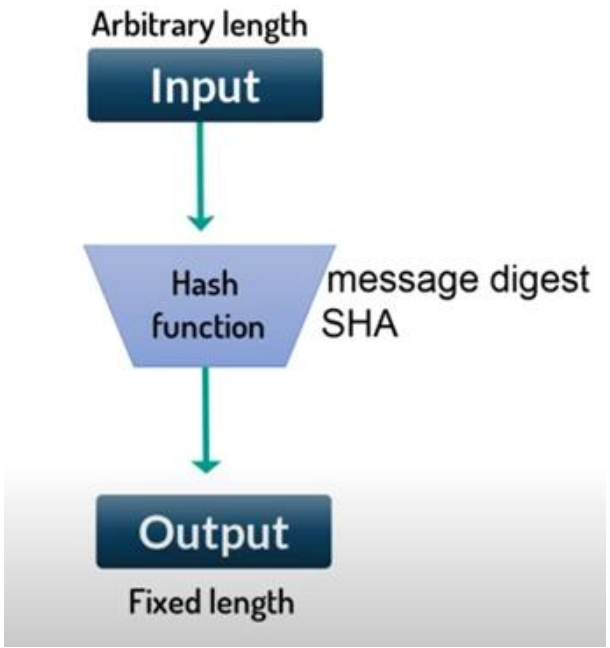
A hash function maps any type of arbitrary data of any length to a fixed-size output. They are efficient and are well-known for one property: they can't be reversed.

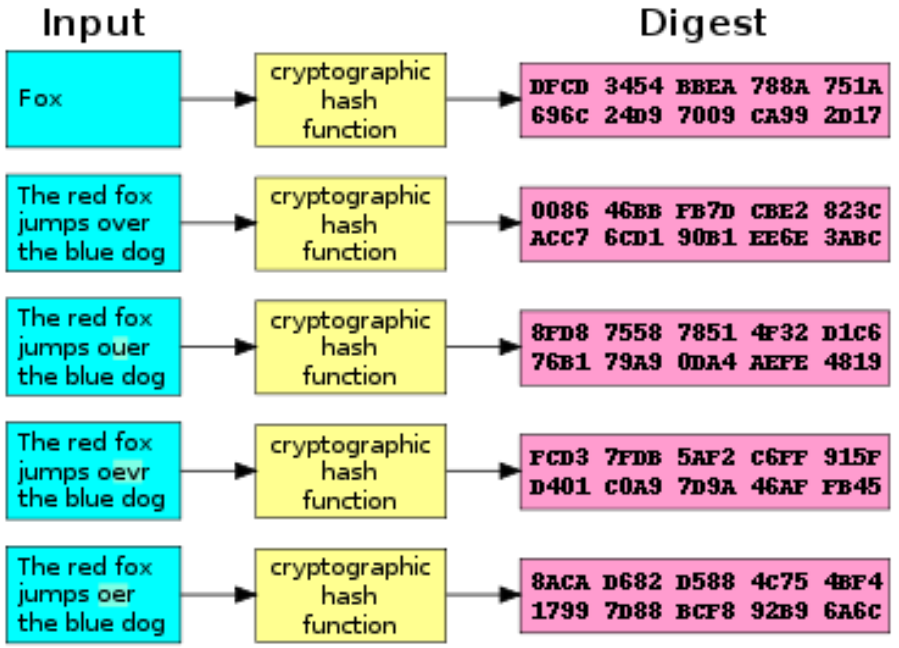
Hash Function for Blockchain



Courtesy : https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain

Cryptographic Hash Functions





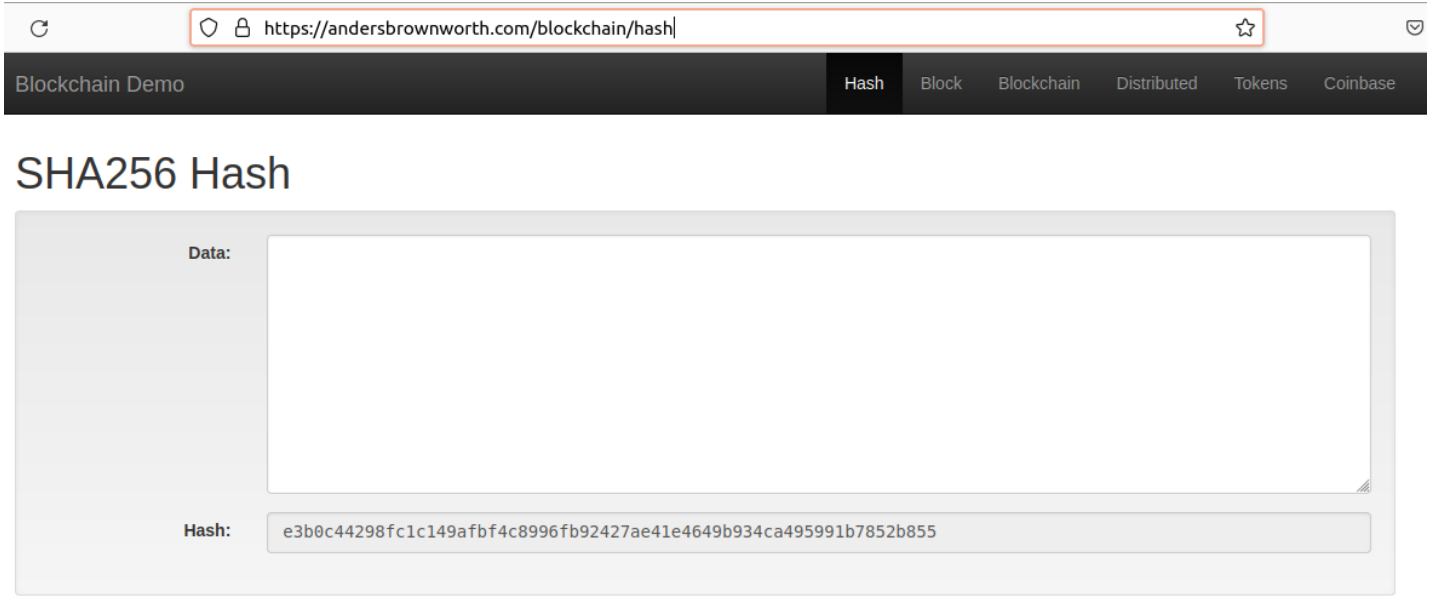
Courtesy : https://en.wikipedia.org/wiki/Cryptographic_hash_function

Cryptographic Hash Functions - Eg.

Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

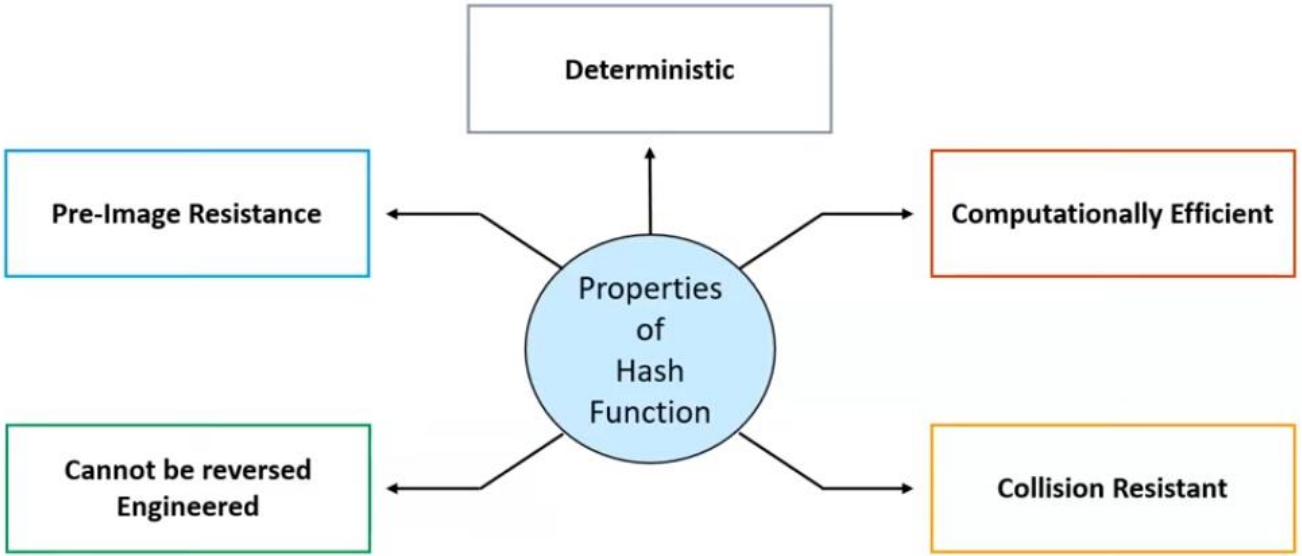
Cryptographic Hash Functions - Demo

Courtesy : https://andersbrownworth.com/blockchain/hash



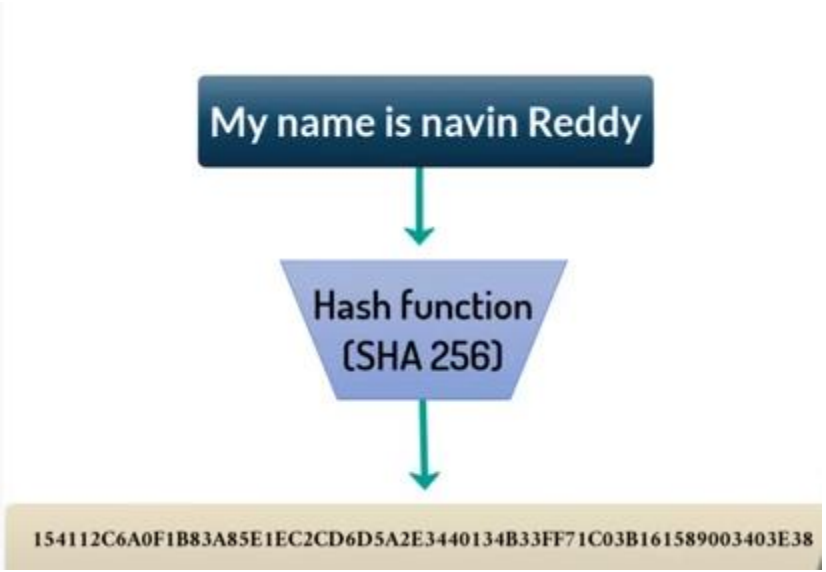
Cryptographic Hash Functions

Let's take an example - If you use the SHA256 hash algorithm and pass 101Blockchains as input, you will get the following output:
fbffd63a60374a31aa9811cbc80b577e23925a5874e86a17f712bab874f33ac9



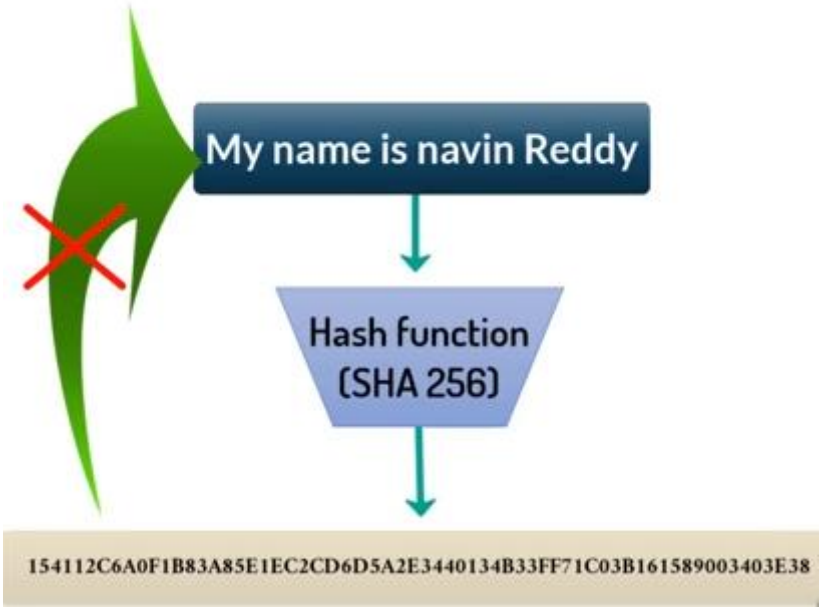
Courtesy : https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain

Cryptographic Hash Functions - Deterministic



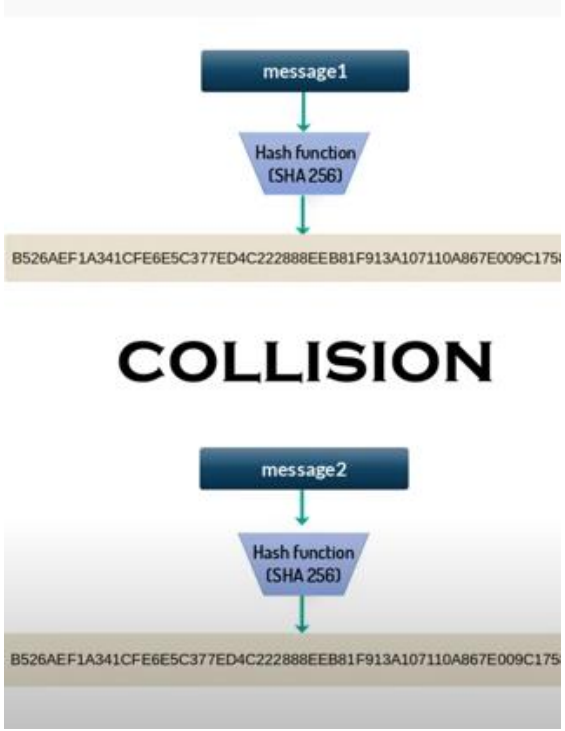
Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

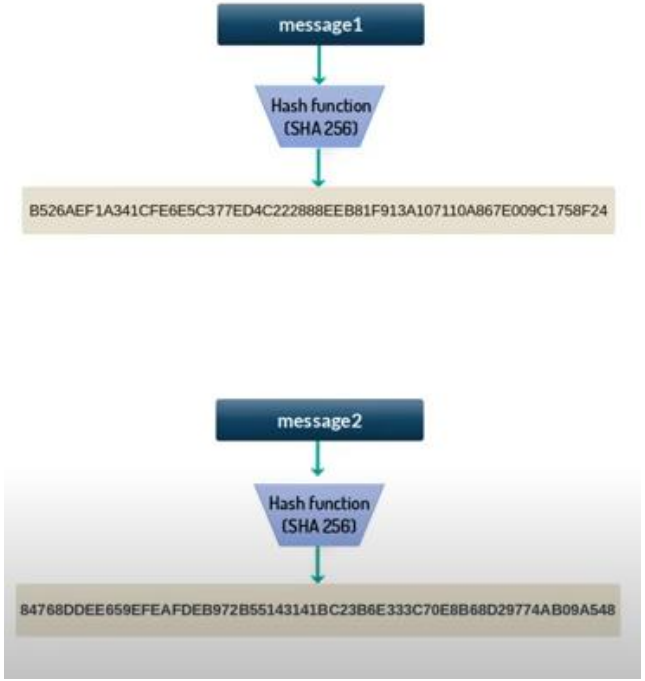
Cryptographic Hash Functions - Cannot be reverse engineered



Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Cryptographic Hash Functions - Collision Resistant





Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

P2P Network in Blockchain

Challenges

1. **Confidentiality**
2. **Integrity**
3. **Non-repudiation**
4. **Authentication**

Solution

- **Digital Signature**

Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

P2P Network in Blockchain

Challenges

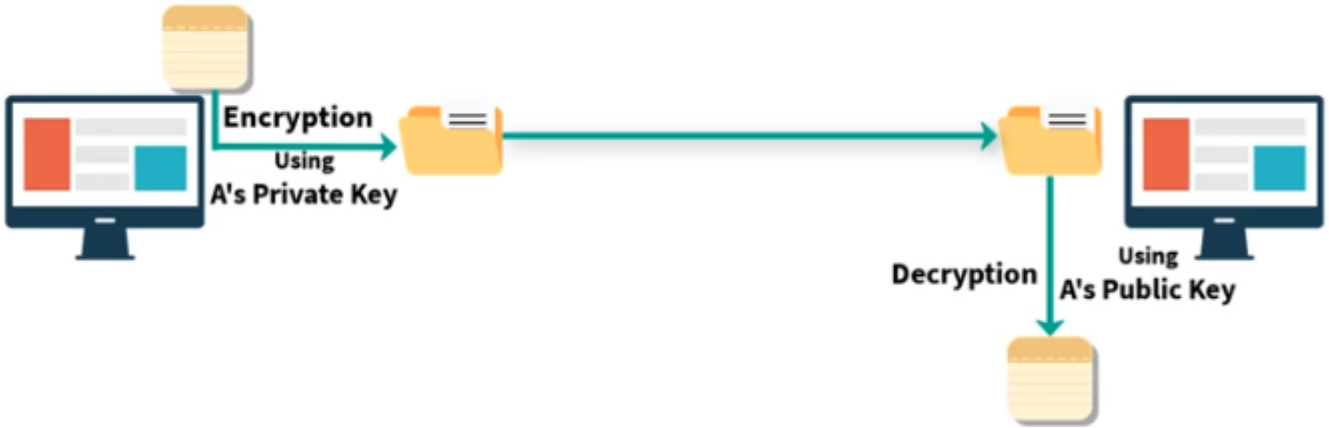
1. **Confidentiality**
2. **Integrity**
3. **Non-repudiation**
4. **Authentication**

Solution

- **Digital Signature**

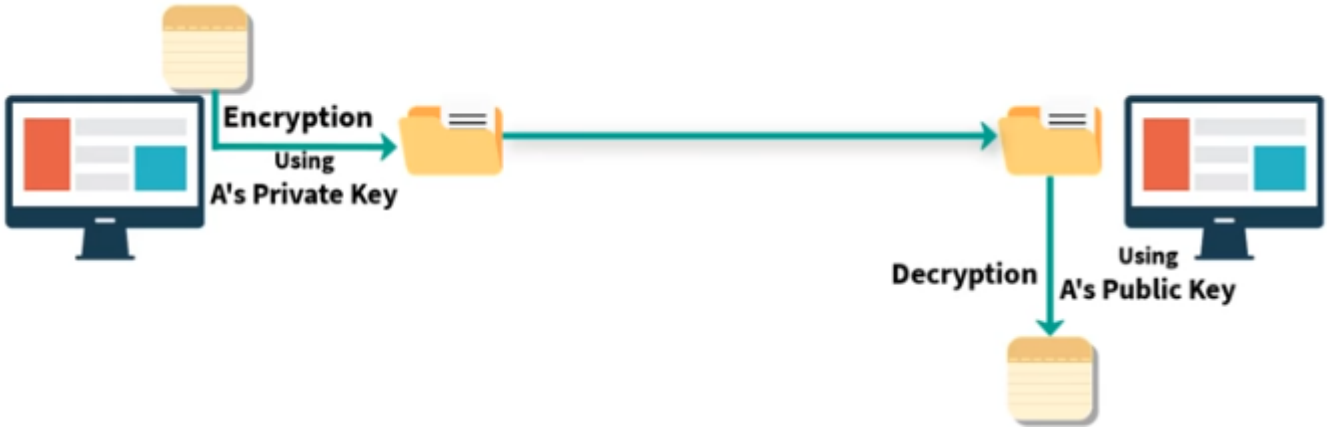
Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Digital Signature - Basic



Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Digital Signature – Ensures only Authentication



Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

Digital Signature - Eg.

Courtesy : https://www.digilocker.gov.in/
https://github.com/jai-singhal/digiLocker

DOMICILE CERTIFICATE SAMPLE

1253200218600827936 5

Office of Executive Magistrate, Andheri

Ref 1: G.R.P.& S.D. No.1586/34-D, Dated 17.5.1951
Ref 2: G.R.GAD No. Mis.31/76-Desk-xxxII, Dated 25.8.1977
Ref 3: [illegible] 1087/9698/ 608 - 32. Dated 2.1.1989

Serial No : **9001604183**
District : **Mumbai Suburban**

Certificate of Age, Nationality and Domicile
(Issued by Authorities in the State of Maharashtra)

On submission of the proofs noted below, it is hereby certified that, **Mr. Jamuna** R/O **JIJA MATA MARG, PUNRVASI SHUKLA AHIR CHAWL, ANDHERI EAST, PUMP HOUSE,** Village **Andheri,** Tehsil **Andheri,** District **Mumbai Suburban** was born on **17/07/1978 (Seventeenth of July in the year One Thousand Nine Hundred and Seventy Eight)** at **HAIDARGANJ,** Tehsil **PALTUPUR,** District **JAUNPUR** in the State of **'UTTAR PRADESH'** within the territory of INDIA and **he** is a CITIZEN OF INDIA and has domiciled in the State of Maharashtra.

PARTICULARS OF PROOFS SUBMITTED

1. **Photo of Applicant** APPLICANT PHOTO
2. **Driving License** ATTACHED APPLICANT DRIVING LICENCE
3. **Pan Card** APPLICANT PAN CARD FOR IDENTITY PROOF
4. **UID** APPLICANT AADHAR CARD FOR ADDRESS PROOF
5. **Electoral Photo ID Card** ATTACHED APPLICANT VOTER ID
6. **Ration Card** APPLICANT RATION CARD FOR ADDRESS PROOF
7. **SSC** SSC CERTIFICATE ISSUED BY MADHYAMIK SHIKSHA PARISHAD DIST JAUNPUR UTTAR PRADESH
8. **HSC** ATTACHED HSC CERTIFICATE ISSUED BY MADHYAMIK SHIKSHA PARISHAD DIST JAUNPUR UTTAR PRADESH
9. **Electricity Bill** ATTACHED ELECTRICITY BILL FROM YEAR 2009 TO 2012
10. **Electricity Bill** ATTACHED ELECTRICITY BILL FROM YEAR 2013 TO 2016
11. **Electricity Bill** ATTACHED ELECTRICITY BILL FROM YEAR 2017 TO 2020
12. **Affidavit** ATTACHED AFFIDAVIT WITH NOTARY AS MENTIONED

Signature valid
Digitally Signed by Balasaheb Sadashiv Mane
Date:27-02-2020 12:18:12 PM

Place : **Andheri**
Date : **27/02/2020**

Executive Magistrate
Andheri

Printed By -**OMTID : VLE Name** :ZAVERCHANDRA , **Date**:27/02/2020 12:12PM

This is a digitally signed document, hence is legally valid as per the Information Technology (IT) Act, 2000.
To verify visit https://www.mahaonline.gov.in/Verify OR SMS "MH<space>CSC<space>VRFY<20 digit Barcode number>" to 166 from a BSNL, MTNL, Tata Mobile and 51969 from others.

Digital Signatures - Demo

Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/signatures

Signatures

Sign | Verify

Message

Myself, Priya Nair from Computer Engineering Department, VESIT

Private Key

14545484946569125683859385438290354156365925667793118176121744876326050849677

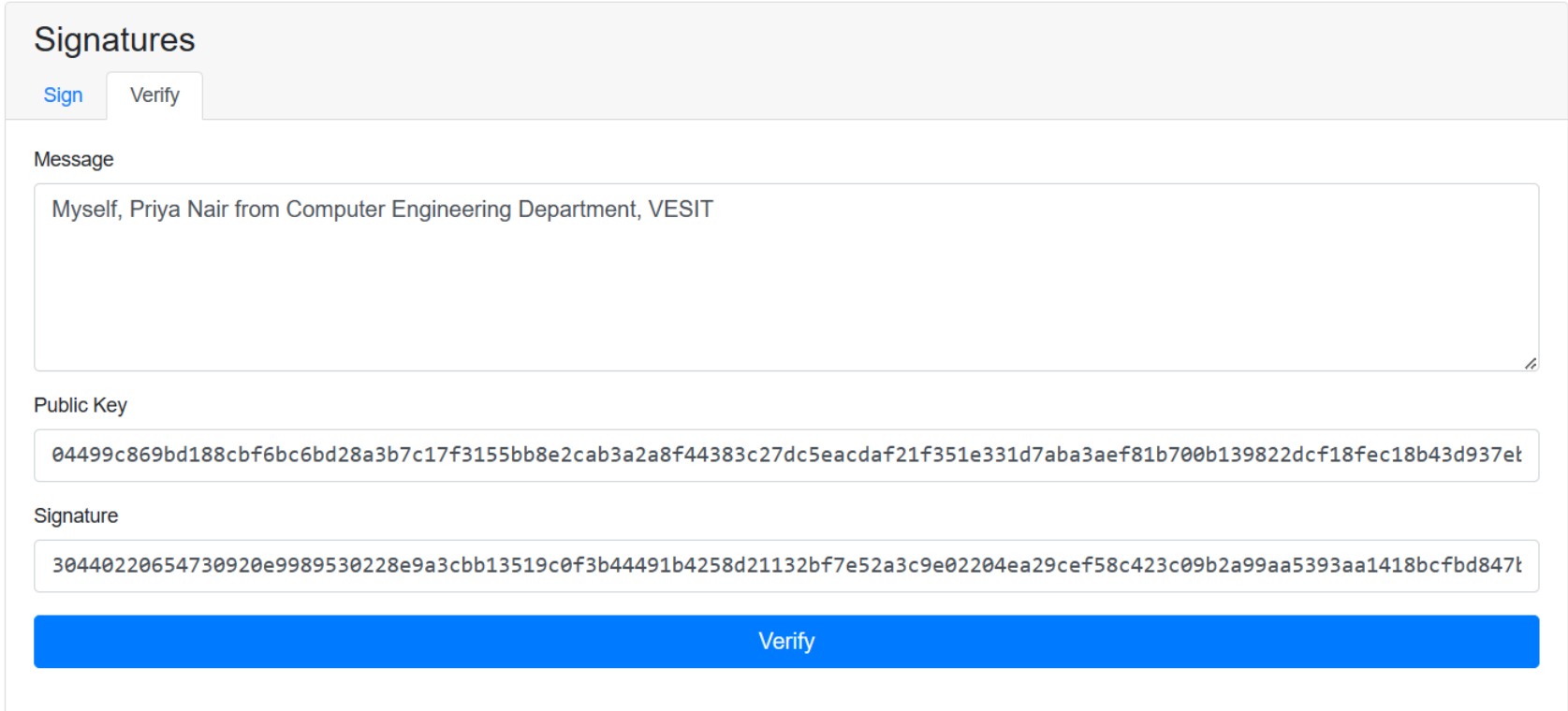
Sign

Message Signature

3044022065473092 0e9989530228e9a3cbb13519c0f3b44491b4258d21132bf7e52a3c9e02204ea29cef58c423c09b2a99aa5393aa1418bcfbd847b

Digital Signatures - Demo

Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/signatures



Digital Signatures - Demo

Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/signatures

Signatures

Sign | Verify

Message

Myself, Priya Nair from Computer Engineering Department, VESIT

Public Key

04499c869bd188cbf6bc6bd28a3b7c17f3155bb8e2cab3a2a8f44383c27dc5eacdaf21f351e331d7aba3aef81b700b139822dcf18fec18b43d937eb

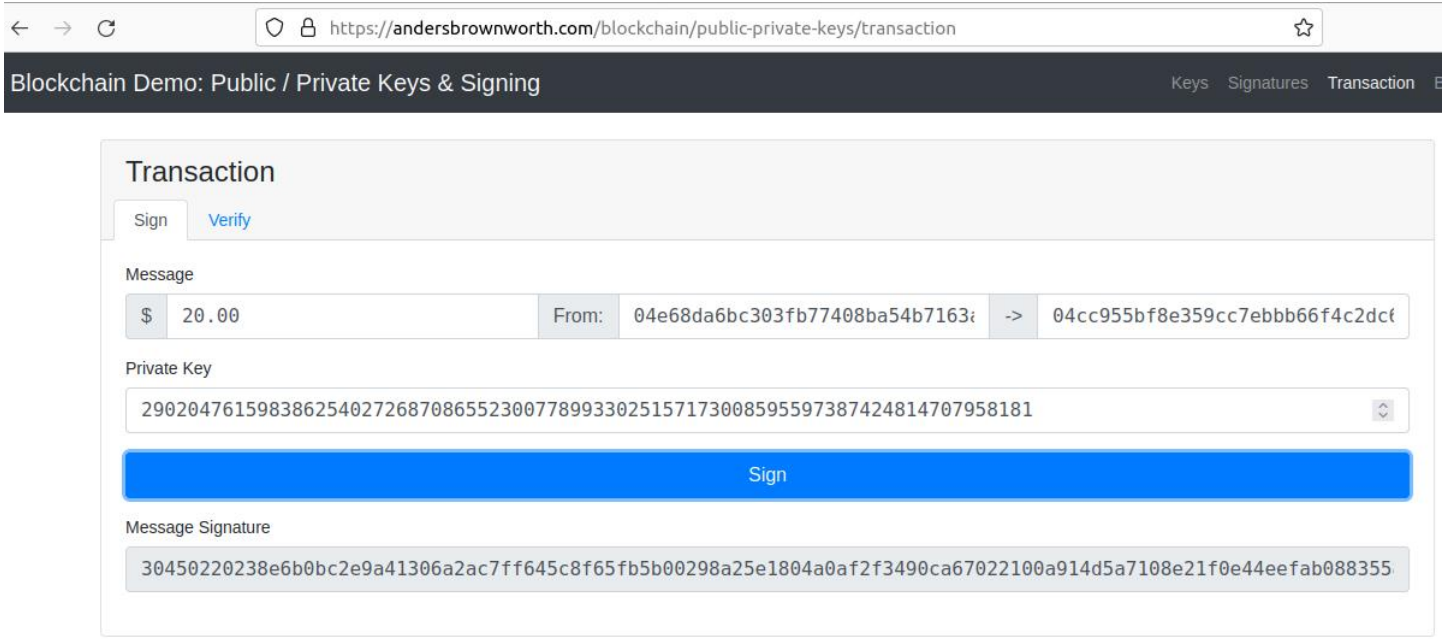
Signature

304402206547309 20e9989530228e9a3cbb13519c0f3b44491b4258d21132bf7e52a3c9e02204ea29cef58c423c09b2a99aa5393aa1418bcfbd847b

Verify

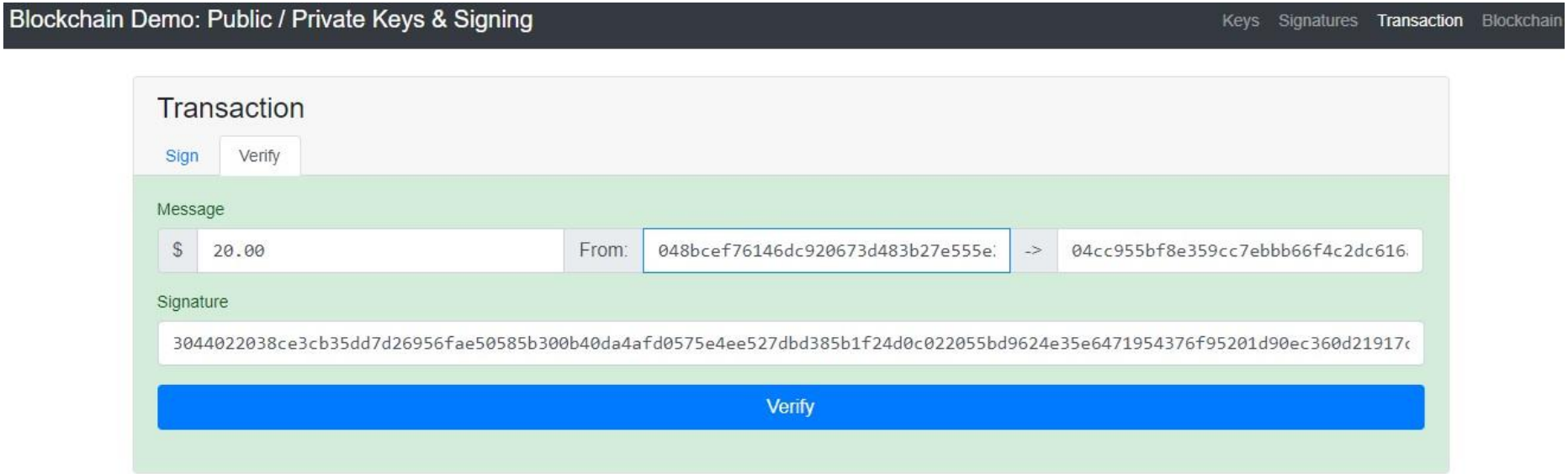
Digitally Signed Transaction - Demo

Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/transaction



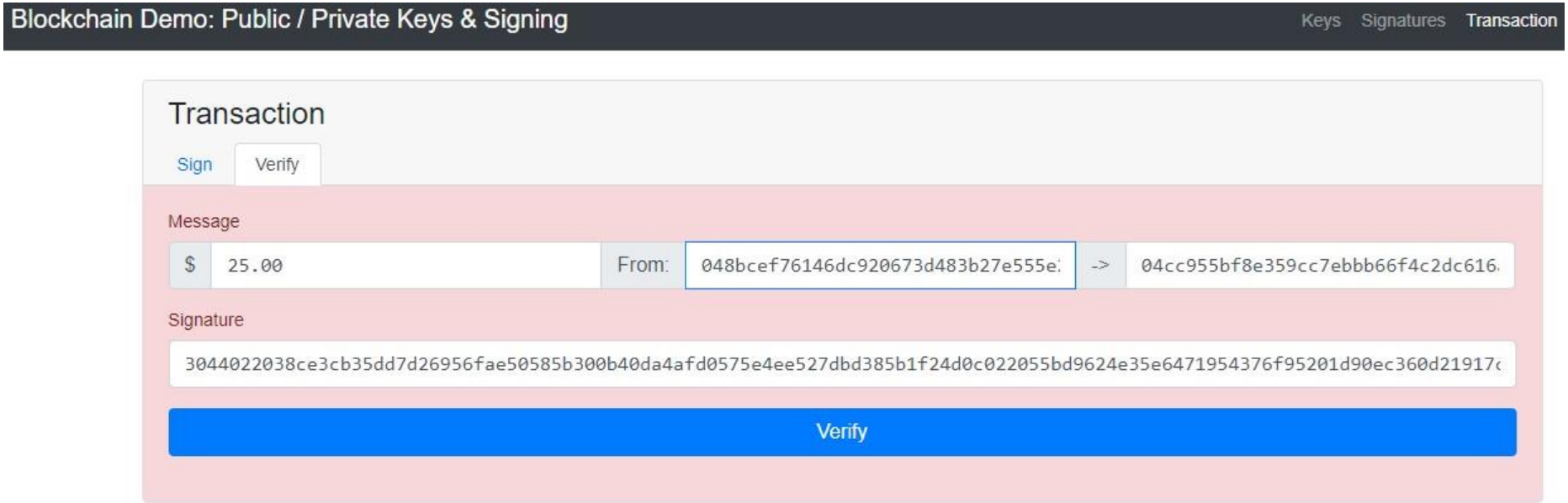
Digitally Signed Transaction - Demo

Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/transaction

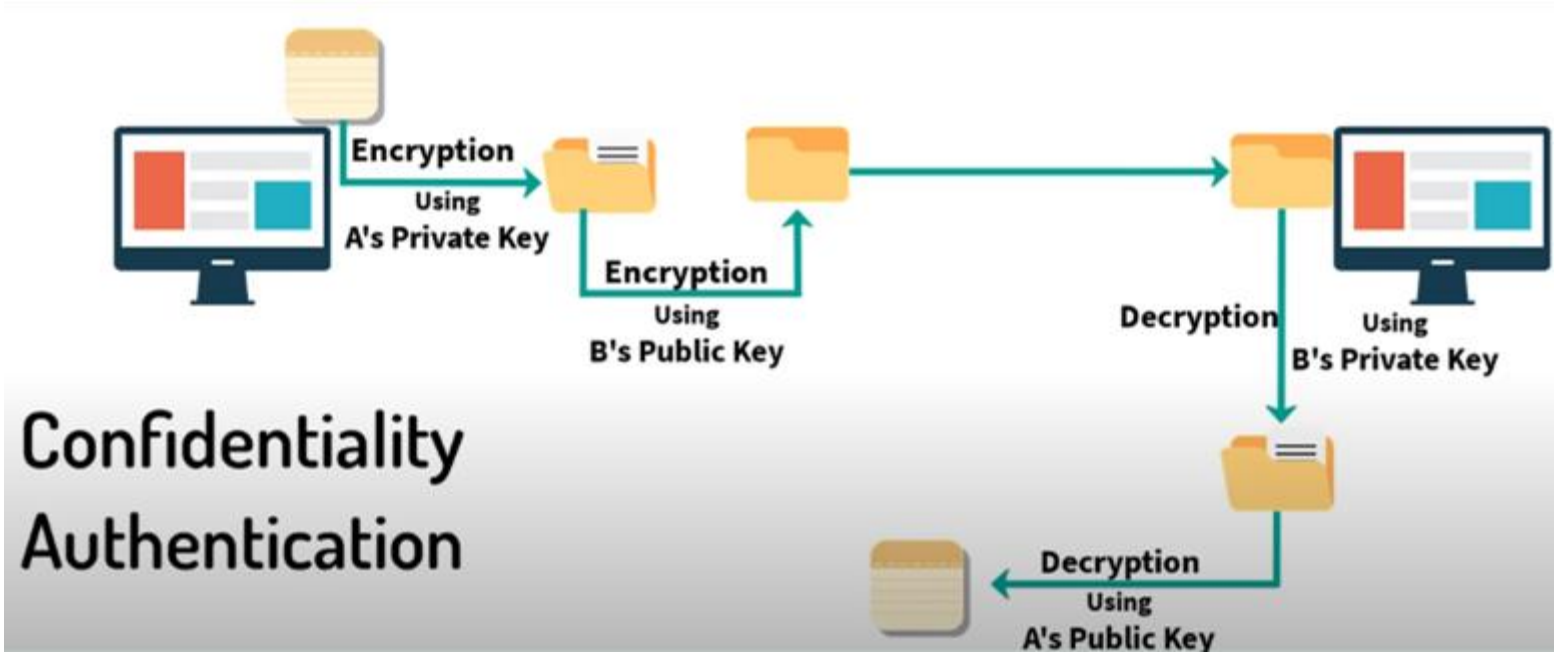


Digitally Signed Transaction - Demo

Courtesy : https://andersbrownworth.com/blockchain/public-private-keys/transaction

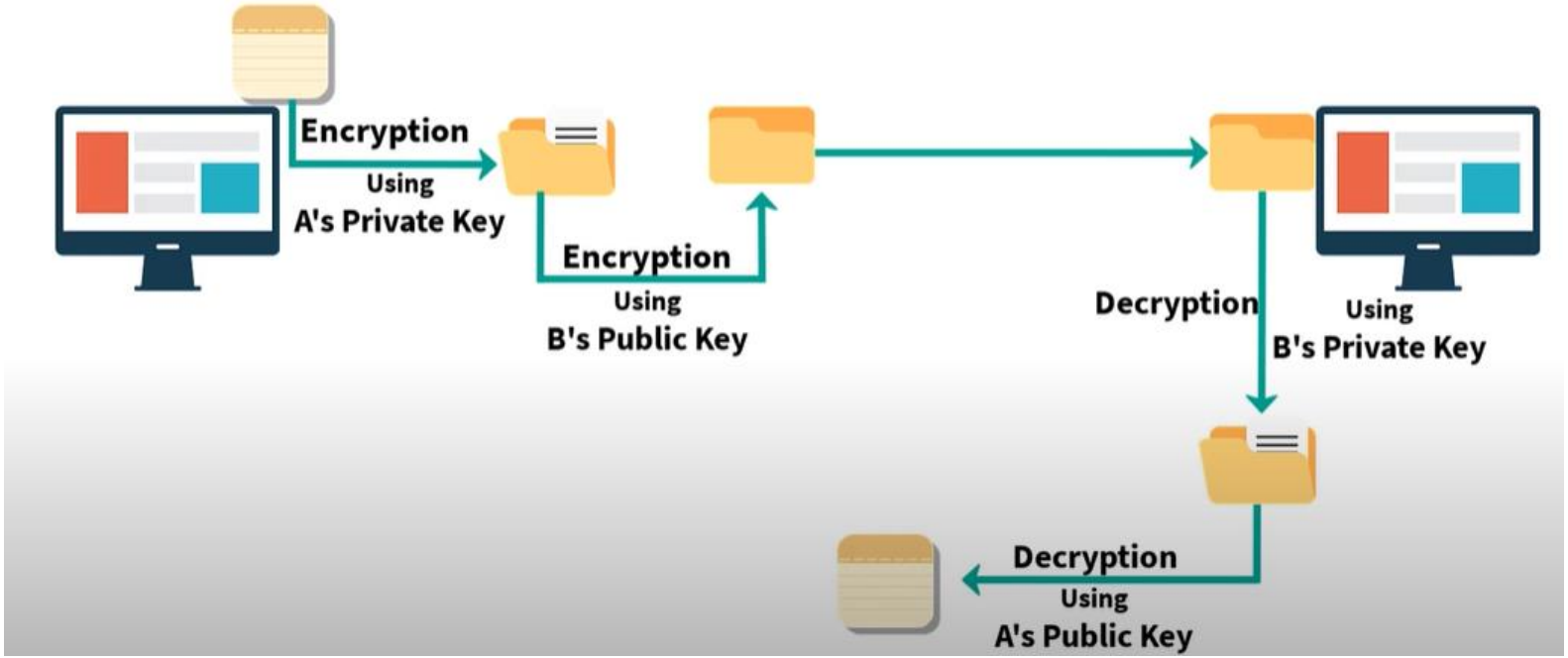


Digital Signature



Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

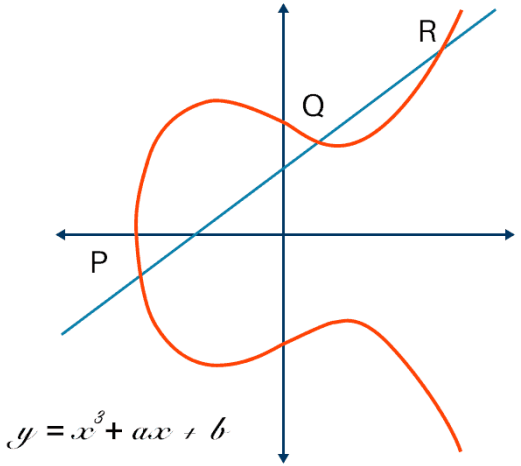
Digital Signature – Ensures both Authentication & Confidentiality



Courtesy : https://www.youtube.com/watch?v=06Un2_F4Y0E&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-&index=7

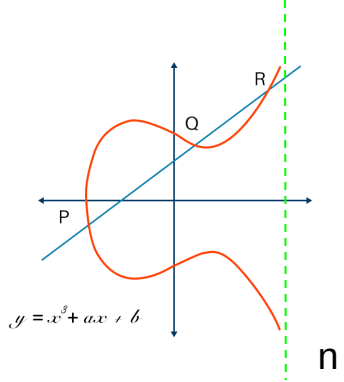
Elliptical Curve Cryptography

- Asymmetric Key Cryptography
- Provides **High Security with smaller key size** (compared to RSA)
- Uses **Elliptical Curves**
  - defined using equations of degree 3
  - Symmetric to x-axis
  - Line drawn will intersect atmost 3 points.

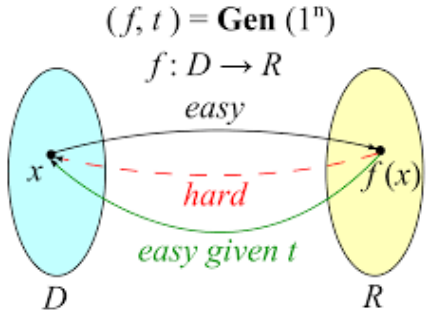


Courtesy : https://www.youtube.com/watch?v=0NGPhAPKYv4

Elliptical Curve Cryptography

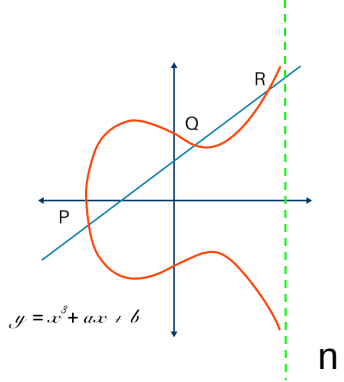


- **What makes ECC hard to crack ?**
  - **Discrete Logarithm Problem**
    - Let E_q (a,b) be the Elliptical Curve, consider the equation, Q = kP ; where Q & P are pts on curve and k < n
      - If k & P is given, its easy to find Q.
      - Otherwise, extremely difficult to find k
  - **Trapdoor Function**



Courtesy : https://en.wikipedia.org/wiki/Trapdoor_function

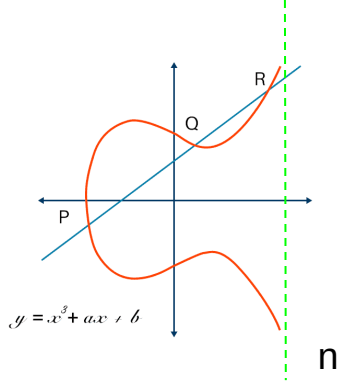
Elliptical Curve Cryptography



- **Global Public Elements**
  - E_q (a,b) :
    - a, b : parameters of elliptical curve
    - q : prime no. or an integer of the form 2^m
  - G : Point on the elliptical curve, > n

Courtesy : https://www.youtube.com/watch?v=0NGPhAPKYv4

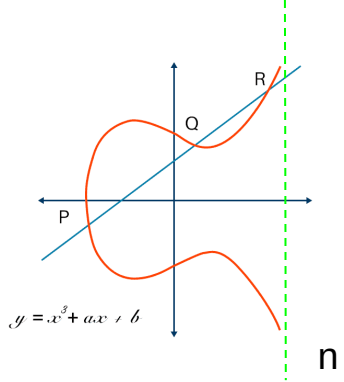
Elliptical Curve Cryptography



- **User A Key Generation**
  - Select Private Key n_A: $n_A < n$
  - Calculate Public Key P_A: $P_A = n_A \times G$
- **User B Key Generation**
  - Select Private Key n_B: $n_B < n$
  - Calculate Public Key P_B : $P_B = n_B \times G$
- **Key Exchange :**
  - **Calculation of secret key by User A :** $k = n_A \times P_B$
  - **Calculation of secret key by User B :** $k = n_B \times P_A$

Courtesy : https://www.youtube.com/watch?v=0NGPhAPKYv4

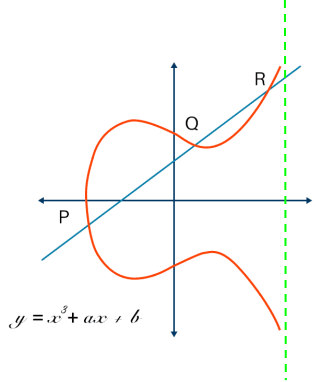
Elliptical Curve Cryptography



- **ECC Encryption**
  - Let **m** be the message.
  - Encode m into a point on the Elliptic curve, P_m
  - For encryption, chose a random +ve integer, **k**
  - The Cipher point, $C_m = \{ kG, P_m + kP_B \}$
  - C_m is forwarded to destination

Courtesy : https://www.youtube.com/watch?v=0NGPhAPKYv4

Elliptical Curve Cryptography



- **ECC Decryption** : $C_m = \{ kG, P_m + kP_B \}$
  - $kG \times n_B$ //(where, n_B : Private key of B)
  - $P_m + kP_B - (kG \times n_B)$ // we know $P_B = n_B \times G$
  - i.e., $P_m + kP_B - kP_B$
  - i.e., P_m // Receiver gets Encrypted point of message

Courtesy : https://www.youtube.com/watch?v=0NGPhAPKYv4

Questions

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	**Prerequisite**	**Introduction to Cryptography:** Hash functions, Public key cryptography, Digital Signature (ECDSA).	**2**	--

- What is Web 3.0 ?
- What is Blockchain? Explain its Significance with an example
- Differentiate between Centralized, Decentralized and Distributed Networks
- Explain Asymmetric Key Cryptography with an example
- Difference between Symmetric Key and Asymmetric Key Cryptography
- Properties of Cryptographic Hash Functions
- Explain Digital Signature with an example.

Online Resources

Theory

- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://komodoplatform.com/en/academy/cryptographic-hash-function/
- https://cse.iitkgp.ac.in/~debdeep/pres/TI/ecc.pdf

Visualization

- https://andersbrownworth.com/blockchain/
- https://andersbrownworth.com/blockchain/hash
- https://andersbrownworth.com/blockchain/public-private-keys/

Useful Videos

- https://nptel.ac.in/courses/106105184
- https://www.youtube.com/watch?v=dCvB-mhkT0w
- https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain
- https://www.youtube.com/watch?v=2uYuWiICCM0&list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-