

Ethical Student Hackers

Tor & Cryptocurrency



The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.



Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at
<https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf>

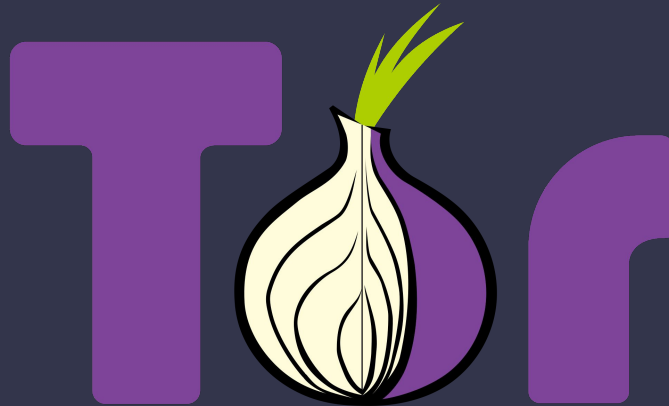


Tor



What is Tor?

- Tor refers to “The Onion Router” and represents a network of volunteer-ran nodes through which you first connect to three different nodes before accessing the ordinary internet (“clearnet”), and to six different nodes before connecting to its special “dark web”, consisting of .onion websites.
- Its name refers to the fact that there are layers of protection for the users, just like a peeled onion has many layers.
- Its goals are to improve user privacy and freedom of expression.



History

- Tor hasn't always been widely available to the masses.
- In fact, it was initially a project of the US Navy, developed in the mid 1990s to protect confidential communications in the country.
- Its alpha version was launched in 2002, and the first public release happened in 2003.
- In 2004, its code was made public under a free licence, making it open-source.



The screenshot shows the GitHub profile for "The Tor Project". The profile includes a header with the organization's name, a link to their GitHub code mirrors, and their website. Below the header are navigation tabs for Overview, Repositories (9), Projects, Packages, and People (11). The main section displays "Popular repositories" with six items:

- gettorbrowser** (Public): 383 stars, 112 forks.
- gettor** (Public archive): GetTor - a Tor Browser distribution system. 96 stars, 37 forks.
- steganatorus** (Public): Advanced development framework for stealthier pluggable transports. 66 stars, 27 forks.
- lepidopter** (Public): lepidopter: raspberry pi image for conducting OONI network measurements. 44 stars, 17 forks.
- tor-messenger-build** (Public): Tor Messenger Build scripts (https://gitweb.torproject.org/tor-messenger-build.git/). 41 stars, 23 forks.
- bwscanner** (Public archive): Bandwidth authority scanner. This project is deprecated in favour of https://gitlab.torproject.org/tpo/network-health/sbws. 33 stars, 30 forks.



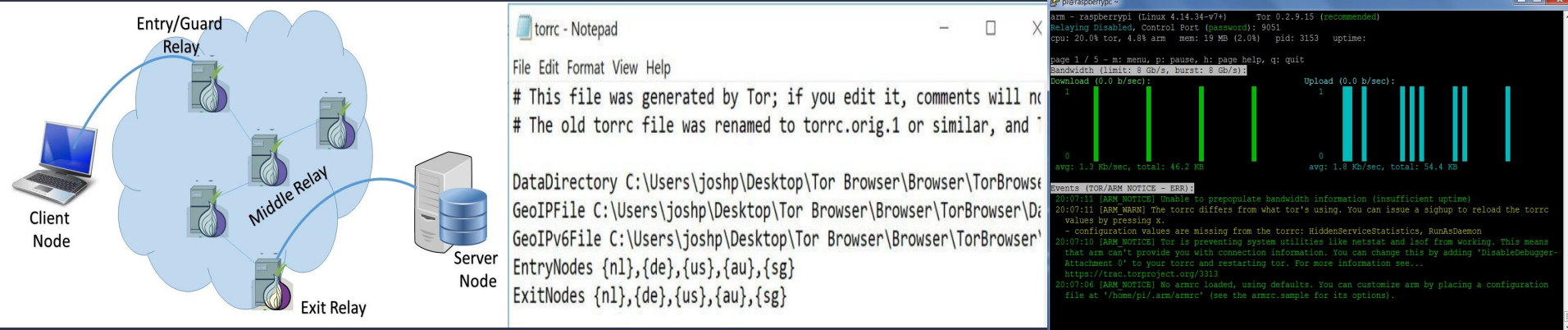
Different types of “webs”

- The concepts of “deep web” and “dark web” are usually misunderstood
- The clearnet is the ordinary internet and contains information that search engines can find
- The deep web is also part of the ordinary internet but its information is not indexed by search engines; its size is much bigger than clearnet’s
- The dark web represents the websites that are accessible through Tor.



Tor nodes

- A typical Tor circuit on clearnet websites consists of three nodes: entry, middle and exit.
- The entry node can see your IP address and knows which middle node to connect to.
- The middle node knows the entry and exit nodes.
- The exit node knows the middle node and the website to connect to, and also does the connection to the website.
- Bridge nodes are hidden nodes used by people in countries where the internet is heavily regulated.
- You can choose your nodes by country in the torrc configuration file or even run your own node, but running an exit node is dangerous because you never know what websites people will access.



The diagram on the left illustrates a typical Tor circuit. A Client Node (laptop) connects to an Entry/Guard Relay (server icon). The Entry/Guard Relay connects to a Middle Relay (server icon). The Middle Relay connects to an Exit Relay (server icon). The Exit Relay connects to a Server Node (server icon). The relays are shown within a cloud-like network.

The screenshot on the right shows the torrc configuration file in Notepad. The file contains the following content:

```
torrc - Notepad
File Edit Format View Help
# This file was generated by Tor; if you edit it, comments will no
# The old torrc file was renamed to torrc.orig.1 or similar, and

DataDirectory C:\Users\joshp\Desktop\Tor Browser\Browser\TorBrowse
GeoIPFile C:\Users\joshp\Desktop\Tor Browser\Browser\TorBrowser\D
GeoIPv6File C:\Users\joshp\Desktop\Tor Browser\Browser\TorBrowser\
EntryNodes {n1},{de},{us},{au},{sg}
ExitNodes {n1},{de},{us},{au},{sg}
```

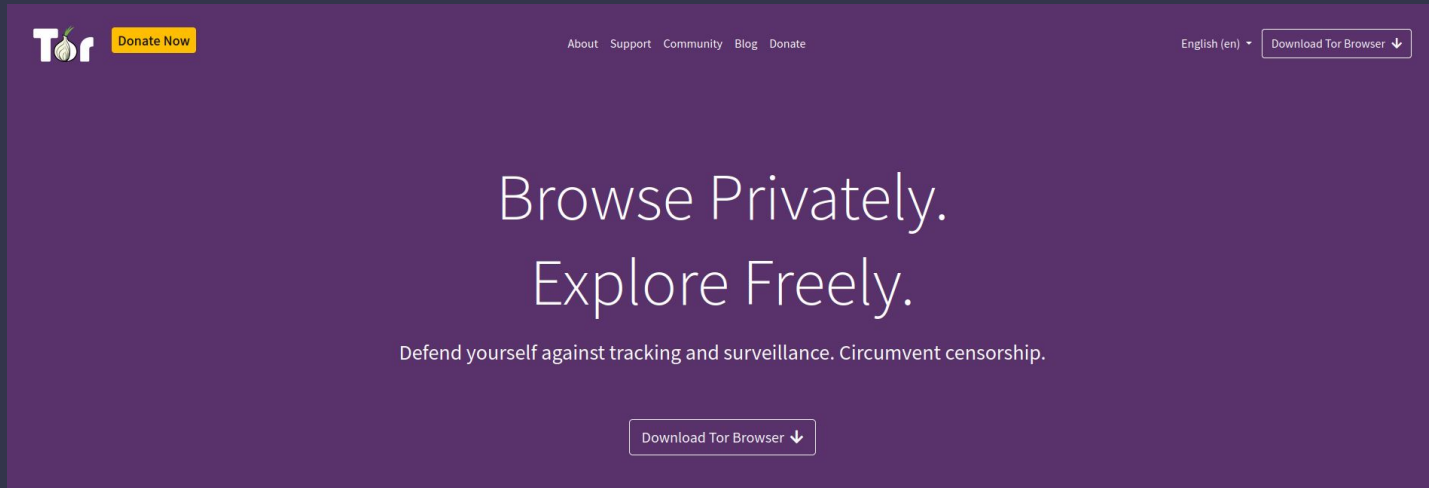
The screenshot also shows a terminal window with the following output:

```
pi@raspberrypi:~$ tor
arm - raspberrypi (Linux 4.14.34-v7+) Tor 0.2.9.15 (recommended)
Relaying Disabled, Control Port (password): 9051
cpu: 20.0% tor, 4.8% arm mem: 19 MB (2.0%) pid: 2153 uptime:
page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 8 Gb/s, burst: 8 Gb/s):
Download (0.0 b/sec):
1
0
avg: 1.3 Kb/sec, total: 46.2 KB
Upload (0.0 b/sec):
1
0
avg: 1.8 Kb/sec, total: 54.4 KB
Events (TOR/ARM NOTICE - ERR):
20:07:11 [ARM NOTICE] Unable to prepopulate bandwidth information (insufficient uptime)
20:07:11 [ARM_WARN] The torrc differs from what tor's using. You can issue a signup to reload the torrc
values by pressing x.
- configuration values are missing from the torrc: HiddenServiceStatistics, RunAsDaemon
20:07:10 [ARM NOTICE] Tor is preventing system utilities like netstat and lsof from working. This means
that arm can't provide you with connection information. You can change this by adding 'DisableDebugger
Attachment 0' to your torrc and restarting tor. For more information see...
https://trace.torproject.org/3113
20:07:06 [ARM NOTICE] No armc loaded, using defaults. You can customize arm by placing a configuration
file at '/home/pi/.arm/armrc' (see the armrc.sample for its options).
```

[Source](#)

Tor Browser

- Tor and the Tor Browser are not actually the same thing.
- The Tor network is the collection of nodes, while the browser is the software that makes use of the nodes to access and display websites for the users.
- The Tor Browser is, in fact, a modified version of the open-source browser Mozilla Firefox, tweaked in order to achieve improved privacy and security.
- It can be found on its official website, <https://www.torproject.org/> .



The image shows a screenshot of the Tor Project website homepage. The background is a dark purple gradient. In the top left corner, there is the Tor logo (a stylized onion) and a yellow button that says "Donate Now". In the top right corner, there is a navigation menu with links for "About", "Support", "Community", "Blog", and "Donate", followed by a language selector set to "English (en)" and a button that says "Download Tor Browser" with a downward arrow. The main content area features the text "Browse Privately. Explore Freely." in a large, white, sans-serif font. Below this, in a smaller white font, is the text "Defend yourself against tracking and surveillance. Circumvent censorship." At the bottom center, there is a button that says "Download Tor Browser" with a downward arrow. In the bottom right corner, there is a circular logo for "SHEFFIELD ETHICAL STUDENT HACKERS" featuring a red padlock icon in the center.

Using the Tor Browser

- Using Tor and its browser is legal (unless you live in a country that banned them, which can be dangerous or raise suspicions), but participating in illegal activities when using them is not.
- The browser can be easily downloaded from the download page, [Tor Project | Download](#).
- You may have noticed it does not cover your entire screen, that is done to make it harder to identify you by your screen dimensions.
- Once installed, connect to Tor and visit a clearnet website.

The image shows two overlapping browser windows. The background window is the Tor Browser's 'Connect to Tor' screen. It features a large Tor logo on the left and the text 'Connect to Tor' in a large font. Below this, it says 'Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.' There is a checkbox labeled 'Always connect automatically' which is checked. At the bottom, there are two buttons: 'Tor Network Settings' and a purple 'Connect' button.

The foreground window is a standard browser window displaying the DuckDuckGo homepage. The address bar shows 'https://duckduckgo.com'. A 'Site information' popup is open, showing the connection is secure and displaying the Tor circuit path: 'This browser' -> 'Finland 84.249.29.37 Guard' -> 'United States 74.208.206.121, 2607:f1c0:1800:5b::1' -> 'Austria 109.70.100.65, 2a03:a600:100:65' -> 'duckduckgo.com'. A green button at the bottom of the popup says 'New Circuit for this Site'. Below the popup, the main content of the page is visible, including the headline 'Tired of being tracked online? We can help.' and a blue button that says 'Add DuckDuckGo to Firefox'.

Using the Tor Browser

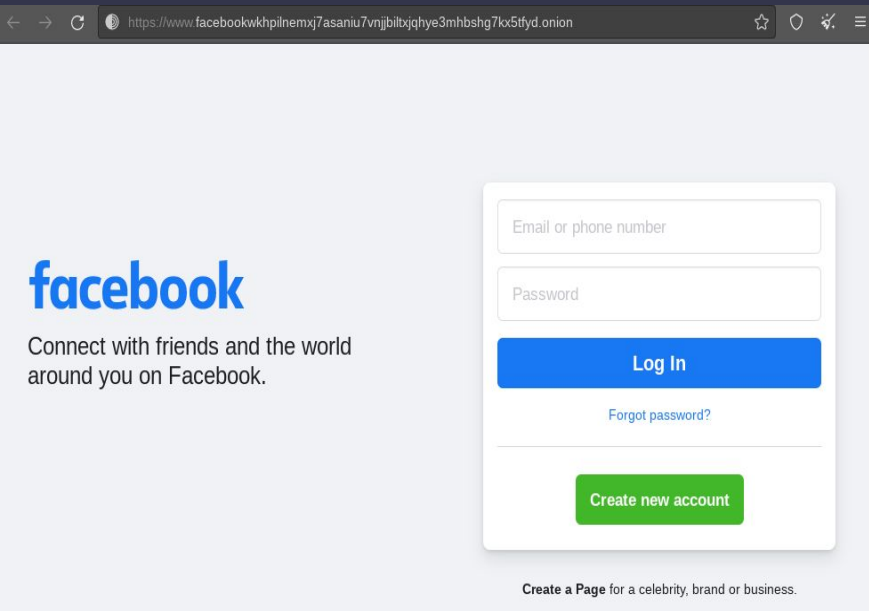
- You can then see your circuit of nodes and request a new one for a specific website.
- You can begin your browsing journey while double-checking the websites you want to visit.

The screenshot shows the Tor Browser interface with a site information overlay for 'zqktlwiuavvqq4t4ybvvgvi7yo4hjl5xgfuvpdf6otjycgwbym2qad.onion/wiki'. The overlay displays connection security, a Tor circuit diagram with nodes in Finland, Germany, and France, and a 'New Circuit for this Site' button. The background shows the 'The Hidden Wiki' page with navigation, search, and tools sections.

The screenshot shows the TORCH search engine interface. The URL is 'xmh57jrknzkvh6y3ls3ubitzfqnrwxhopf5aygthi7d6rplyvk3noyd.onion/cgi-bin/omega/omega'. The page features the TORCH logo, a search bar, and options for 'Matching any words' and 'Matching all words'. It displays 'Searching 1,762,693 documents' and a link to 'Advertise now in Torch. Click here.' Below the search area are several advertisements: 'BUY REAL MONEY', 'INDEX | SEARCH ENGINE', 'TorLinks CLICK HERE', 'Tor HIDDEN WIKI 2022', and 'DeepMarket FREE SHIPPING GET \$10 FOR FREE'. At the bottom, there are icons for Bitcoin, a credit card, and 'TORBUY escrowmarket'.

Using the Tor Browser

- You will find normal websites that simply have an .onion address and some Tor-exclusive websites with various content.



facebook

Connect with friends and the world around you on Facebook.

Email or phone number

Password

Log In

Forgot password?

Create new account

Create a Page for a celebrity, brand or business.



Bitcoin and Tor, a perfect Team

When using Bitcoin together with Tor you are combining the best online currency with the best encryption and privacy technology available.

When you're using normal internet websites to manage your bitcoin funds you can't know who's tracing you.

Only a shared Web Wallet on Tor will provide you with maximum anonymity and privacy.



Is Tor truly secure?

- Even with everything that it offers, the truth is that Tor is not 100% secure and attacks/vulnerabilities have been found over the years.
- At the same time, apart from seeing vulnerabilities, there is no clear way for people to know how compromised the network or the browser currently is or what governments are capable of.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-38385	617			2021-08-30	2021-09-02	5.0	None	Remote	Low	Not required	None	None	Partial
Tor before 0.3.5.16, 0.4.5.10, and 0.4.6.7 mishandles the relationship between batch-signature verification and single-signature verification, leading to a remote assertion failure, aka TROVE-2021-007.														
2	CVE-2021-34550	119		Overflow	2021-06-29	2021-09-20	5.0	None	Remote	Low	Not required	None	None	Partial
An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-006. The v3 onion service descriptor parsing allows out-of-bounds memory access, and a client crash, via a crafted onion service descriptor														
3	CVE-2021-34549	755			2021-06-29	2021-09-20	5.0	None	Remote	Low	Not required	None	None	Partial
An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-005. Hashing is mishandled for certain retrieval of circuit data. Consequently, an attacker can trigger the use of an attacker-chosen circuit ID to cause algorithm inefficiency.														
4	CVE-2021-34548	863		Bypass	2021-06-29	2021-09-14	5.0	None	Remote	Low	Not required	None	None	Partial
An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-003. An attacker can forge RELAY_END or RELAY_RESOLVED to bypass the intended access control for ending a stream.														
5	CVE-2021-28090				2021-03-19	2021-07-10	5.0	None	Remote	Low	Not required	None	None	Partial
Tor before 0.4.5.7 allows a remote attacker to cause Tor directory authorities to exit with an assertion failure, aka TROVE-2021-002.														
6	CVE-2021-28089	400			2021-03-19	2021-07-10	5.0	None	Remote	Low	Not required	None	None	Partial
Tor before 0.4.5.7 allows a remote participant in the Tor directory protocol to exhaust CPU resources on a target, aka TROVE-2021-001.														
7	CVE-2020-15572	119		Overflow	2020-07-15	2021-07-21	4.3	None	Remote	Medium	Not required	None	None	Partial
Tor before 0.4.3.6 has an out-of-bounds memory access that allows a remote denial-of-service (crash) attack against Tor instances built to use Mozilla Network Security Services (NSS), aka TROVE-2020-001.														
8	CVE-2020-10593	401		DoS	2020-03-23	2020-03-25	5.0	None	Remote	Low	Not required	None	None	Partial
Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (memory leak), aka TROVE-2020-004. This occurs in circpad_setup_machine_on_circ because a circuit-padding machine can be negotiated twice on the same circuit.														
9	CVE-2020-10592			DoS	2020-03-23	2022-01-01	7.8	None	Remote	Low	Not required	None	None	Complete
Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (CPU consumption), aka TROVE-2020-002.														
10	CVE-2020-8516				2020-02-02	2022-04-18	5.0	None	Remote	Low	Not required	Partial	None	None
** DISPUTED ** The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information. NOTE: The network team of Tor claims this is an intended behavior and not a vulnerability.														
11	CVE-2019-8955	770		DoS	2019-02-21	2020-08-24	5.0	None	Remote	Low	Not required	None	None	Partial
In Tor before 0.3.3.12, 0.3.4.x before 0.3.4.11, 0.3.5.x before 0.3.5.8, and 0.4.x before 0.4.0.2-alpha, remote denial of service against Tor clients and relays can occur via memory exhaustion in the KIST cell scheduler.														
12	CVE-2018-0491	416		DoS	2018-03-05	2019-03-26	5.0	None	Remote	Low	Not required	None	None	Partial
A use-after-free issue was discovered in Tor 0.3.2.x before 0.3.2.10. It allows remote attackers to cause a denial of service (relay crash) because the KIST implementation allows a channel to be added more than once in the pending list.														
13	CVE-2018-0490	476		DoS	2018-03-05	2019-04-30	5.0	None	Remote	Low	Not required	None	None	Partial
An issue was discovered in Tor before 0.2.9.15, 0.3.1.x before 0.3.1.10, and 0.3.2.x before 0.3.2.10. The directory-authority protocol-list subprotocol implementation allows remote attackers to cause a denial of service (NULL pointer dereference and directory-authority crash) via a malformed relay descriptor that is mishandled during voting.														



Tor & Cryptocurrencies

- Tor and cryptocurrencies can be related to each other because you can make payments go through the Tor network for added layers of security and privacy.

TOR (TOR)

Anonymous cryptocurrency based on Tor browser. Safe, Open source, Community run and maintained.



Anonymous



Decentralized



Open Source



Autonomy



Cryptocurrency



Cryptocurrency



A digital currency using cryptography to secure transactions



Bitcoin - Background

Proposed by Satoshi Nakamoto in 2008

(Fake name, 1 person vs group of people, nationality...all unknown)

- Digital coins being transferred to users through electronic signatures
- Transactions added to blockchain for verification
- Removes requirement for financial authority (bank etc.)

Read Bitcoin whitepaper

https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf



Bitcoin - Beginner Terms

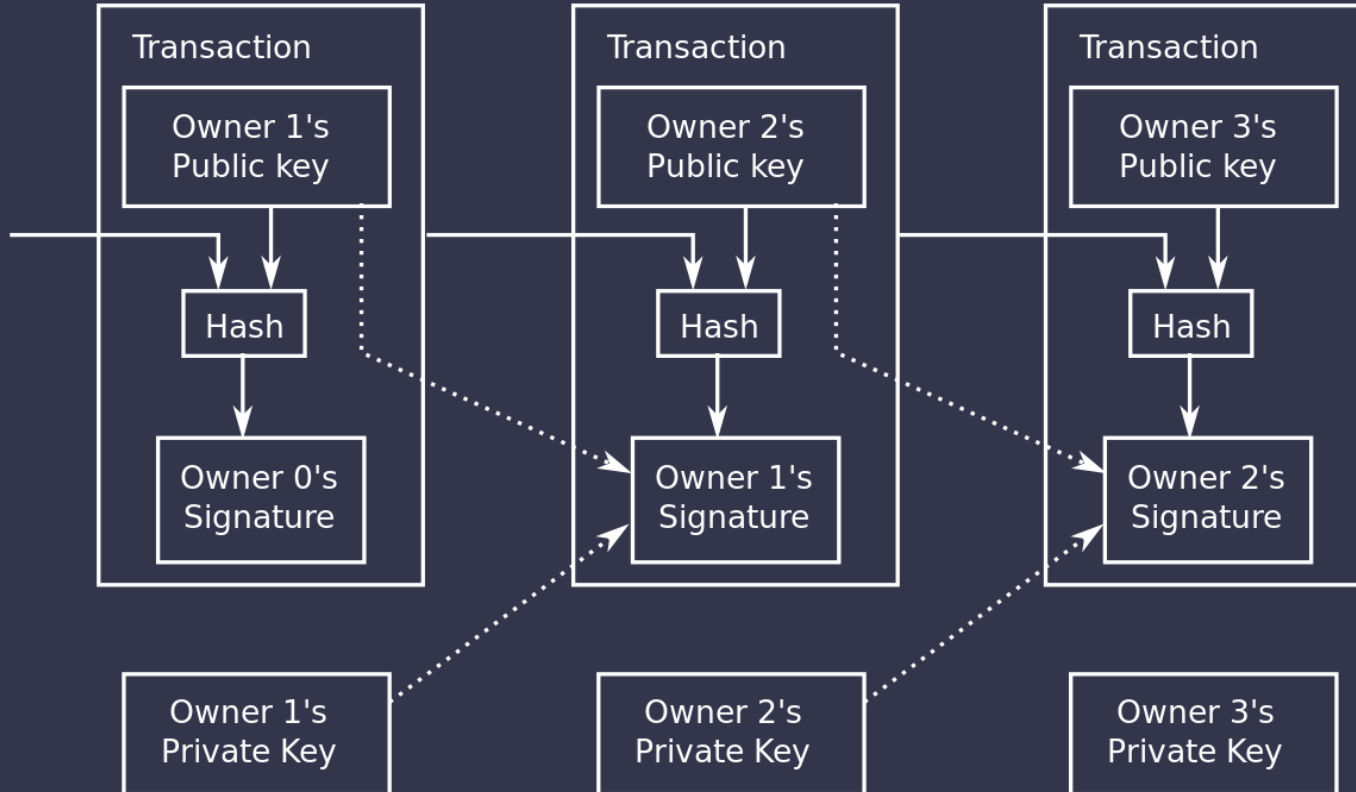
- Cryptographic public key - Key assigned to recipient. Publicly available to everyone want to send the recipient an encrypted message
- Cryptographic private key - Key assigned to recipient. Private to recipient only and used for decrypted a received message
- Cryptographic hash - Created by a hash function. A hash function maps an input to a distinct output of fixed length. Irreversible

- Address - Hash of a public key. Attributed to a cryptocurrency user in control of the private key. Bitcoins registered here
- Wallet - Store of private and public key pairs
- Block - Group of new accepted transactions
- Blockchain - Distributed and public ledger of all Bitcoin transactions

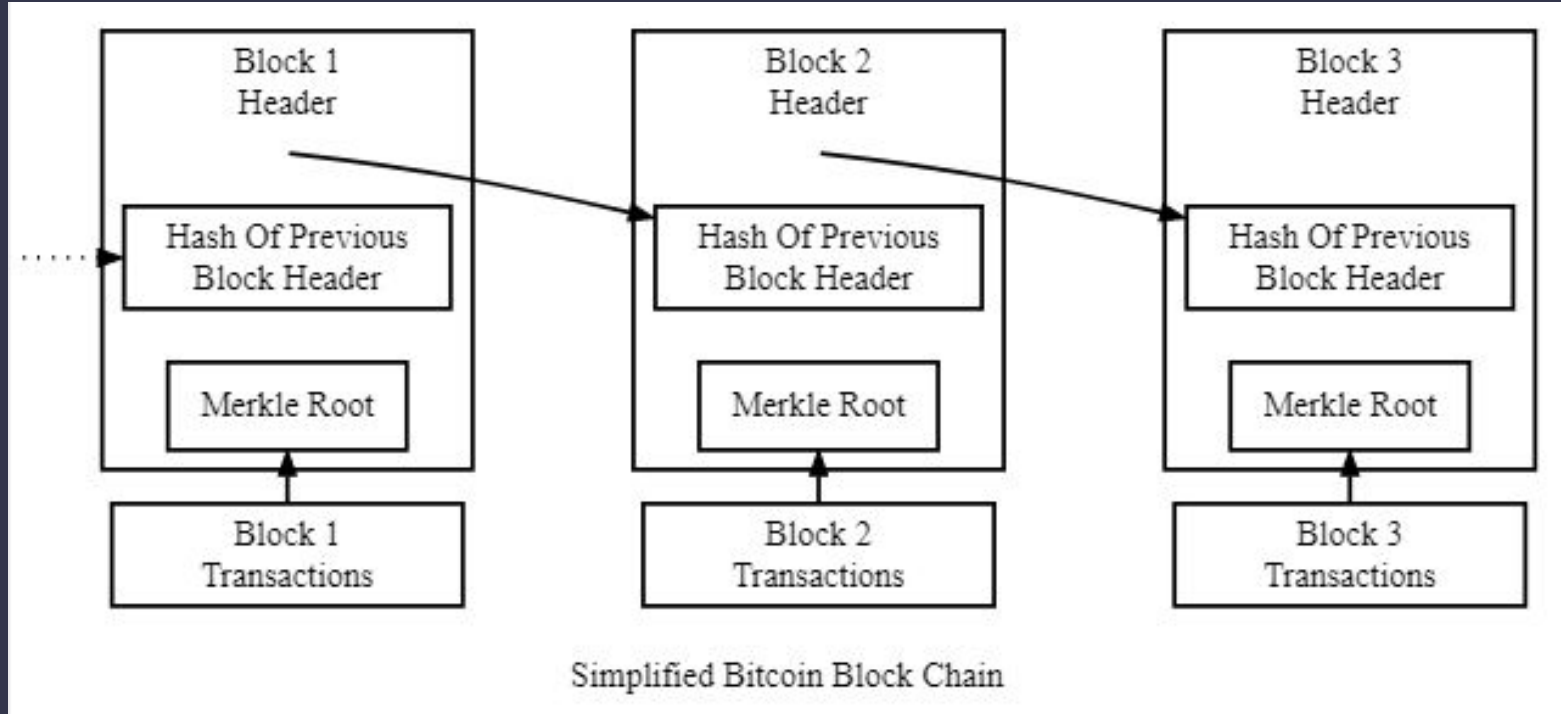


Bitcoin - Transaction

https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf



Blockchain



Mining Bitcoin

Create a new block on the blockchain -> Create new Bitcoins

Done through computationally complex operation

- Find a value when hashed contains a minimum number of leading 0s and is also below a set target
- Nonce = Number of minimum required leading 0s

Block difficulty is adjusted every 2,016 blocks

Block reward is halved every 210,000 blocks

Block owners will receive Bitcoin transaction fees for any transactions on the block



Using Bitcoin

1. RESEARCH A LOT

2. Choose a wallet - Hardware vs software, company, legal restrictions in your country...
3. Get some Bitcoin - In return for goods/services, buy from an exchange
4. Spend

Recommended platforms to get started:

- Exchanges - Coinbase, eToro, crypto.com
- Wallets - Many exchanges also offer wallet services, Exodus
- Viewing the blockchain - blockchain.com/explorer



Challenges

1. When was the ETH block 14648855 mined?
2. What was the reward for mining this block?
3. What was the total of the transaction fees for this block?
4. What is the current value of this Bitcoin address
bc1q87shjz3tr9u3dty5dcu334zm78c8c4c
pufgask?
5. Which address sent the 0.00867699 BTC to this Bitcoin address?



Challenges

1. When was the ETH block 14648855 mined?

April 24, 2022 at 6:48 PM GMT+1

2. What was the reward for mining this block?

Approx. \$6,703.35 USD

3. What was the total of the transaction fees for this block?

Approx. \$898.87 USD

4. What is the current value of this Bitcoin address

bc1q87shjz3tr9u3dty5dcu334zm78c8c4c
pufgask?

Approx. \$1,480.16 USD

5. Which address sent the 0.00867699 BTC to this Bitcoin address?

bc1qt7jt8gql3tcljh2trdusjgdt4l66re9x8edt
2x



Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Red Teamer's Viewpoint - 2nd of May

Blue Teamer's Viewpoint - 9th of May

Any Questions?



www.shefesh.com
Thanks for coming!

