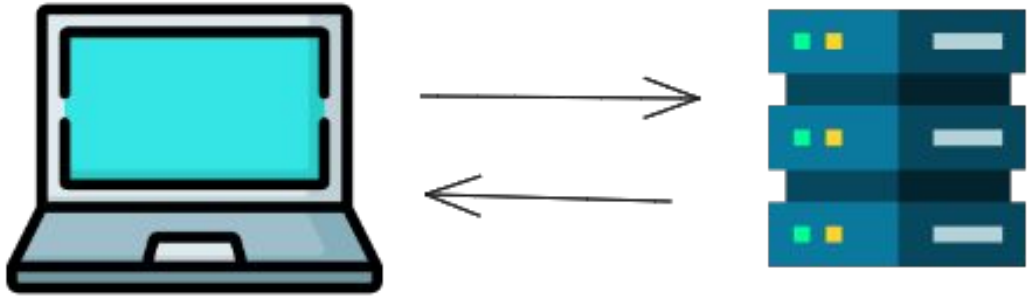
Web Development
Session-4

Web 1 - Static Web

- Read only

Web 2: Social Web

- Read-Write


Client
Server

Traditional carmakers speed towards an electric future — BIG READ, PAGE 9

Stripped of their specialness, they are just like us — PILITA CLARK, PAGE 14

Why a starring role was followed by infamy — ANDREW HILL, PAGE 12

Cathy Newman On Jordan Peterson, trolls & Max Mosley

G2

The Guardian

www.theguardian.com

£2.00

THE SOCIAL NITWIT

Pressure grows on Facebook and data firm over mass breach of personal files

Carole Cadwalladr
Emma Graham-Harrison

acebook and the analytics firm hat worked with Donald Trump's lection team were under mounting ressure last night with calls for new nvestigations and hearings to explain vast data breach that affected tens of illions of people.

In Britain, the head of the parlia- entary committee investigating fake ews accused Cambridge Analytica and Facebook of misleading MPs after revelations in the Observer that more than 50m Facebook profiles were harvested and used to build a system that may have influenced voters in the 2016 US Presidential campaign.

Damian Collins MP said he would call the heads of both companies – Alexander Nix and Mark Zuckerberg – to give further testimony.

His intervention came after a whistleblower spoke to the Observer and described how the profiles, mostly of US voters, were harvested for Cambridge Analytica, in one of Facebook's biggest ever data breaches.

The disclosures caused outrage on both sides of the Atlantic – in the US, a state attorney general has called for investigations and greater accountability and regulation.

The pressure comes amid reports Cambridge Analytica is trying to stop the broadcast of an undercover Channel 4 News expose in which Nix, the company CEO, is said to talk unguardedly about the company's practices.

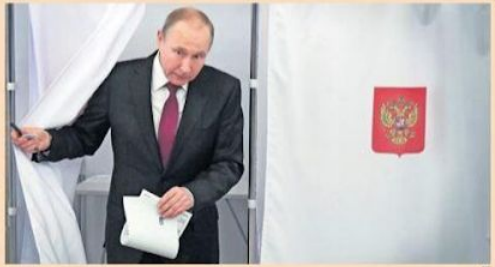
According to the Financial Times, reporters posed as prospective clients and secretly filmed a series of meetings, including one with the chief executive. The report is due to air this week.

Labour said news of the vast data breach should be a spur to further action. The party will now call for a new law to control online advertisements and improve transparency about what advertisements are being put out and who is paying for them, to mirror the Honest Ads Act that has been proposed in the US Congress.

"[It would mean] voters finally learn who is targeting them with what 'news' – and who's writing the cheques," said Liam Byrne, shadow digital minister, writing in today's Guardian. He plans to put forward an amendment to

The Cambridge Analytica files

Putin set for victory amid rigging claims



Vladimir Putin emerges from a polling booth in Moscow yesterday as Russia voted in presidential elections. According to an exit poll published by the Public Opinion Research Centre, Mr Putin won – as expected – with 71.9 per cent of the vote. The Central Election Commission said turnout was almost 60 per cent by 6pm.

However, there were thousands of complaints of irregular Kremlin the voting process, such as ballot stuffing. Kremlin aides had set a target of 70 per cent of the vote for Mr Putin on 70 per cent turnout, spurring provincial governors to whip up support. In Moscow, food stalls at polling stations offered free tea and officials gave out badges and chocolate.

Reports & Analysis page 6

Briefing

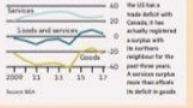
- **Melrose in £1bn pension pledge to GKN** The turnaround specialist has stepped up its battle to win support for its hostile £18bn cash-and-shares bid for the engineering company, with a pledge to pump £1bn into its pension fund.– PAGE 31
- **Davis to hold Brussels transition talks** Britain's chief Brexit negotiator will hold urgent talks in Brussels today to try to secure the exit transition deal demanded by business, amid fears of a last-minute row over the Irish border.– PAGE 2
- **Weir seeks to axe LTIP pay schemes** The engineering company will revive the push to reform executive pay with a plan this week to ditch the reward scheme that has been linked to excessive boardroom remuneration.– PAGE 31
- **Johnson steps up Russia poison claims** The foreign secretary has said the UK will step up sanctions on Vladimir Putin's associates, as he claimed Russia had stockpiled nerve agents "in the last 10 years".– PAGE 2

- **More work on compliance at Barclays** The bank's board has declared there is still more work to do to improve controls and compliance, as it called on senior managers to try harder to hold individuals to account when they fall short.– PAGE 29
- **Beijing names new central bank chief** China's parliament is to name US-educated economist Yi Gang as central bank chief, ensuring policy continuity as Beijing moves aggressively to control risk in its financial system.– PAGE 2
- **Fed policymakers to weigh rate moves** A buoyant outlook is expected from the Federal Reserve this week as policymakers discuss lifting interest rates further than had been previously expected.– PAGE 3, ROBIN WIGGLESWORTH, PAGE 29

Datawatch

Northern comfort

US trade balance with Canada ($bn)



Source: BEA

Despite President Donald Trump's assertion that the US has a trade deficit with Canada, it has actually registered a surplus with its northern neighbour for the past three years. A services surplus more than offsets its deficit in goods

Facebook feels the pressure over claims its data helped Trump win

affected

Alphabet to shut Google+ after user data expose

Google will shut down the consumer version of its social network Google+ after announcing data from up to 500,000 users may have been exposed to external developers by a bug that was present for more than two years in its systems.

The company said in a blog on Monday it had discovered and patched the leak in March of this year and had no evidence of misuse of user data or that any developer Interfaces (API) partly due to fears of regulatory scrutiny, citing unnamed sources and internal documents.

Google said it had reviewed the issue, looking at the type of data involved, whether it could accurately identify the users to inform, whether there was any evidence of misuse, and whether there were any actions a developer or user could take. "None of these thresholds were met in this instance," it said. "We found no evidence that

Google CEO Sundar Pichai was briefed on the plan not to notify users about the breach after an internal committee had reached that decision

memo, prepared by Google's legal and policy staff and shared with senior executives, warned that disclosing the incident would likely trigger "immediate regulatory interest" and invite comparisons to Facebook's leak of user information to data firm Cambridge Analytica.

Allegations of the improper use of data for 87 million Facebook users by Cambridge Analytica, which was hired by President Trump's

Web3: The new internet?

The term "Web3" was coined in 2014 by Ethereum co-founder Gavin Wood

- Read Write Own
- ***Blockchain*** technology - provides decentralization

DApps: What Web 3.0 Looks Like

As we move into the future, we find increasing need for a zero-trust interaction system. Even pre-Snowden, we had realised that entrusting our information to arbitrary entities on the internet was fraught with danger. However, post-Snowden the argument plainly falls in the hand of those who believe that large organisations and governments routinely attempt to stretch and overstep their authority. Thus we realise that entrusting our information to organisations in general is a fundamentally broken model. The chance of an organisation not meddling with our data is merely the effort required minus their expected gains. Given they tend to have an income model that requires they know as much about people as possible the realist will realise that the potential for convert misuse is difficult to overestimate.

The protocols and technologies on the Web, and even at large the Internet, served as a great technology preview. The workhorses of SMTP, FTP, HTTP(S), PHP, HTML, Javascript each helped contribute to the sort of rich cloud-based applications we see today such as Google's Drive, Facebook and Twitter, not to mention the countless other applications ranging through games, shopping, banking and dating. However, going into the future, much of these protocols and technologies will have to be re-engineered according to our new understandings of the interaction between society and technology.

Web 3.0, or as might be termed the "post-Snowden" web, is a reimagination of the sorts of things that we already use the Web for, but with a fundamentally different model for the interactions between parties. Information that we assume to be public, we publish. Information that we assume to be agreed, we place on a consensus-ledger. Information that we assume to be private, we keep secret and never reveal. Communication always takes place over encrypted channels and only with pseudonymous identities as endpoints; never with anything traceable (such as IP addresses). In short, we engineer the system to mathematically enforce our prior assumptions, since no government or organisation can reasonably be trusted.

There are four components to the post-Snowden Web: static content publication, dynamic messages, trustless transactions and an integrated user-interface.

The first, we already have much of: a decentralised, encrypted information publication system. All this does is take a short intrinsic address of some information (a hash, if we're being technical) and return, after some time, the information itself. New information can be submitted to it. Once downloaded, we can be guaranteed it's the right information since the address is intrinsic to it. This static publication system accounts for much of HTTP(S)'s job and all that of FTP. There are already many implementations of this technology, but the easiest to cite is that of Bit Torrent. Every time you click on a magnet link of Bit Torrent, all you're really doing is telling your client to download the data whose intrinsic address (hash) is equal to it.

In Web 3.0, this portion of the technology is used to publish and download any (potentially large) static portion of information that we are happy to share. We are able, just as with Bit Torrent, to incentivise others to maintain and share this information, however combined with other portions of Web 3.0, we can make this more efficient and precise. Because an incentivisation framework is intrinsic to the protocol, we become (at this level, anyway) DDoS-proof by design. How's that for a bonus?

The second portion of Web 3.0 is an identity-based pseudonymous low-level messaging system. This is used for communicating between people on the network. It uses strong-cryptography in order to make a number of guarantees about the messages; they can be encrypted with an identity's public key in order to guarantee only that identity can decode it. They can be signed by the sender's private key to guarantee that it does indeed come from the sender and provide the receiver with a secure receipt of communication. A shared secret can provide the opportunity to communicate securely, including between groups, without the necessity of proof of receipt.

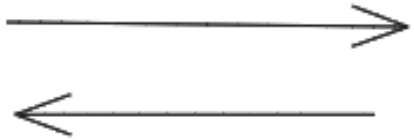
Since each of these provide ultimate message logistics, the use of transmission-protocol level addresses becomes needless; addresses, where once user or port together with IP address, now become merely a hash.

Messages would have a time-to-live, allowing the disambiguation between publication messages that one may wish to be 'alive' for as long as possible to guarantee as many identities see it and instant signalling messages that wish to be transmitted as quickly as possible across the network. Thus the dichotomy of latency and longevity is traded.

Actual physical routing would be carried out through an game-theoretic adaptive network system. Each peer attempts to maximise their value to other peers in the assertion that the other peers are valuable to them for the incoming information. A peer whose information is not valuable would be disconnected and their slot taken with a connection to some other, perhaps unknown (or perhaps second-degree), peer. In order that a peer be more useful, messages with some specific attributes would be requested (e.g. of a sender address or topic---both unencrypted---beginning with a particular bit string).

https://gavwood.com/dappsweb3.html

Client



Blockchain

Web3 Applications

- **Brave Browser** - Privacy focussed web browser
- **Odysee** - Video Streaming platform
- **Minds** - Social media network
- **Uplandme** - Gaming platform
- **Mastodon** - Open source social network

WHAT

ARE WE

LEARNING

HERE ?

Stage-01

Web Page Development : HTML

Styling :CSS & tailwind

Interactive: JS

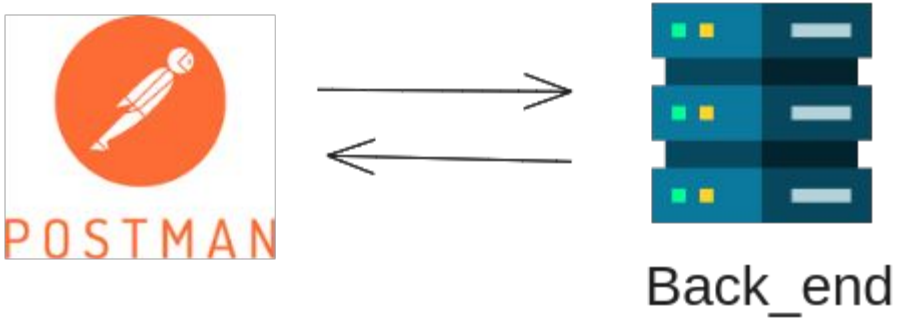
Client

Stage-02

Back-end : Node JS , Express

Testing : Postman

Database : MongoDB



Stage-03

Front-end : React

Styling : Tailwind

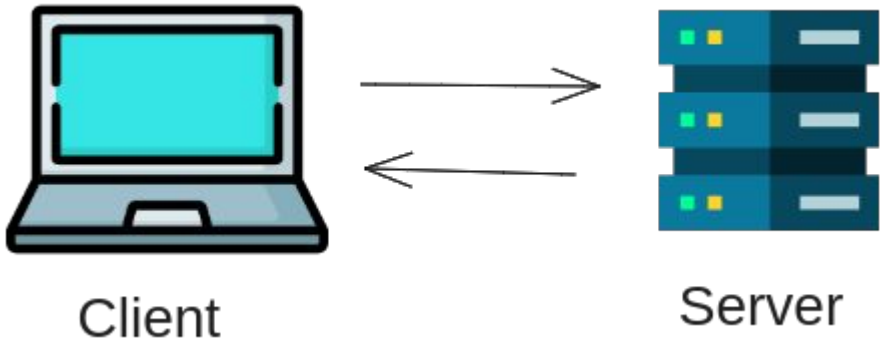
Client

Stage-04

Front-end : React

Back-end : Node JS , Express

Database : MongoDB

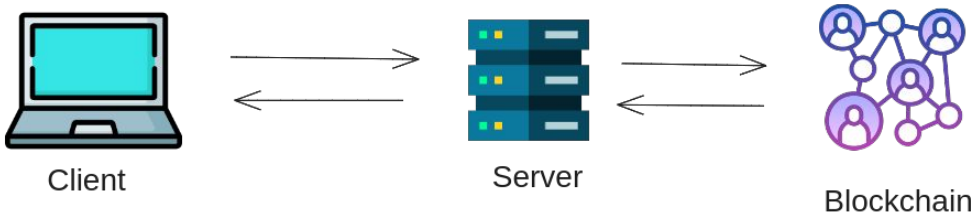


Stage-05

Front-end : React

Back-end : Node JS , Express

Blockchain : Ethereum & Hyperledger




JOBS
AWAITING

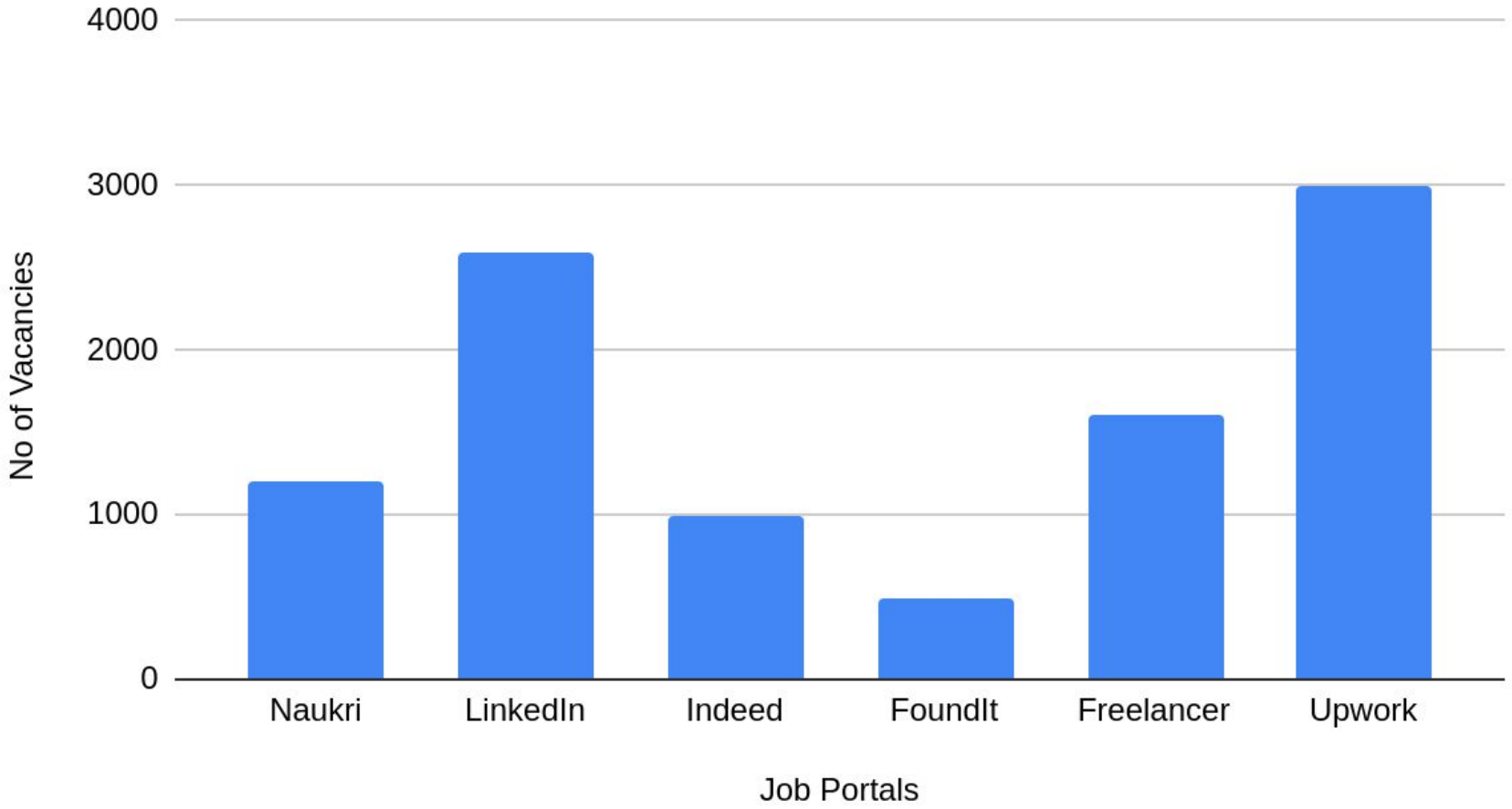
Web2 Jobs

- Web Developer
- Front-end developer
- UI Developer
- React Developer
- Back-end Developer
- NodeJs Developer
- MERN Developer
- Full-Stack Developer
- Web Developer Intern
- Web Developer Trainee
- Technical Content Writing
- Teaching/ Training

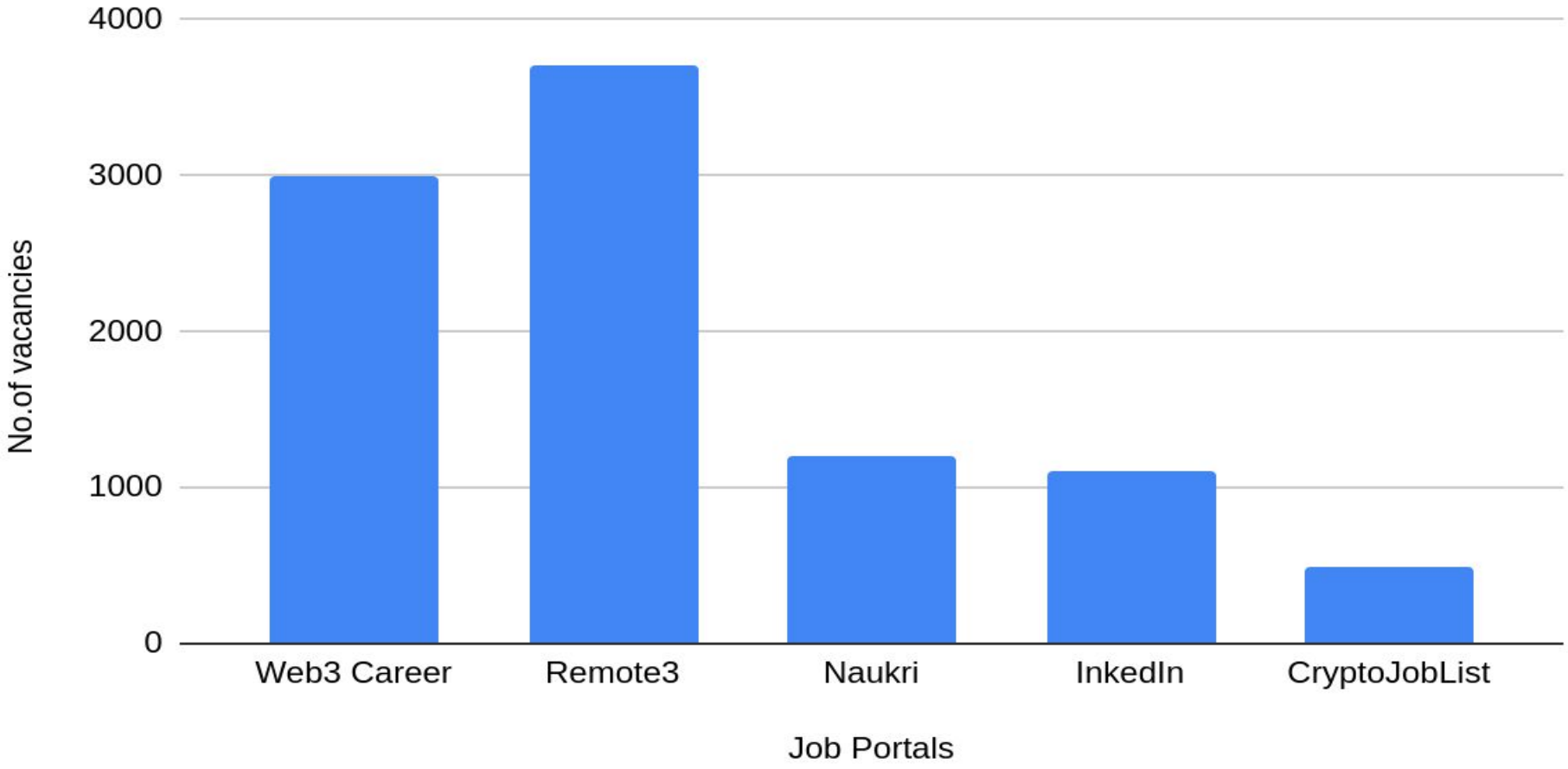
Web3 Jobs

- Blockchain Developer
- Web3 Engineer
- Research Engineer
- Blockchain Intern
- Blockchain Architect
- Blockchain Consultant
- Blockchain Engineer
- Ethereum Developer
- Solidity Contract Developer
- Hyperledger Fabric developer
- Blockchain Trainer
- Blockchain Content Writer
- Blockchain Trainee
- Private Blockchain Developer

Web2 Jobs


4000
3000
2000
1000
0
No of Vacancies
Naukri
LinkedIn
Indeed
FoundIt
Freelancer
Upwork
Job Portals

Web3 Jobs


4000
3000
2000
1000
0
No.of vacancies
Web3 Career
Remote3
Naukri
InkedIn
CryptoJobList
Job Portals


CSS
HTML
C++

- W3Schools
- MDN Web Docs
- GeeksforGeeks
- DevDocs
- Medium

- Simplilearn
- Traversy Media
- freeCodeCamp.org
- Net Ninja
- Telusko
- Brototype

https://digitrendz.blog/tech-news/5166/bard-rebrands-as-gemini/
https://nazhimkalam.medium.com/github-copilot-695122622831