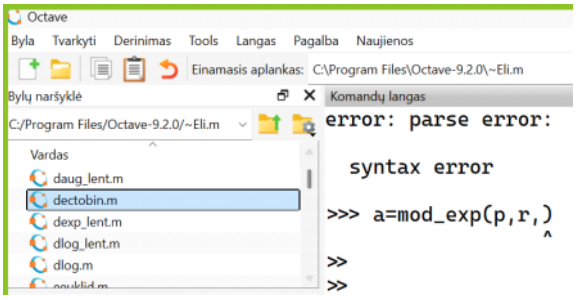
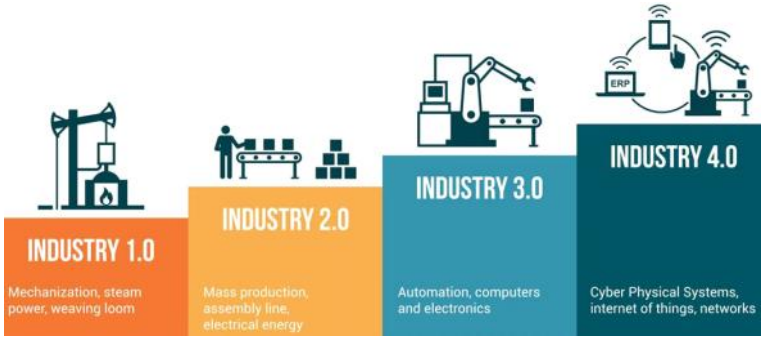
Lectures are translated throuh the **Zoom**:
https://liedm.zoom.us/j/9999112448
Passcode: **12345678**

The material of the lecture consists of pdf file and of audio/video file recorded in mp4 format.
These files can be found in the site:
https://crypto.fmf.ktu.lt/telekonf/archyvas/B111_Kriptologija/B111_2026-P/

http://crypto.fmf.ktu.lt/xdownload/

- octave-9.2.0-w64-installer.exe
- octave.Stud.7z

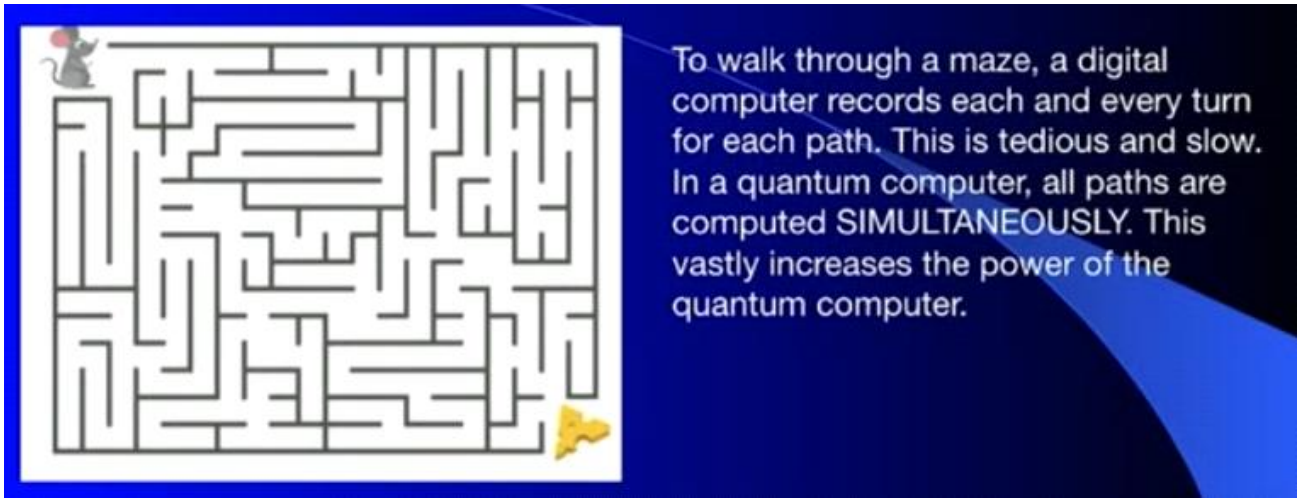




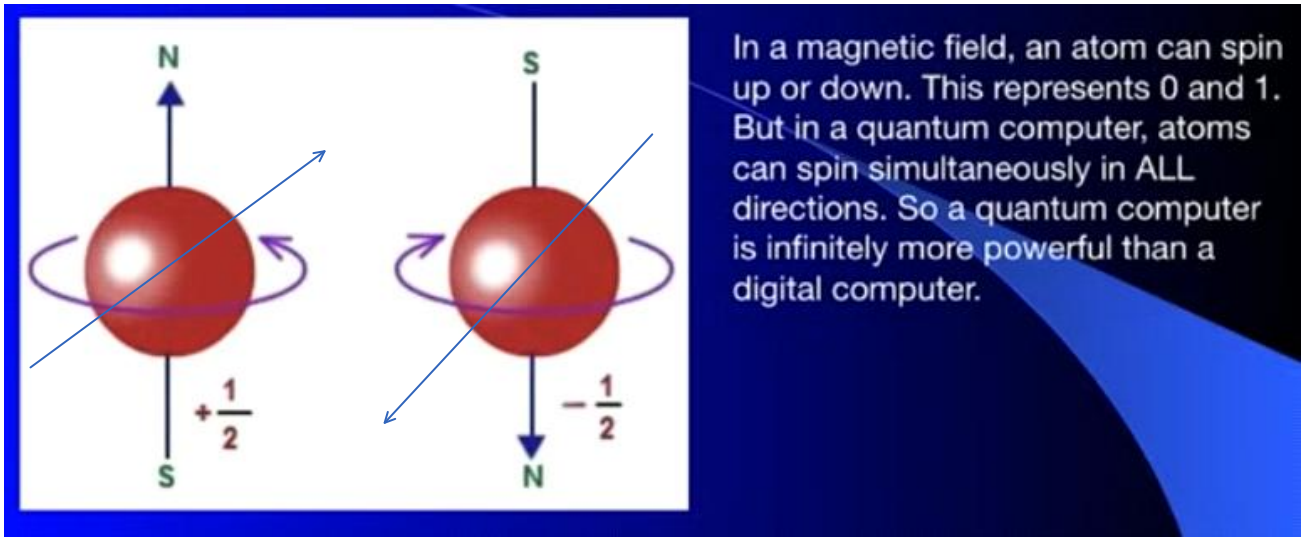
Quantum Computers --> Existing cryptographic methods can be broken by the algorithms realized in Quantum Computers, e.g. Peter Shor algorithm.
It is named as Quantum Cryptanalysis. Year-to-Quantum - Y2Q.

Post-Quantum Cryptography - **PQC**:
Cryptographic methods are realized by classicall computers but they can not be broken by Quantum Computers.

Michio Kaku
https://www.youtube.com/watch?v=_OjRClPzU6Y



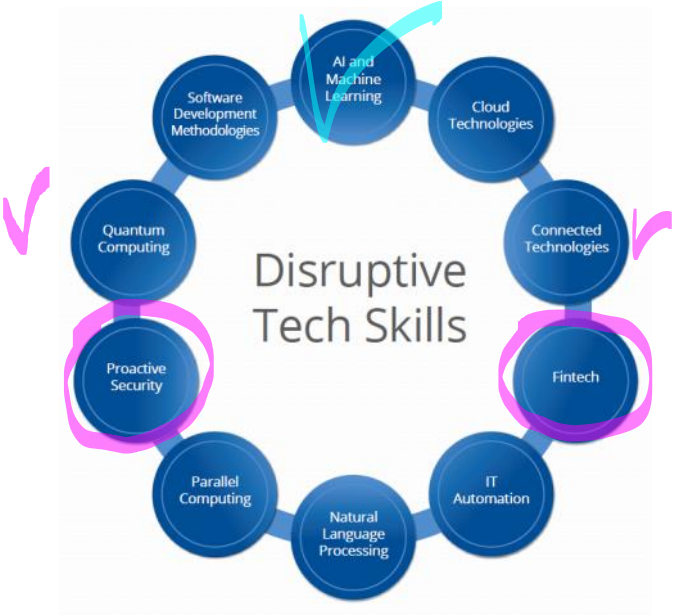
The mouse surveys all paths in the maze simultaneously due to Quantum Entalgement phenomena in quantum world.



https://www.burning-glass.com/
https://www.burning-glass.com/wp-content/uploads/2020/12/Skills-of-Mass-Disruption-Report.pdf
Skills-of-Mass-Disruption-Report.pdf

Skills of Mass Disruption Tecnologies
Įgūdžiai Masinio Proveržio Technologijose

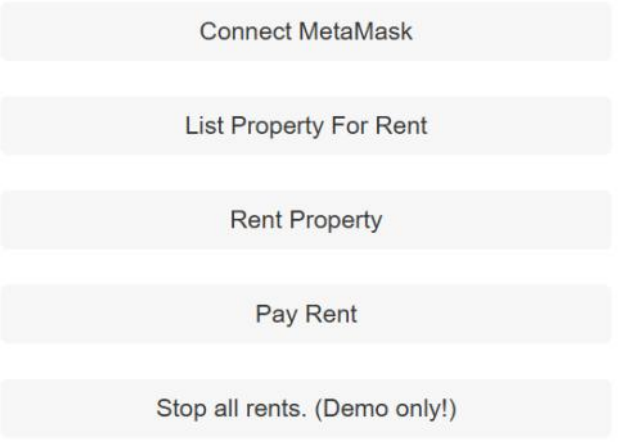
burningglass TECHNOLOGIES Solutions



Skills of Mass Disruption
To help organizations pinpoint disruptive tech skills, Burning Glass Technologies analyzed more than 17,000 unique skills demanded across our database to identify the top 10 most disruptive skills in tech.

Fintech: Skills related to technologies such as **blockchain** and others aimed at making **financial transactions more efficient and secure**.

https://tokenvita.net/



http://crypto.fmf.ktu.lt/xdownload/

- EuroNews 2019.01.23 11 Carlos.Moedas_Davos_Day 2.mp4
- Euronews 17-03-2015 15-38 CET_150316_HTSU_121B0-172837_E.mp4

eBanking ← Smart Id

Documents\REKLAMA

New Economic Movement - NEM

Industry Tokenization
Crowd Funding

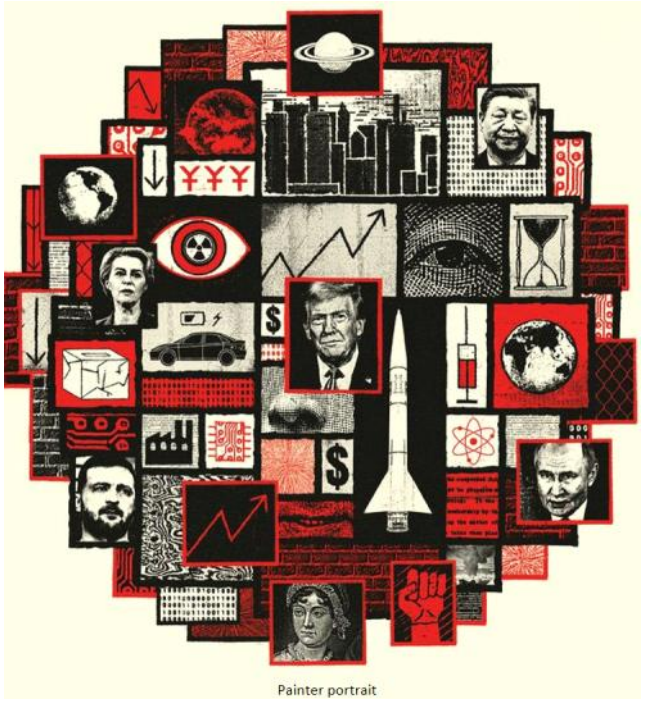
Blockchain technology for business monitoring and control:

1. Cryptocurrency.
2. Smart Contracts: Solidity, Go Language --> Ethereum programming: GEth
3. Tokens -Investment Tools: ICO - Initial Coin Offer
   STO - Secure Token Offer - unsufficient regulation
   NFT - Non-Fungible Tokens

TSMC

https://boomers-daily.com/2022/11/15/analysis-the-world-ahead-2023-the-economist/

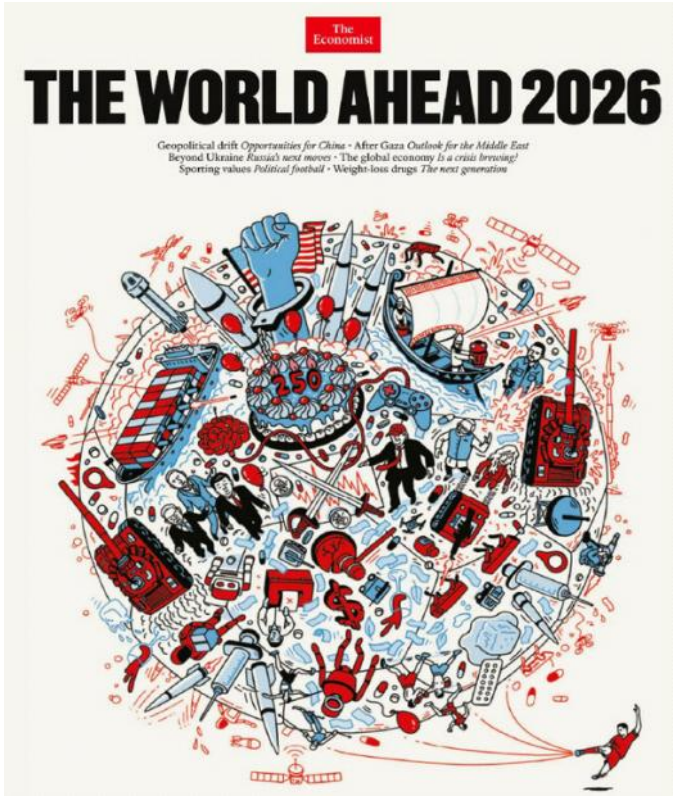
https://www.economist.com/the-world-ahead/2024/11/18/tom-standages-ten-trends-to-watch-in-2025



Painter portrait

The year of Saturn

THE WORLD AHEAD 2026 - The Economist - 15 Nov 2025
From <https://www.scribd.com/document/949792345/THE-WORLD-AHEAD-2026-The-Economist-15-Nov-2025-1>



https://www.burning-glass.com/research-project/skills-mass-disruption/
Organizations and technology executives know they must adopt new technologies to remain competitive. To help organizations pinpoint the disruptive technology skills that they can begin planning for today, Burning Glass Technologies analyzed more than 17,000 unique skills demanded across our database of over 1 billion historical job listings to identify the top 10 most

disruptive skills in tech.
Some of the key findings from ***Skills of Mass Disruption*** are:
• **Many disruptive tech skills are already in demand and growing fast**. In the past 12 months there were 1,714,483 U.S. job openings requesting at least one of the disruptive skill areas. Over the next five years, they are projected to grow between 17% and 135%. The skill areas projected to grow the fastest include Quantum Computing and Connected Technologies, with forecasted growth rates of 135% and 104%, respectively.
• **These skill areas are spreading across many different occupations and industries**. Eight of the 10 skill areas are already commonly requested in over 30% of occupations. None of the skill areas except Quantum Computing have more than 40% of demand concentrated within one industry. This diffusion of skills across different jobs and industries is hybridizing many roles and teams, requiring employers to be thoughtful in determining which roles are best suited for embedding these skills.
• **Organizations with future-ready skills create future-ready solutions**. The most disruptive organizations are more likely to request the disruptive tech skills. Across all IT and R&D occupations, Unicorn employers – i.e., startups valued at $1 billion or more –are 33% more likely to request disruptive tech skills than legacy firms in the Fortune 100. This underscores a key maxim: future-ready teams create future-ready solutions.
* **Employers have to pay more to hire workers with these skill areas**. The average salary premiums for the disruptive skills areas range between $4,200 to $25,000. The two skill areas with the greatest average salary premiums – IT Automation and AI and Machine Learning – are both focused on automating existing tasks to become more efficient. This means many employers face a Catch-22: They need disruptive skills to remain future-ready and gain efficiencies, but they may not be able to afford hiring individuals from a limited pool of existing workers with these skills.
* **But employers have realistic options for upskilling current workers to meet the need**. By identifying existing employees in "adjacent roles" that have similar skill sets, employers may be able to strategically reskill and upskill to meet the need at less cost. For all but two of these skill areas, there are at least 200 occupations that represent strong candidates for upskilling. The two remaining skill areas, Parallel Computing and Quantum Computing, are both highly technical fields, but there are still numerous adjacent roles that can be upskilled for each.

In order to identify the most disruptive skills in tech, we analyzed over 17,000 unique skills demanded across Burning Glass's database of over one billion historical job listings. We grouped similar technology skills into related skill areas and assessed both the projected growth of each skill area over the next five years as well as each skill area's hardness to fill — a composite measure of the average time it takes to fill jobs requesting each skill, as well as the average cost premium to fill each skill. This allowed us to plot skills within Burning Glass's disruptive skills matrix — a methodology previously developed for Quant Crunch: How the Demand for Data Science Skills is Disrupting the Job Market, a joint report with IBM and the Business-Higher Education Forum.

The disruptive skills matrix classifies skills within one of the following four quadrants:
+ **Stabilizers** are skills with low projected growth and low hardness to fill. These skills are typically plentiful across the market but may still be important to key roles.
+ **Escalators** are skills with high projected growth but low hardness to fill. These are high-growth skills that are important to building a future-ready workforce but are typically common across the job market.
+ **Challengers** are skills with low projected growth and high hardness to fill. These are skills associated with established fields that provide strong value, but

there is a limited pool of talent.
+ **Disruptors** (**proveržio**) are skills with **high** projected growth and **high** hardness to fill. These are high-value skills that help firms differentiate their workforce and become future-ready – but are also the hardest for employers to find in the job market.

To narrow the list down to the top 10 most disruptive skill areas in tech, we then ranked each skill in the Disruptors category by summing their normalized projected growth, average salary premiums, and average time to fill. The 10 skills with the highest aggregate scores were selected as the 10 most disruptive skills in tech. These skills include the following:
+ **AI and Machine Learning**: Skills related to developing and utilizing programs, tools, and solutions powered by algorithms and other technologies that automatically respond and improve based upon prior experience or data.
+ **Cloud Technologies**: Skills related to developing, implementing, and securing cloud computing infrastructure and strategy.
+ **Connected Technologies**: Skills related to the Internet of Things and connected physical tools, as well as the telecommunications infrastructure needed to enable them, such as 5G.
+ **Fintech**: Skills related to technologies such as **blockchain** and others aimed at making **financial transactions more efficient and secure**.
+ **IT Automation**: Skills related to automating and orchestrating digital processes and workflows.
+ Natural Language Processing (NLP): Skills related to developing solutions and technologies build upon machineenabled processing of natural language.
+ **Parallel Computing**: Skills related to a form of computation where many calculations, or the execution of computational processes, are carried out simultaneously.
+ **Proactive Security**: Skills related to proactively securing and protecting digital infrastructure from cybercriminals and preventing cyberattacks before they occur.
+ **Quantum Computing**: Skills related to building and utilizing quantum computers and their applications.
+ **Software Development Methodologies**: Skills related to Agile, DevOps, and related approaches to developing software more rapidly, effectively, and securely.

Many disruptive tech skills are already in demand and growing fast
In the past 12 months (December 2019-November 2020) there were 1,714,483 job postings requesting at least one of the disruptive skill areas. This already represents sizable demand throughout the market, and this level of sustained employer need is especially impressive given the market-wide decline in postings due to the COVID-19 pandemic. But these skills are still maturing and are poised to continue growing at a rapid pace. Over the next five years, each skill is projected to grow at least 17%, and some are projected to grow considerably faster. The skill areas projected to grow the fastest include Quantum Computing and Connected Technologies, with forecasted growth rates of 135% and 104%, respectively.
Table 1: Job Openings and Growth by Disruptive Skill Area.

Table 1: Job Openings and Growth by Disruptive Skill Area

Skill Area	Total Job Openings (Last 12 Months)	Projected 5-Year Demand Growth
Software Dev Methodologies	634,660	35%
Cloud Technologies	462,963	28%
Proactive Security	373,123	39%
IT Automation	282,380	59%
AI and Machine Learning	197,810	71%
Connected Technologies	68,313	104%
NLP	36,941	41%
Fintech	35,667	96%
Parallel Computing	11,056	17%
Quantum Computing	2,718	135%

2020

Table 3: Average Salary Premium by Disruptive Skill Area

Skill Area	Average Salary Premium
IT Automation	$24,969
AI and Machine Learning	$14,175
Fintech	$13,799
Software Dev Methodologies	$13,762
Connected Technologies	$10,873
Cloud Technologies	$10,588
Proactive Security	$8,851
Parallel Computing	$7,797
NLP	$6,368
Quantum Computing	$4,204

Table 2. Share of All Occupations Commonly Requesting Disruptive Skill Areas

Skill Area	Share of Occupations Commonly Requesting Skill Area: (Dec. 2019-Nov. 2020)	Share of Occupations Commonly Requesting Skill Area: 2015
Proactive Security	64%	57%
Cloud Technologies	58%	55%
Software Dev Methodologies	57%	53%
AI and Machine Learning	56%	37%
Connected Technologies	41%	25%
NLP	35%	27%
IT Automation	34%	16%
Fintech	33%	13%
Parallel Computing	10%	12%
Quantum Computing	4%	1%

Figure 3: **Demand for Disruptive Tech Skills by Industry Sector**

	AI and Machine Learning	Cloud Technologies	Connected Technologies	Fintech	IT Automation	NLP	Parallel Computing	Proactive Security	Quantum Computing	Software Dev Methodologies
Professional Services	25%	31%	29%	40%	32%	28%	22%	28%	76%	31%
Finance and Insurance	17%	14%	4%	30%	18%	22%	5%	24%	3%	20%
Information / IT	13%	19%	26%	11%	17%	14%	10%	7%	6%	12%
Manufacturing	15%	8%	14%	3%	11%	7%	26%	11%	2%	12%
Retail Trade	8%	7%	6%	3%	4%	7%	10%	3%	2%	5%
Adminstrative Services	3%	6%	3%	6%	6%	4%	3%	5%	0%	5%
Educational Services	5%	2%	1%	1%	2%	5%	7%	3%	8%	1%
Health Care and Social Assistance	5%	3%	11%	1%	2%	4%	3%	4%	0%	3%
Public Administration	3%	3%	1%	2%	3%	3%	2%	8%	1%	3%
Transportation and Warehousing	2%	2%	1%	1%	1%	1%	2%	1%	0%	2%
Other Industries	4%	6%	4%	2%	4%	6%	10%	5%	1%	5%

ConsenSys.com
Ethereum

IBM Hyperledger Fabric
(HF)
Maersk Renault

Employers have to pay more to hire workers with these skill areas.
Disruptive skills are disruptive for a reason: They are **high value and not everyone has them**.
Not surprisingly, this puts significant upward pressure on salaries. On average, the disruptive skill areas come with salary premiums ranging between $4,200 and $25,000. The two skill areas with the greatest average salary premiums – IT Automation and AI and Machine Learning – are both focused on automating existing tasks to make them more efficient. This means many employers face a Catch-22: They need disruptive skills to remain future-ready and gain efficiencies, but they may not be able to afford hiring individuals from a limited pool of existing workers with these skills.

But employers have realistic options for upskilling current workers to meet the need.
To combat the increased cost and difficulty of filling positions with the disruptive skill areas, employers can build these skills within their workforce more efficiently by strategically reskilling and upskilling existing employees who already perform work using similar skills.
For all but two of these skills, there are at least 200 occupations that represent strong candidates for upskilling in these fields, as determined by analyzing roles in which each skill can both

align with existing responsibilities and typically comes with a significant salary premium. The two remaining skill areas, ***Parallel Computing*** and ***Quantum Computing***, are both **highly technical fields**, but there are still numerous roles that can be upskilled in each skill area. Organizations can, therefore, more rapidly and effectively integrate these disruptive skills into their teams by upskilling existing employees, rather than relying solely on new hires to fill gaps in their capabilities.

Table 4: **Upskilling Opportunities by Disruptive Skill Area**

Skill Area	Number of Occupations Representing Strong Upskilling Candidates*
Proactive Security	598
Software Dev Methodologies	544
Cloud Technologies	524
AI and Machine Learning	512
Connected Technologies	313
Fintech	311
IT Automation	282
NLP	226
Parallel Computing	67
Quantum Computing	10

4. Implications and Recommendations

Employers

+ Make Developing Disruptive Skills a Priority, Based Upon Your Strategic Goals. Teams with future-ready skills build future-ready solutions. Therefore, it is imperative for organizations to determine which disruptive skills are most important for them to integrate into their teams to support their current and future strategic priorities. Firms can also take inspiration from disruptive newcomers – such as Unicorns – to understand how these skills can help them build next-generation solutions.

+ Break Down Silos to Build a Future-Ready Workforce. Many roles are hybridizing and demand emerging tech skills, even when on non-technical teams. This requires leaders across teams to collaborate on developing a workforce with the skills needed to thrive. Since tech is often the driver of workforce hybridization, the IT and HR (Human Resources) departments make natural bedfellows in many strategic workforce planning endeavors.

+ Invest in Your Workers with Targeted Upskilling. Hiring workers who already have disruptive skills is costly and can take a long time. Upskilling and reskilling workers in adjacent roles can reduce the cost and time it takes to build a future-ready team, while also supporting employee retention and advancement.

Students and Job Seekers

+ Identify and Learn High-Value Disruptive Skills. The disruptive tech skills are growing rapidly and can lead to significant salary boosts. Individuals who identify and develop these future-ready skills – and continuously update their skill sets as new needs emerge – will be best-positioned to enhance their career prospects, both in tech and beyond.

Training Providers

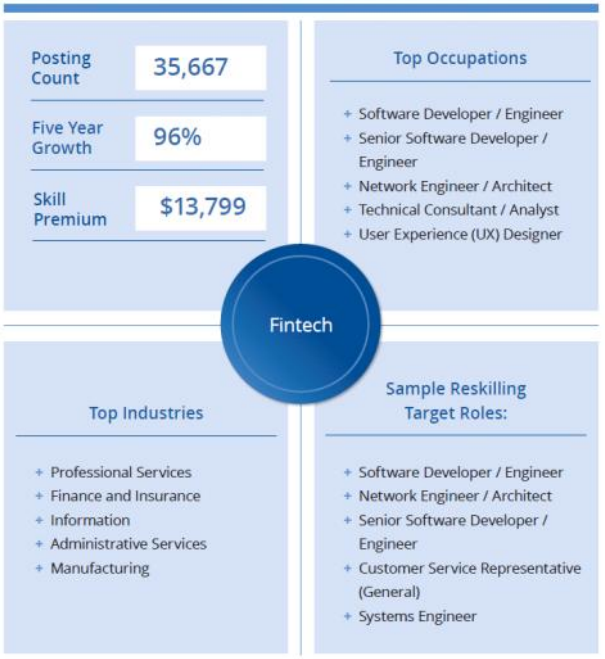
+ **Incorporate Disruptive Skills into Existing Programs**.
The job market is changing much faster than most curricula. Students who graduate with future-ready skills are best positioned to thrive in the job market, and training providers can ensure they leave school with these skills by incorporating them into existing programs. This includes both tech programs and other disciplines, where workers in nontechnical fields can benefit by building a hybrid skill set combining emerging tech skills and other competencies.

+ **Build Short-Term Programs to Teach Disruptive Skills to Working Learners**.
Many existing workers will be looking to continuously upskill in emerging fields. Training providers can support them by building short-term training programs specifically tailored to workers and individuals looking to enhance their abilities in new fields in order to improve their employment prospects.
+ **Communicate the Value of Disruptive Skills**.
The disruptive tech skills can be highly lucrative for individuals who possess them. Training providers can motivate students to learn these skills by communicating the value they confer, in terms of both increased salaries and increased employment opportunities. This will also encourage students to enter and remain within programs dedicated to teaching these emerging, high-value skills.

Technology Vendors

+ **Build a Community of Disruptors**.
To build a large user base for a disruptive solution, you need to educate workers in the skills needed to use it.
Communicating the value of learning these disruptive skills to students and workers – while also providing the resources needed to help them build these skills – can dramatically expand your pool of potential users.

Fintech



CRYPTOGRAPHY

Euronews 17-03-2015 15-38 CET _150316_HTSU_121B0-172837_E https:// ← KAP

http://crypto.fmf.ktu.lt/xdownload/

Euronews 17-03-2015 15-38 CET _150316_HTSU_121B0-172837_E.mp4

Smart Id

Identification from the Bank' side: certificate recognizable in User's browser. Verisign
Weak identification on the User's side.
Public Key Infrastructure - PKI + Biometrics + Multifactor Id (Smart Id. - GPRS).

Diagram

https://imimsociety.net/en/

https://www.facebook.com/IMIMSociety-776869965820856/

https://imimsociety.net/en/home/15-wolf-goat-and-cabbage-transfer-across-the-river-algorithm.html

Central Bank Digital Currency - CBDC

Researcher: Massachusets Institute of Technology - MIT

Platform Ethereum

Developer: ConsenSys.com

WP_20190124_19_21_36 Davos_2019.MP4

http://crypto.fmf.ktu.lt/xdownload/

- EuroNews_2019.01.23_11 Carlos.Moedas_Davos_Day 2.mp4

$O(Log_2N)$
$O(N)$
$O(2^N)$
2^{64}

Quantum computers → compromizes traditional cryptography

Y2Q: Year to Quantum = 20XX

P vs NP : P = NP P ≠ NP

BlockChain

For monitoring and control business processes.

https://onlineprogrammes.sbs.ox.ac.uk/presentations/lp/oxford-blockchain-strategy-programme/?ef_id=c:355184111442_d:c_n:g_ti:kwd-296270282059_p:_k:cryptocurrency_m:e_a:61795563965&gclid=Cj0KCQiAmsrxBRDaARIsANyiD1rST3aJzQINrHxPs0oyIVh8VAwoZ49Qo3zlSI664JR

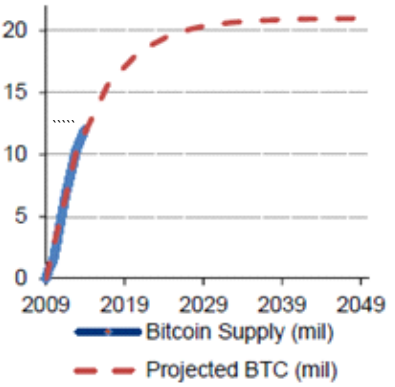
JXZ5xgab4CJAaAkIVEALw_wcB&gclsrc=aw.ds

https://coinmarketcap.com/

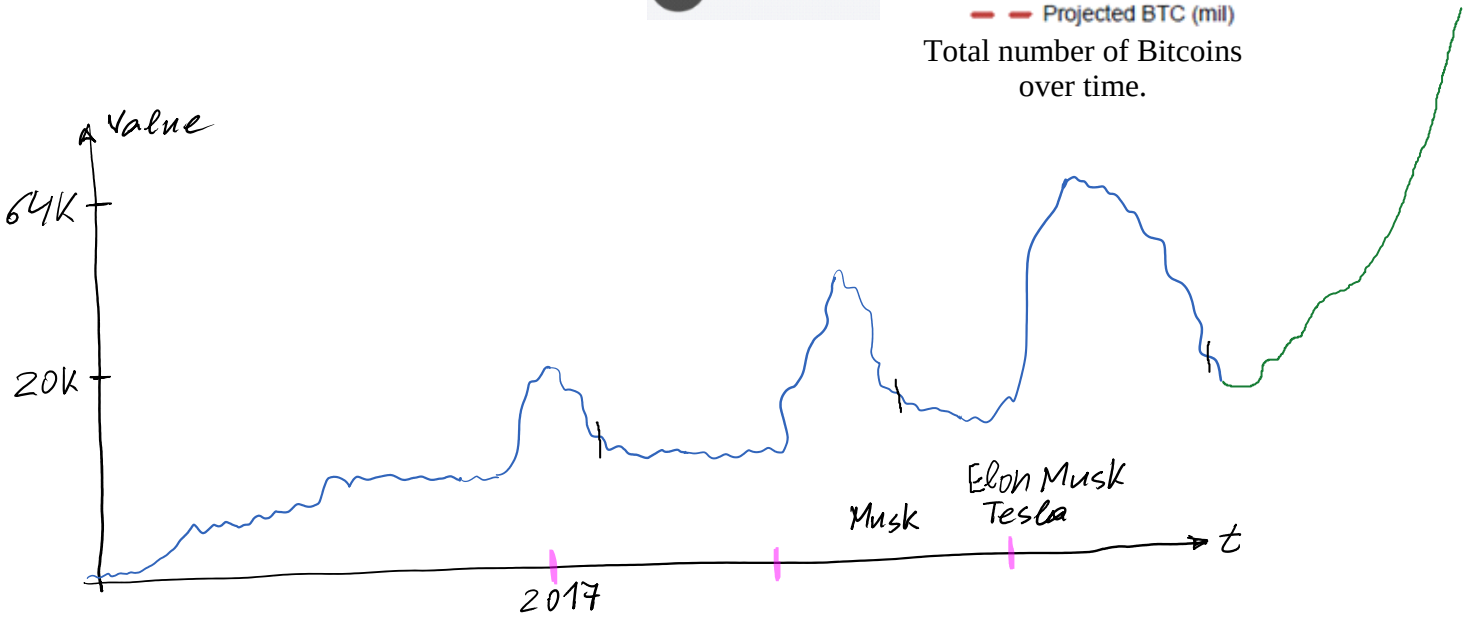
Bitcoin - BTC https://bitcoin.org/en/

Ethereum - ETH https://ethereum.org/

Monero https://www.getmonero.org/



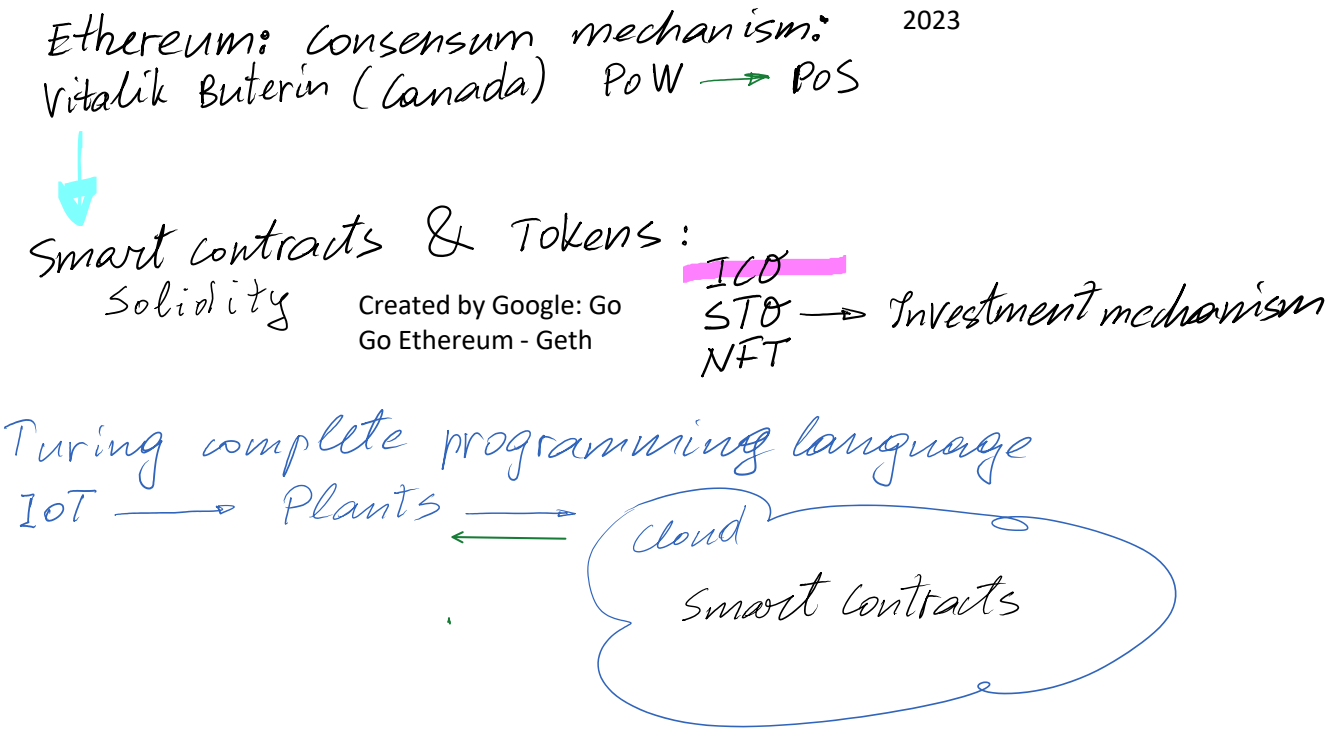
Total number of Bitcoins over time.



In addition, the most middle term dangerous threat for the internet security is the rapid development of quantum computers. At the end of 2023 IBM presented a 1121-qubit microprocessor. A very rapid development of quantum computers is observed in China creating 504-qubit chip. In 2024 Russia Lomonosov claimed to have developed a 50-qubit microprocessor. Referencing to quantum computers capabilities P. Shorr presented the quantum cryptanalysis algorithms breaking classical cryptographic methods. Such threats forced National Institute of Standards and Technology (NIST) to stimulate creation of post-quantum cryptography methods. This cryptography means that cryptographic methods are created for classical computers but they are not vulnerable to recently known quantum cryptanalysis. In December 2016, they released a call for proposals announcement to initiate the development of such schemes. In 2022 four algorithms were selected. Three of them were digital signature schemes. On August 13th, 2024 NIST published FIPS 204 and FIPS 205 where digital signatures based on the CRYSTALS-Dilithium and the SPHINCS+ schemes were standardized. Despite of a great attempts it is only the first step toward creation of post-quantum cryptography. Proposed schemes do not guarantee required functionality.

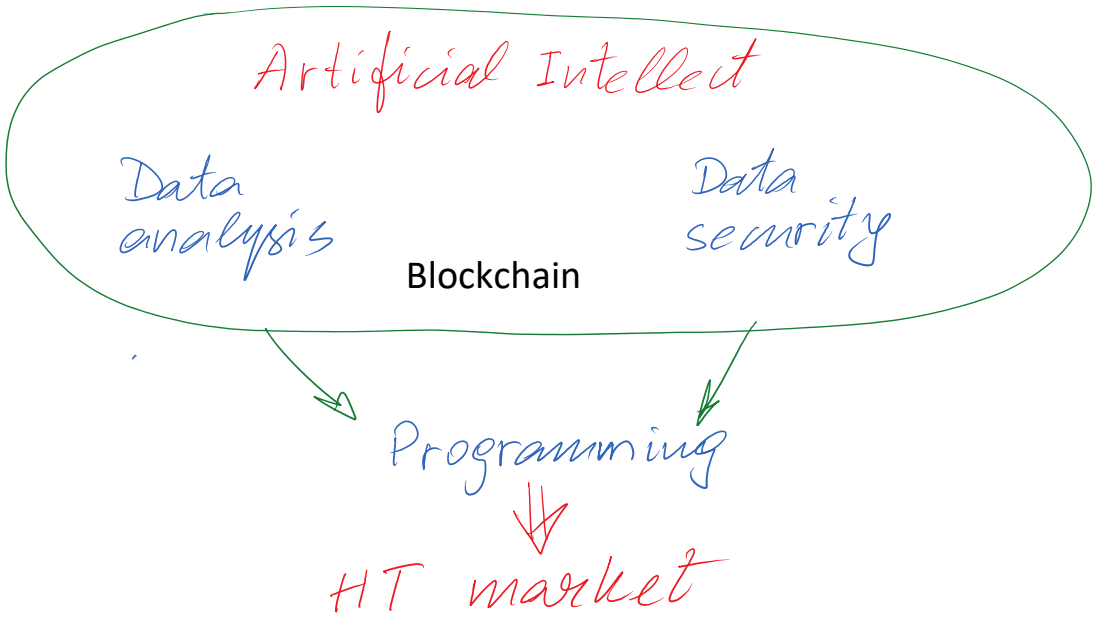
The worldwide trend is the penetration of blockchain technology to global finances and business processes monitoring and control. Recently there are many discussions concerning creation of Central Bank Digital Currency (CBDC) or certain alternatives for it. Therefore, blockchain technology is a leading direction in this global trend. It will be impossible to guarantee the security of these technologies without implementation of post-quantum cryptography in near future. The

operational devices of users in blockchain technology are classical computers and mobile devices providing secure e-wallets with other security services. The public blockchain technology provides security, transparency, and immutability and hence trustworthiness of transaction. In private blockchain the privacy of transactions must coexist with their verifiability for all net of users. It can be achieved by additional functionality of post-quantum cryptography.



Temos:
Kriptografija: šifravimas, e-parašas, identifikacija internete, duomenų integralumas.
Bitcion‘as: nauja pinigų era, technologija, saugumas, socialinė įtaka, kasyba, vertės sukūrimas.
Kriptovaliutos:technologija, įvairovė ir egzotika, saugumas, panaudojimo įvairovė, t.t.
Blokų grandinės: e-dokumentai, patikima ekonominė ir socialinė veikla, t.t.
Daiktų Internetas: technologija, ateities gamyklos, globalizacija, 5G ir 6G internetas.
Išmanieji Kontraktai: technologija, panaudojimas.

Topics:
Cryptography: encryption, e-signature,identification in internet, data integrity.
Bitcoin: new age of money, technology, security, social impact, mining, value creation.
Cryptocurrencies: technology, diversity and exoticism, security, variety of applications, etc.
Blockchain: e-documents, trusted economical and social activity, etc.
Internet of Things (IoT): technology, future manufactures, globalization, 5G and 6G internet.
Smart Contracts: technology, applications.



Practice

http://crypto.fmf.ktu.lt/ --> Octave tools to learn Cryptography
--> Study materials
--> Other downloadable information

```
>> 2*2
ans = 4
>> mod(15*5,10)
ans = 5
>> 15*5
ans = 75
>> mod(37,11)
ans = 4
>> mod_exp(2,3,7)
ans = 1
>> p=genstrongprime(28)
p = 266352323
>> isprime(p)
ans = 1
```

```
>> r=123456678
r = 1.2346e+08              // float variable format
>> r=int64(123456789)   // integer format 64 bits
r = 123456789
>> dec2bin(p)
ans = 11111110000000110110110000011
>> g=randi(p)
g = 1.0487e+08
>> g=int64(randi(p))
g = 158646790
>> x=r;
>> a=mod_exp(g,x,p)
a = 196830972
```