KTH Computer Science
and Communication

Är kryptovalutor* någonting för framtiden?

*kryptovalutor är fullt digitala valutor som förlitar sig på kryptografi för att skapa och administreras. Största och mest kända heter Bitcoin (฿, BTC, XBT).

PETTER SALMINEN

School of Computer Science, CSC
Information Search LI1101, HT2013

Innehåll

Kapitel 1

Sökuppgiften

1.1 Notation

Söksträngar är skrivna i verbatim, som exempel `"en sök sträng"`. Booleska operatorer är skrivna in VERSAL STIL, dessa är, AND, OR samt NOT.

1.2 Databaser

I uppgiften var det givet att man skulle använda 2 olika databaser för sin sökning. Men jag har tagit det aktiva valet att expandera detta till samtliga fem: *ACM Digital Library*[1], *ArXiv.org*[2], *IEEE Xplore*[3], *Inspec*[4] och *Scopus*[5].

1.3 Sökningen

Min initiala sökning som beskrivs i 1.3.1, med analys av sökningen och resultat. Denna sökning förbättras till 1.3.2 genom att använda ord i *Inspec* ur deras kontrollerade och kontrollerade ordlista.

Senare gick jag över till att eftersom min sökning handlar om någon ganska nytt, och svårplacerat i deras tesaurus, så bestämde jag mig som beskrivs i 1.3.3 att bredda min sökning med färre söktermer, men manuellt kolla på sammanfattningarna och titlarna för att göra en relevansvärdering.

Eftersom jag inte var ännu nöjd med mitt resultat, breddade jag även ut mig för att söka i fler databaser, detta beskrivs vidare i 1.3.4.

1.3.1 Första försök

Jag började att söka igenom databaserna *IEEE Xplore* och *Inspec* med följande fråga.

("Digital currency") AND ("future")

Båda databaser gav under vanliga förutsättningar inga svar, däremot gav *IEEE Xplore* 49st svar om man ändrade inställningarna på sökningen till en fulltext sökning.

Analys av sökstrategi

Själva sökningen gav inte några större resultat, vilket antagligen berodde på att orden ej var standardiserade och att jag endast fick resultat då jag sökte via fulltext sökning. Detta för att folk har i sina rapporter använt orden "future" och "digital currency" men dessa är vare sig 'taggar' eller välanvända ord i sammanfattningarna.

Resultat

Trotts detta fick jag en bra referens[6], som även hjälpte mig med att hitta bättre sökord inför nästa iteration. Den gav mig detta resultat i *IEEE Xplore*, vilket antagligen skulle hjälpa mig med framtida sökningar.

```
INSPEC: CONTROLLED INDEXING
electronic money.

INSPEC: UNCONTROLLED INDEXING
Bitcoin

IEEE TERMS
Cryptography
Currency
```

Övrigt hade denna artikel en väldigt ögonfallande 'abstract', som inledde med "*There's nothing like a dollar bill for paying a stripper.*". Resten av sammanfattningen är bifogad i Bilaga A.1.

1.3.2 Andra iterationen

Till andra sökningen har jag nu anpassat mig lite, och använder många fler ord än "digital currency" för att leta efter digitala valutor. Jag använder mig av OR för att slå ihop sådant att en artikel kan innehålla något av de följande pengar-termena *Digital currency*, *Bitcoin*, *electronic money* eller bara *currency*. Sen binder jag ihop med att artikeln även måste vara taggad med orden *cryptography* samt *future* med AND-operatorn. Detta gav mig följande söksträng.

("Digital currency" OR "Bitcoin" OR "electronic money" OR "currency") AND ("cryptography") AND ("future")

Denna gång fick jag betydligt mycket fler svar , men precisionen var ännu ganska låg. *IEEE Xplore* gav mig 5 resultat utan, och 554 resultat med fulltext sökning. Samt *Inspec* gav mig denna gång 23 resultat.

Analys av sökstrategi

Tillägget av fler ord än "digital currency" gav betydligt fler resultat, speciellt eftersom dessa ord finns i tesaurus och är relativt vanliga och bra ord. Sen även är många saker som vanligen handlar om icke digitala pengar (om de skulle vara 'taggade' med "currency") bortfiltrerade av satsen "AND ("cryptography")".

Utan denna sats skulle det förekomma betydligt fler resultat i min resultatlista speciellt irrelevanta sådana.

Resultat

Trots att jag denna gång fick fler resultat, så hittade jag bara en[7] som kändes relevant. Detta är en relativt gammal men titeln var extremt relevant till min fråga. "Electronic cash-technology will denationalise money" - "Elektronisk pengar-teknik kommer avnationalisera pengarna". Den handlar inte direkt om Bitcoins, men mer ett socio-ekonomiska effekter av teknologisk framgång.

Även gav mig denna mig ett bra ord för framtida sökningar, istället för "future" ska jag använda "technological forecasting" för artiklar som försöker förutse framtiden genom teknologiska förändringar. Om bra artiklar finns kan de hända använda denna 'tag'.

1.3.3 Tredje iterationen

I denna sökning så tänkte jag att jag mer eller mindre, egentligen bara ville ha saker taggade av "technological forcasting" istället för "future" samt utbredda min Bitcoin sökning till olika derivat genom att asterisk som ett jokertecken i slutet av bitcoin för att matcha med alla andra, exempelvis "Bitcoins", "Bitcoin technology" som jag har sett dyka upp i olika tesaurus. Jag kände att jag ville försöka vara mer precist, och därmed ta bort "cryptography" och "currency". Detta gav mig följande sökning.

("bitcoin*" OR "electronic money") AND ("technological forecasting")

Denna gång gav gick jag 2 resultat (varav 12 via fulltext) på *IEEE Xplore* och 11 resultat via *Inspec*.

Analys av sökstrategi

Min känsla här är att det inte finns speciellt mycket skrivet om "Bitcoin", och skälet till att jag får väldigt få resultat kan vara mitt mycket begränsade område, samt

även att det är relativt nytt. Jag borde helt enkelt bara kolla hur många artiklar som innehåller ordet "Bitcoin" och om de är rätt få, gå igenom dem manuellt - samt, även använda andra databaser.

Resultat

Fastän jag fick väldigt få resultat så fick jag en artikel i ögonvrån[8]. Denna måste läsas mer noggrant för att kunna analysera om detta val var en succé eller en flopp. Den handlar inte direkt om "Bitcoin" konstigt nog, utan mer generellt om virtuella pengar och inflation.

1.3.4 Slutgiltiga sökningen

Jag bestämde mig sedan slutligen att bara söka efter "Bitcoin*" för att se hur många resultat detta skulle ge. Däremot fick jag inte några nya relevanta artiklar till min sökning, så jag bestämde mig att söka igenom några andra databaser efter ny information. Detta gav mig många bra papper om relevanta saker.

Jag sökte då även igenom databaserna *ACM Digital Library*, *ArXiv.org* och *Scopus*[5].

Analys av sökstrategi

Just i denna uppgift verkar det som det är mer relevant att söka efter allt man kan hitta som innehåller "Bitcoin" snarare än att använda logik för att begränsa sökningen för att undvika att få för många träffar. Att jag bestämde mig att kolla igenom ännu fler databaser kändes som en bra idé och visar sig ha lönat sig något avsevärt.

Resultat

Sökningen av bara ``` ``bitcoin*'' ``` gav mig inte många resultat. 34 (respektive 7) via *IEEE Xplore* på vid fulltext läge, samt 21 resultat på *Inspec*. Via *Inspec* så hittade jag en artikel om pengartvättning då det gäller kryptovalutor[9]. I *ACM* fann jag 45 resultat, varav tre stycken intressanta[10, 11]. *ArXiV* fann jag 11 olika resultat, varav ett stort papper som påminner om ett exjobb om bitcoins[12]. *Scopus* fann jag 26 resultat, varav tre stycken intressanta[13–15].

1.4 Diskussion om databaserna

De två första databaserna jag valde var *IEEE Xplore* och *Inspec* då dessa verkar vara något av de främsta artikel databaserna för data- och elektro-ingenjörer. Däremot kan man märka att man får en del krockar mellan dessa databaser då det mesta antas komma från "Institution of Engineering and Technology". Båda dessas sök-verktyg fungerade ganska bra, dessvärre tror jag att det är mitt informationsbehov som sätter pinnen i hjulet för att visa hur pass bra de fungerar egentligen.

Detta gjorde att jag mot slutet lade till *The ACM Digital Library* som har sedan länge varit en stor motståndare till IEEE dominans. Tyvärr gav dig mig endast en artikel som är intressant, men tyvärr inte nödvändigtvis den bästa till mitt informationsbehov.

Då jag ändå inte var nöjd så använde jag även *ArXiv.org* från Cornell Universitetet och fick en som jag tror är riktigt bra. *ArXiv* har däremot ett lite sämre tillgängligt sökverktyg. Eftersom det är en liten ruta längst upp i hörnet förstår man inte att man kan göra vanliga sökningar i den.

Sist men inte minst använde jag även *Scopus* för att få några extra artiklar.

Alla databaserna verkade ha bristande information av det just jag behövde, men detta beror nog på att informationsmängden om "Bitcoin" är ganska låg. Utifrån mitt eget perspektiv så tror jag att den absolut bästa artikeln kan vara den jag fick från *ArXiv*, som har ett långt papper med massor av diskussion, men även gott om referenser till tidigare och relevanta verk.

1.5 Mitt informationsbehov

Hur stort är mitt vidare informationsbehov efter dessa sökningar i alla dessa fem olika databaser?

Jag skulle själv påstå att mitt informationsbehov med den information jag nu mottagit är relativt låg. Jag har många bra artiklar däremot som jag måste läsa igenom för att kunna fullfölja min uppgift och besvara på frågan.

Hur får jag tag på all denna information då? Ja, stora delar finns fulltexter länkade till via databaserna. Det var lite bökigt att göra det hemifrån, men jag kollade och såg att jag kunde ladda ned alla fulltexter via *KTHB* för samtliga referenser. Skulle nu inte detta varit fallet, skulle jag behöva skicka en befrågan till biblioteket sådant att dem skulle kunna fixa fram en kopia till mig.

Finns det kanske mer information jag inte hittat? Antagligen finns detta, och jag antar att dessa kan finnas i andra databaser, precis som att jag hittade många fler då jag sökte i fler databaser, så tvivlar jag inte på att det finns mer i andra. Sen finns det nog inom andra mer socio-ekonomiska artiklar skrivna av ekonomer och samhällsvetare som kan ha funderat kring framtida pengarsystem, mindre direkt länkade till "Bitcoin" men principiellt samma sak - globala valutor med mera.

1.5.1 Val av litteratur

Jag valde min litteratur först genom att kolla på titeln på dokumentet. Om det låter relevant eller intressant så gick jag vidare och läste sammanfattningen, "abstract", på engelska. Då jag hade gjort detta så fick jag i några få fall även skumma lite snabbt igenom fulltexten för att se om den är överblickande av intresse för sökfrågan.

Litteratur

[1] *Acm digital library*, This is an electronic document. Date of publication: [Date unavailable]. Date retrieved: September 13, 2013. Date last modified: September 13, 2013, 2013. URL: http://arxiv.org/.

[2] *Arxiv*, This is an electronic document. Date of publication: [Date unavailable]. Date retrieved: September 13, 2013. Date last modified: September 13, 2013, 2013. URL: http://arxiv.org/.

[3] *Ieee xplore*, This is an electronic document. Date of publication: [Date unavailable]. Date retrieved: September 13, 2013. Date last modified: September 13, 2013, 2013. URL: http://ieeexplore.ieee.org/Xplore/home.jsp.

[4] *Inspec*, This is an electronic document. Date of publication: [Date unavailable]. Date retrieved: September 13, 2013. Date last modified: September 13, 2013, 2013. URL: http://www.engineeringvillage.com/search/expert.url.

[5] *Scopus*, This is an electronic document. Date of publication: [Date unavailable]. Date retrieved: September 13, 2013. Date last modified: September 13, 2013, 2013. URL: http://www.scopus.com/.

[6] M. Peck, "The cryptoanarchists' answer to cash", *Spectrum, IEEE*, vol. 49, nr 6, s. 50–56, 2012, ISSN: 0018-9235. DOI: 10.1109/MSPEC.2012.6203968.

[7] D. Birch och N. McEvoy, "Electronic cash-technology will denationalise money", English, Berlin, Germany, 1997//, s. 95 –108.

[8] Y. Zhao, "The analysis on inflation transmission mechanism from virtual world to real world", i *Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on*, 2011, s. 703–706. DOI: 10.1109/AIMSEC.2011.6010275.

[9] R. Stokes, "Virtual money laundering: the case of bitcoin and the linden dollar", *Inf. Commun. Technol. Law*, vol. 21, nr 3, s. 221–236, okt. 2012, ISSN: 1360-0834. DOI: 10.1080/13600834.2012.744225. URL: http://dx.doi.org/10.1080/13600834.2012.744225.

[10] N. Christin, "Traveling the silk road: a measurement analysis of a large anonymous online marketplace", i *Proceedings of the 22nd international conference on World Wide Web*, ser. WWW '13, Rio de Janeiro, Brazil: International World Wide Web Conferences Steering Committee, 2013, s. 213–224, ISBN: 978-1-4503-2035-1. URL: http://dl.acm.org/citation.cfm?id=2488388.2488408.

[11] S. Martins och Y. Yang, "Introduction to bitcoins: a pseudo-anonymous electronic currency system", i *Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research*, ser. CASCON '11, Toronto, Ontario, Canada: IBM Corp., 2011, s. 349–350. URL: http://dl.acm.org/citation.cfm?id=2093889.2093944.

[12] J. A. Bergstra och K. de Leeuw, "Bitcoin and beyond: exclusively informational monies", *CoRR*, vol. abs/1304.4758, 2013. URL: http://arxiv.org/abs/1304.4758.

[13] B. Maurer, T. Nelms och L. Swartz, "When perhaps the real problem is money itself!: the practical materiality of bitcoin", *Social Semiotics*, vol. 23, nr 2, s. 261–277, 2013, cited By (since 1996)0. URL: http://www.scopus.com/inward/record.url?eid=2-s2.0-84878118835&partnerID=40&md5=4dc783b3742dc71cc010266b3be10b7b.

[14] N. Dodd, "Simmel's perfect money: fiction, socialism and utopia in the philosophy of money", *Theory, Culture and Society*, vol. 29, nr 7-8, s. 146–176, 2012, cited By (since 1996)1. URL: http://www.scopus.com/inward/record.url?eid=2-s2.0-84872008496&partnerID=40&md5=7216ffda968e516d9211dad7a5664bd1.

[15] S. Barber, X. Boyen, E. Shi och E. Uzun, "Bitter to better - how to make bitcoin a better currency", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7397 LNCS, s. 399–414, 2012, cited By (since 1996)3. URL: http://www.scopus.com/inward/record.url?eid=2-s2.0-84865819620&partnerID=40&md5=ab0c2e010d9d78a79f2b94fc5fbfc46b.

Bilaga A

The cryptoanarchists' answer to cash

A.1 Abstract

There's nothing like a dollar bill for paying a stripper.

Anonymous, yet highly personal-wherever you use it, that dollar will fit the occasion. Purveyors of Internet smut, after years of hiding charges on credit cards, or just giving it away for free, recently found their own version of the dollar-a new digital currency called Bitcoin.