Jméno a příjmení: **Adam Šárek**
Osobní číslo: **SAR0083**
Datum: **30.11.2022**

Forenzní analýza - Protokol (9)

Analýza kryptoměn

1. **Seznamte se s problematikou Blockchainu**
2. **Seznamte se s problematikou Kryptoměn**
3. **Seznamte se s problematikou trasování transakcí kryptoměn**
4. **Seznamte se s problematikou anonymity / pseudo anonymity kryptoměn**

5. **Na základě získaných a nastudovaných informací proveďte tyto úkoly:**
    a. Udělejte jednoduchý program, který simuluje proces těžení. Výsledné bloky zapište do .txt souboru ve formátu. V souboru udělejte alespoň 5 bloků s obtížnosti od 2 do 6. Obtížnost reprezentuje počet “0” na začátku hashe daného bloku:

```
Výška bloku: 0
Hash bloku: 00ce901f811158b22f286538f6e433f6
Hash předchozího: -
Data: 1b6efcb512f39f7219901e3bb7285305
Data RAW: 2000
Nonce: 10543
Obtížnost: 2

Výška bloku: 1
Hash bloku: 00565c1babd714f13157f014638bb237
Hash předchozího: 00ce901f811158b22f286538f6e433f6
Data: f6a9f0e834179d811edf8528961cc314
Data RAW: 123236
Nonce: 109882
Obtížnost: 2

Výška bloku: 2
Hash bloku: 0005153e64bc251fbe30de152da0cb58
Hash předchozího: 00565c1babd714f13157f014638bb237
Data: 8c9d6ad0746bbf3fc0761e2490760800
Data RAW: 876655
Nonce: 988323
Obtížnost: 3
```

    b. Prozkoumejte GENESIS blok Bitcoinu a zjistěte tyto informace:
        i. Hash bloku
        ii. Výška odměny
        iii. Datum
        iv. Nonci
        v. Hash COINBASE transakce
        vi. Adresu příjemce odměny za vytěžení bloku
        vii. Získejte RAW data z COINBASE Data a poté je převeďte na text
        viii. Najděte článek, který je zde zmíněn

c. Najděte první blok, ve kterém se objevila první transakce mimo COINBASE. Uveďte:
    i. Hask bloku
    ii. Hash dané transakce
    iii. Odesílatel a příjemce
    iv. Hodnotu transakce (V BTC + V $ v kurzu v okamžiku transakce + V $ s aktuálním kurzem)
    v. Poplatek za transakci (V BTC + V $ v kurzu v okamžiku transakce + V $ s aktuálním kurzem)
d. Najděte 5 adres, které momentálně drží nejvíce BTC. Napište jejich adresu + aktuální zůstatek + se pokuste najít informace o této adrese.
e. Zjistěte informaci o této adrese:
    13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
    i. Čím je tato adrese zajímavá a na co byla použita?
    ii. bitc
    iii. Na jaké adresy a v jakých transakcích byla většina prostředků odeslána?
    iv. Kam dále tyto prostředky směřovaly? Pokuste se trasovat ty největší převody.
    v. Využijte i některý z nástrojů pro vizualizaci transakcí.
f. Zjistěte jaké transakce se nachází v bloku:
    00000000152340ca42227603908689183edc47355204e7aca59383b0aaac1fd8
    i. Vyberte a popište zajímavost o dané zajimav= transakci, které je v tomto bloku.
    ii. Napište její hash a částku + zjistěte informace o co se jedná.
g. Vyzkoušejte si nástroj https://glasschain.org/ na libovolné transakci nebo adrese.
    i. V čem je tento nástroj zajímavý a co přináší navíc za data proti Exploreru?

Vypracujte tyto otázky:

1) Popište a vysvětlete jak probíhá proces těžby kryptoměn s algoritmem PoW a s algoritmem PoS. Tyto přístupy porovnejte.
2) Jaký je rozdíl mezi BTC a XMR z pohledu anonymity. Popište proč je obtížné skoro až nemožné trasovat XMR (popis, princip, algoritmy).
3) Co je to kryptoměnový mixér, detailně popište jak funguje.

Vypracování

Průzkum GENESIS bloku Bitcoinu

Hash bloku:
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Výška odměny:
50 BTC

Datum:
3.1.2009 19:15:05 SEČ

Nonce:
2 083 236 893

Hash COINBASE transakce:
4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Adresa příjemce odměny za vytěžení bloku:
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

RAW data a text z COINBASE data:

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

Obr. 1 - RAW data z COINBASE data a převedený text

Článek, který je zde zmíněn:

THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1969 levels
Business, page 47

Michael Sheen Frost, Nixon and me
Magazine

Working mums So that's how she does it
Body&Soul

Detox in style The best spas on the planet
Travel

Salman Rushdie I won't marry again
Pages 22, 23

Giant killing? Guide to the FA Cup third round
Sport

Obr. 2 - Článek uvedený v COINBASE transakci GENESIS bloku, který byl publikován v deníku The Times

První blok, ve kterém se objevila první transakce mimo COINBASE

Hash bloku:
00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee

Hash transakce:
f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

Odesílatel:
12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S

Příjemce:
1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3

Hodnota transakce:
50 BTC = $0.00 (12.1.2009 4:30 SEČ) = $841,779.50 (30.11.2022 18:20 SEČ)

Poplatek za transakci:
0 BTC = $0.00 (12.1.2009 4:30 SĚC) = $0.00 (30.11.2022 18:20)

5 adres, které momentálně drží nejvíce BTC

1) 34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo

Zůstatek:
250 597.32717536 BTC (30.11.2022 18:45)

Počet transakcí:
785

Vlastník:
Binance

Typ adresy:
P2SH (BASE58) – SegWit – Pay to Script Hash

2) bc1qgdjqv0av3q56jvd82tkdjpy7gdp9ut8tlqmgrpmv24sq90ecnvqqjwvw97

Zůstatek:
168 009.98775617 BTC (30.11.2022 18:45)

Počet transakcí:
102

Vlastník:
Bitfinex

Typ adresy:
P2WPKH (BECH32) – Native SegWit – Pay to Witness Public Key Hash

3) 1LQoWist8KkaUXSPKZHNvEyfrEkPHzSsCd

Zůstatek:
141 664.89990350 BTC (30.11.2022 18:45)

Počet transakcí:
122

Vlastník:
neznámý

Typ adresy:
P2PKH (BASE58) – Legacy – Pay to Public Key Hash

4) 3JJmF63ifcamPLiAmLgG96RA599yNtY3EQ

Zůstatek:
127 351.05702497 BTC (30.11.2022 18:45)

Počet transakcí:
1

Vlastník:
neznámý

Typ adresy:
P2SH (BASE58) – SegWit – Pay to Script Hash

5) bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h

Zůstatek:
106 606.64824506 BTC (30.11.2022 18:45)

Počet transakcí:
598 192

Vlastník:
Binance

Typ adresy:
P2WPKH (BECH32) – Native SegWit – Pay to Witness Public Key Hash

Informace o adrese: 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

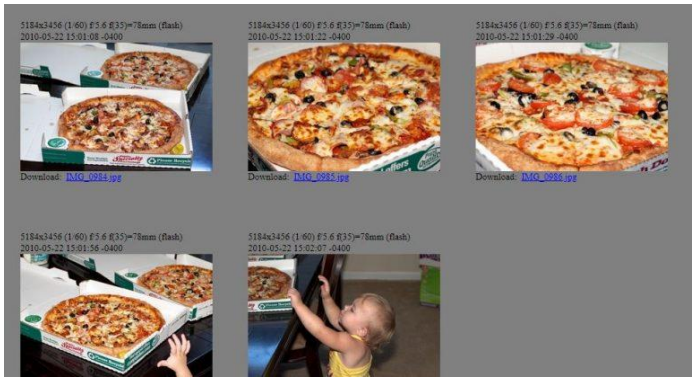
Adresa byla využita k výběru výkupného od obětí napadených ransomwarem WannaCry. Tento ransomware napadl 209 653 zařízení v 99 zemích a cílil na nemocnice, univerzity, dopravní infrastrukturu a bankomaty. Týkal se společností jako FedEx, NHS, Telefonica či Renault.

Tato adresa byla použita v rámci 143 transakcí z čehož většina transakcí byla směřována na velké množství dalších výstupních adres. Z toho lze usuzovat, že byl využit mixér ke skrytí původu prostředků pro cílové adresy. Do 30.11.2022 bylo z celkových přijatých 20.07353352 BTC odesláno celkem 19.74510304 BTC.

Transakce v bloku: 00000000152340ca42227603908689183edc47355204e7aca59383b0aaac1fd8

Tento blok obsahuje kromě COINBASE transakce pouze 1 další transakci. Tato transakce má hash: a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d a bylo pomocí ní odesláno 10 000 BTC mezi programátorem Laszlo Hanyeczem a Jeremym Sturdivantem, kteří se na ní domluvili skrze Internet Relay Chat (IRC).

Na této transakci je zajímavé především to, že se jedná o první zdokumentovaný nákup pomocí Bitcoinu. Kuriozitou této transakce je, že takové množství BTC bylo vyměněno za 2 Papa John's pizzy. V době transakce se jednalo o $41 zatímco nyní by tyto pizzy stály okolo $170,000,000. Do dnes se 22.5. slaví mezi Bitcoinovou komunitou jako Bitcoin Pizza Day.



Obr. 3 - Snímek pizzy, která byla v rámci transakce nakoupena

Zkouška nástroje glasschain.org

Nástroj glasschain.org byl využit pro zjištění informací o

Závěr

1) Popište a vysvětlete, jak probíhá proces těžby kryptoměn s algoritmem PoW a s algoritmem PoS. Tyto přístupy porovnejte.

Algoritmy PoW a PoS se používají k ověřování transakcí, zabezpečení sítě a odměňování jejich ověřovatelů. V rámci PoW (Proof of Work) se ověřují transakce pálením elektrické energie použité při procesu těžení pomocí grafických karet či v dnešní době spíše ASIC minery. Těžení je proces, při kterém se těžař snaží uhodnout nonci, která společně s hashem předchozího bloku a transakcemi bude po zahashování splňovat předem stanovenou složitost. Jakmile některý těžař tuto nonci uhádne, tak jej systém odmění nově „vyraženými“ mincemi dané kryptoměny a společně s poplatky za jednotlivé transakce v bloku jsou pomocí COINBASE transakce odeslány na adresu těžaře. V případě, že je těžař součástí nějakého těžebního poolu, tak se odměny následně rozdělí mezi jednotlivé těžaře v poolu v poměru poskytnutého výpočetního výkonu. Pro zajímavost, první těžební pool na Bitcoinu byl český Slush Pool založený 27.11.2010. Po zapsání bloku do blockchainu celý proces hádání nonce začíná od znovu. Proces odměňování těžařů motivuje k těžení, které zároveň zajišťuje zabezpečení sítě proti útoku dvojí útraty, kterou může provést útočník, který má více než 50% výpočetní síly sítě. Čím vyšší hashrate tedy daná sít má tím nižší je pravděpodobnost tohoto útoku. Útočník by tedy postupem času musel utratit více peněz za elektrickou energii pro zprovoznění dané výpočetní síly, než kolik by byl schopen vydělat na dané dvojí útratě. Zvyšující se složitost těžby pak vede k zvyšující se efektivitě těžebních strojů, a proto se dnes např. již snižuje využití grafických karet, které mají oproti ASIC minerům mnohem menší výkon. Těžba bývá často vyobrazována jako velmi neekologická, což se však díky společenskému tlaku postupně mění. Aby byla totiž těžba profitabilní, tak musí být prováděna na místech, kde je levná elektrická energie. Levná energie je pak dostupná např. u obnovitelných zdrojů energie, jejichž přebytky mohou být využity k těžbě. Dnes je okolo 58% těžby prováděno pomocí udržitelných zdrojů.

Mnohem ekologičtější je však algoritmus PoS (Proof of Stake), který vyžaduje násobně menší množství elektrické energie. Ověřování transakcí se říká validace a provádí ji validátoři. Principy fungování PoS se mezi kryptoměnami mírně liší. Zatímco Ethereum vyžaduje pro stakování uzamčení minimálně 32 ETH a aktuálně neumožňuje výběry (měly by být přidány v některé z budoucích aktualizací sítě), tak Cardano žádný spodní limit nemá a výběry možné jsou. U etheru se validátoři mohou také sdružovat do validačních uzlů (Cardano má stake pooly), které mají vyšší šanci být vybrány k validaci než jednotliví menší validátoři. Náhodně vybraný validátor pak získává nově vyražené kryptoměny včetně transakčních poplatků. Nevýhodou PoS oproti PoW je fakt, že validátor, který má více než 50 % kryptoměnových prostředků, může ovlivnit vývoj dané sítě, což vede k větší centralizaci. U etheru pak také díky minimální výši uzamčené kryptoměny, která je vysoká pro malé validátory (32 ETH = $40,000 30.11.2022), dochází k tomu, že je validátorů mnohem méně než např. u Cardana a lidé, kteří chtějí stakovat, musí své prostředky poskytnout nějakému validačnímu uzlu. Těchto uzlů je pak díky stejnému problému méně a mohou např. cenzurovat nevyhovující transakce. Po přechodu etherea na PoS je pak od této doby na ethereu dle webu https://www.mevwatch.info přibližně 70 % bloků obsahujících cenzuru transakcí.

Kromě PoW a PoS pak existují také méně rozšířenější algoritmy – Proof of Capacity, Proof of Activity, Proof of Elapsed Time, Proof of Importance, Proof of Burn či Proof of Weight.

2) Jaký je rozdíl mezi BTC a XMR z pohledu anonymity. Popište, proč je obtížné skoro až nemožné trasovat XMR (popis, princip, algoritmy).

Bitcoin je pseudoanonymní, jelikož i přestože jeho transakce neobsahují jméno či jiné osobní údaje odesílatelů či příjemců, tak všechny transakce jsou veřejně dostupné. V případě, že je odhalen majitel dané adresy, tak je možné postupně vystopovat síť transakcí, ve které daná adresa figuruje.

Monero (XMR) je kryptoměna, která je označovaná jako privacy coin, jelikož využívá technologie, které vedou k anonymitě transakcí a zachování soukromí uživatelů. Soukromí odesílatele zajišťují **kruhové podpisy**. Odesílatel pomocí podpisu dokazuje, že je schopen utratit určité množství XMR. V rámci kruhu jsou pak smíchány tyto podpisy od několika odesílatelů tak, že není možné jednoduše spojit konkrétní podpis s danou transakcí. Soukromí příjemce pak zajišťují **stealth adresy**, což jsou náhodné jednorázové adresy pro každou transakci vytvořenou odesílatelem. Příjemce tedy zveřejní pouze jednu svoji veřejnou adresu a z této adresy může vytvořit unikátní stealth adresy o kterých bude vědět pouze on a daný odesílatel. Pouze příjemce je pak schopen si pomocí view klíče zobrazit transakce na danou adresu. Důvěrnost transakcí zajišťují kromě kruhových podpisů a stealth adres také **kruhové důvěrné transakce (RingCT)**, které skrývají částky jednotlivých transakcí, které si mohou zobrazit pouze odesílatelé a příjemci. Pro zajištění zvýšené ochrany proti odhalení IP adresy je pak možné využít navíc **síť Tor** či **I2P**, což je však možné i u Bitcoinu.

3) Co je to kryptoměnový mixér, detailně popište, jak funguje.

Kryptoměnový mixér je služba, která přijímá Bitcoiny od několika uživatelů a mixuje je tak, aby nebylo možné dohledat pravého odesílatele k danému příjemci. V rámci mixéru je prováděno spousta transakcí, a nakonec se k příjemci nemusí dostat ty stejné mince, které byly odesílatelem odeslány. **Centralizované mixéry** fungují tak, že odesílatel odešle bitcoiny na konkrétní adresu mixéru a vyplní formulář ve kterém uvede cílovou adresu. Toto řešení je obvykle spojeno s relativně vysokými poplatky, které jsou placeny nejen za jednotlivé transakce, které mixer provádí, ale také dané společnosti, která za daným mixérem stojí. **Decentralizované mixování (CoinJoin)** pak funguje tak, že se použijí vstupy několika uživatelů do jedné velké transakce, což ztěžuje odhalení toho, kdo odeslal prostředky komu.