

# TECHNOLOGIE BLOCKCHAIN A JEJÍ POUŽITÍ K ARBITRÁŽNÍM OBCHODŮM (BLOCKCHAIN TECHNOLOGY AND ITS USE FOR ARBITRATION DEALS)

*Josef Kokeš<sup>1</sup>*

<sup>1</sup> ČVUT Praha, josef.kokes@fs.cvut.cz

*Abstrakt: Cílem této práce bylo zjistit, zda lze reálně napsat automatizovaný systém pro arbitrážní obchody na trhu s kryptoměny. V článku jsou vysvětleny pojmy nutné k pochopení problematiky a fungování technologie blockchain. V další části pak je naznačena funkcionální aplikace a shrnuty základní výsledky.*

*Klíčová slova: peníze, kryptoměna, blockchain, arbitrážní obchod, burzy*

## 1. Úvod

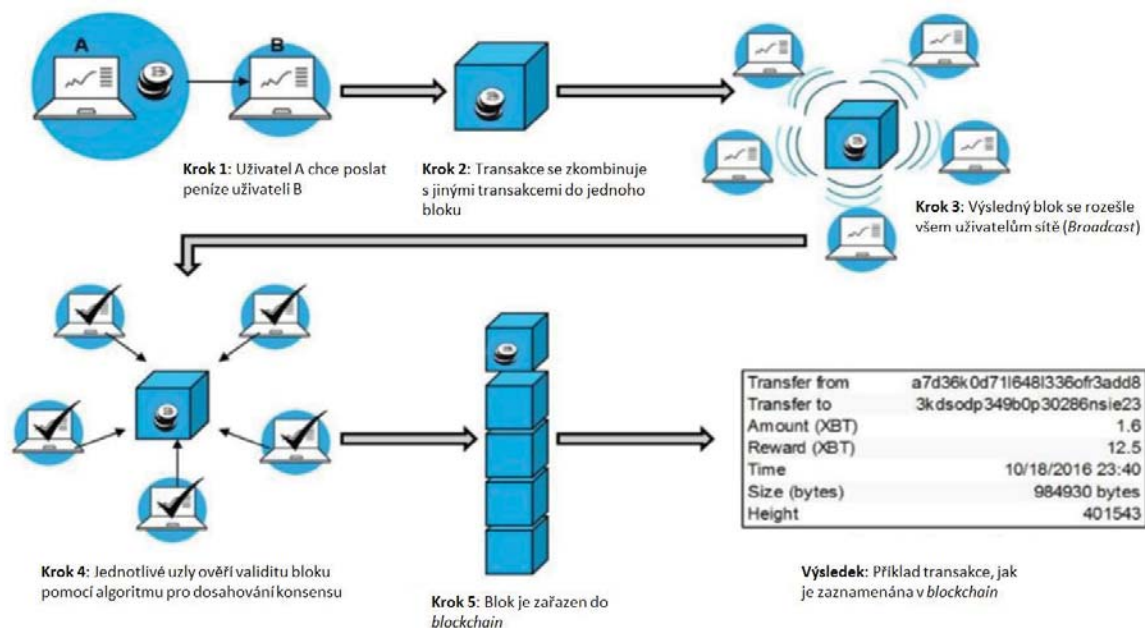
V poslední době je věnována pozornost technologii, zvané *blockchain*, zejména pak možnostem její aplikace na arbitrážní obchody s kryptoměny. Sdílená kontrola a praktická nezkorumpovatelnost této technologie umožňuje více stranám (případně i soupeřícím či nepřátelským) spolupracovat k oboustranné spokojenosti. Toho je využito k realizaci umělých platidel, kryptoměn (*cryptocurrency*).

## 2. Pojem *blockchain*

Označení *blockchain* má z technologického pohledu dva základní významy. Prvním z nich je označení množiny softwarových protokolů, které umožňují realizaci fungování *blockchainu* jako technologické platformy. Druhým významem je pak označení *blockchainové* databáze, nad kterou jednotlivé *blockchain* protokoly operují. Mezi klíčové vlastnosti *blockchainu* patří:

1. Systém funguje bez centralizované důvěry.
2. Všichni znají stav všech ostatních účtů.
3. Transakce jsou schvalovány konsensuálním způsobem, který je reprezentován procesem těžení.
4. Autenticita transakcí je chráněna asymetrickou kryptografií.
5. Za jednotlivé transakce jsou odváděny transakční poplatky.
6. Databáze je distribuována mezi jednotlivé účastníky.
7. Integrita databáze je silně chráněna procesem těžení a řetězením bloků.

Princip *blockchainu* schématicky znázorňuje obrázek 1 na následující stránce.

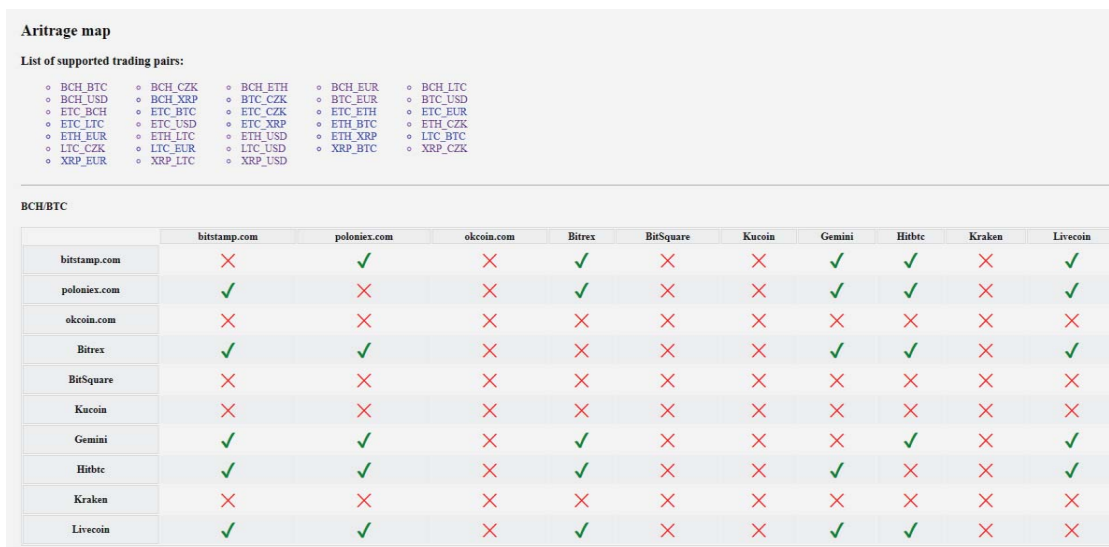
Obrázek 1 Princip technologie *blockchain*

### 3. Kryptoměny

Různých kryptoměn dnes existují desítky. K nejznámějším patří:

- **Bitcoin** se považuje za nejstarší kryptomenu. Bitcoin samotný byl definován v oficiálním dokumentu "white paper", volně dostupném na <https://bitcoin.org/bitcoin.pdf>.
- **Bitcoin Cash (BCH)** vznikla jako hard fork z Bitcoinu. Hard fork je tvrdé rozdělení existující měny na základě různé představy s fungováním měny. Změna spočívala v tom, že těžaři se dožadovali možnosti zpracovávat více transakcí v jednom bloku.
- **Ethereum** můžeme označit jako kryptomenu druhé generace. Jeho idea byla v tom, aby se výpočetní výkon počítačů potřebných pro dosažení konsenzu proof of work využíval efektivněji.
- **Litecoin** je měna podobná bitcoinu. Litecoin na rozdíl od Bitcoinu používá hashovací funkci Scrypt, která patří do kategorie paměťově náročných algoritmů. To znamená, že její algoritmus je paměťově náročný a současně je odolný vůči paralelizaci.
- **Ripple** usiluje o efektivnější převody mezi bankami, firmami a finančními institucemi.

Podobných kryptoměn existuje mnohem víc. Kromě toho, existují desítky decentralizovaných směnár, ve kterých se kryptoměny (všechny, anebo jen některé) průběžně obchodují a směňují navzájem. Na následujícím obrázku jsou příklady některých směnár a měnových párů, které v nich lze obchodovat:

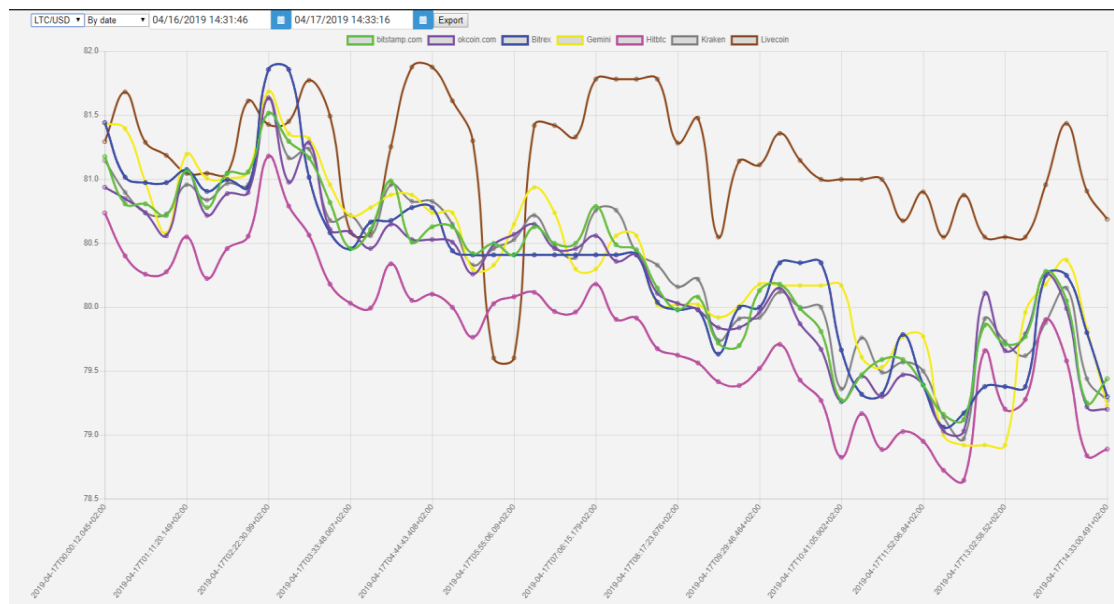


Obrázek 2 Některé směnárny a kryptoměnové páry

#### 4. Arbitrážní obchody

Odtud je už jen krůček k myšlence, porovnat ceny, za které lze různé kryptoměny v různých směnárnách v daném okamžiku zobchodovat, s cílem, dosáhnout zisku. Jedná se tedy o typickou úlohu počítačového řízení, zaměřeného na automatizaci a optimalizaci řídicího procesu. Toto je oblast, které jsme se ve svém výzkumu věnovali.

Tuto myšlenku podporuje ještě jedna okolnost – a sice, že všechny kryptoměny jsou vysoce volatilní, tzn. proměnlivé v čase. Demonstruje to 3.



Obrázek 3 Volatilita LTC proti USD v různých směnárnách

Omezujícím faktorem pro realizaci arbitrážních operací jsou jednak poplatky, jednak doby, za které lze dosáhnout potvrzení transakce. Poplatky se většinou skládají z poplatku pro burzu, který je převážně menší než 1% z transakce a z odměny pro těžaře. Tato odměna je u některých burz fixní, někde je tato

hodnota v určitém rozmezí a uživatel si může vybrat, nebo není vůbec uvedena. Všechny burzy považují transakci za uskutečněnou, až když se blok nachází dostatečně hluboko v *blockchainu*. Na základě množství potvrzení a průměrné doby řešení bloků jednotlivých měn se dopočítává trvání transakce.

Tím je způsobeno, že ne všechny transakce, které se zdají být v čase začátku transakce potenciálně v plusu, musí při zohlednění trvání transakce a měněního se měnového kurzu musí být v plusu i ve skutečnosti. Proto byla provedena počítačová simulace obchodů, při které se zohlednily jednak proměnlivé kurzu jednotlivých měn, jednak skutečná doba transakcí.

## 5. Simulace obchodů

Simulační výpočet byl proveden ex-post, to znamená, že nejprve byla z burz po určitou dobu stahována a ukládána data, načež zpětně byl proveden výpočet podle těchto dat. Výsledky okazuje obrázek 4:

Begin of transaction †	Base currency	Base currency type	Expected result of trans.	Expected profit at beginning of trans.	Duration	Transaction path	Result of trans.	Profit of trans.	Profit of trans converted to [USD]
2019-04-18T05:28:42.1213826+02:00	87.72635226516752	XRP	88.0666344367444	0.34028217157687823	02:40:00	BTC/XRP[Kucoin] ==> XRP/BTC[Livecoin]	87.30083326772923	-0.42551899743829047	-0.14656895487012556
2019-04-18T05:28:42.1213826+02:00	0.09378313894202472	BCH	0.11202076353005963	0.018237624588034906	02:40:00	BTC/BCH[bitstamp.com] ==> BCH/BTC[poloniex.com]	0.11202076353005963	0.018237624588034906	5.821162578020979
2019-04-18T05:28:42.1213826+02:00	0.09378313894202472	BCH	0.108244202312173	0.014461063370148271	03:10:00	BTC/BCH[bitstamp.com] ==> BCH/BTC[hitbtc]	0.10787376439859413	0.014090625456569405	4.497505758644943
2019-04-18T05:28:42.1213826+02:00	0.09378313894202472	BCH	0.11078239926983642	0.016999260327811697	04:50:00	BTC/BCH[Bittrex] ==> BCH/BTC[poloniex.com]	0.11078239926983642	0.016999260327811697	5.415503271931401
2019-04-18T05:28:42.1213826+02:00	0.09378313894202472	BCH	0.10703501673168779	0.01325187778966306	05:20:00	BTC/BCH[Bittrex] ==> BCH/BTC[hitbtc]	0.10869063563098472	0.014907496688959992	4.749124111199601
2019-04-18T05:28:42.1213826+02:00	0.09378313894202472	BCH	0.11117393105218946	0.017390792110164737	03:00:00	BTC/BCH[Cemini] ==> BCH/BTC[poloniex.com]	0.11117393105218946	0.017390792110164737	5.5448287541922445
2019-04-18T05:28:42.1213826+02:00	0.09378313894202472	BCH	0.10741732313435935	0.013634184192334625	03:30:00	BTC/BCH[Cemini] ==> BCH/BTC[hitbtc]	0.10711225450449437	0.013329115562469643	4.249815808880537
2019-04-18T05:28:42.1213826+02:00	0.17384759040037448	ETH	0.17528787041239774	0.001440280012023274	02:04:48	ETH/BTC[bitstamp.com] ==> BTC/ETH[BitSquare]	0.17528787041239774	0.001440280012023274	0.24922823839103986

Obrázek 4 Výsledek arbitrážních příležitostí při zohlednění trvání transakce

Na závěr jsou na následující stránce v obrázku 5 ukázány denní statistiky pro případ, že bychom provedli všechny transakce, které můžeme detekovat a které se zdají být ziskové v čase začátku transakce. Úplně první tabulka poskytuje údaje o celkové denní statistice. V řádku s názvem "*SUM of daily profit*" najdeme celkový součet všech kladných transakcí i se zohledněním délky trvání transakce. "*SUM of daily loss*" nám poskytuje informaci, jaké byly ztráty za tento den, i když v době začátku realizace transakce se zdálo, že tato transakce bude v plusu.

Řádky "*Number of daily profit*" a "*Number of daily loss*" obsahují počty, kolik bylo takových transakcí celkově za den, které byly ziskové případně ztrátové po započtení délky trvání transakce. V dalších tabulkách se nacházejí také denní statistiky, ale tyto nám ukazují, kolik bylo a jak výnosných arbitrážních obchodů pro jednotlivé arbitrážní cesty. Každá jedna z těchto transakcí je uskutečněna v množství ekvivalentním 40 amerických dolarů.

## 6. Závěr

Cílem této práce bylo, navrhnout automatizovaný systém, který by ověřil možnost arbitrážních obchodů na burzách. Byl realizován pokusný program, kterým byla tato možnost úspěšně obchodování na kryptoměnových burzách úspěšně vyzkoušena. Je napsán zatím jako nástroj, který obchoduje v teoretické rovině, tedy neuskutečňuje skutečné obchody se skutečnými penězi.

## Literatura

- [1] LÁNSKÝ, J. Kryptoměny. Praha: C.H. Beck, 2018. 312 s. ISBN 978-80-7400-722-4.
- [2] KALISKÝ, B. Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn. Praha: IFP Publishing, 2018. 106 s. ISBN 978-80-87383-71-1.
- [3] SKALICKÝ, J. -- STROUKAL, D. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Praha: Grada Publishing, 2018. 253 s. ISBN 978-80-271-0742-1.
- [4] HOSP, J. Kryptomeny. Bratislava: TATRAN, 2018. 178 s. ISBN 978-80-222-0945-8.

Total stats for day: 2019-04-28T00:00:00+02:00	
SUM of daily profit	390982.6248769814
SUM of daily loss	-636537.8688404412
Number of daily profit	73596
Number of daily loss	4498

Day stats for paths:	
<b>BTC/ETC[poloniex.com] ==&gt; ETC/BTC[BitSquare]</b>	
SUM of daily profit	14156.240014279047
SUM of daily loss	0
Number of daily profit	1340
Number of daily loss	0

<b>BTC/ETC[Bitrex] ==&gt; ETC/BTC[BitSquare]</b>	
SUM of daily profit	14244.736089759781
SUM of daily loss	0
Number of daily profit	1354
Number of daily loss	0

<b>ETC/BTC[BitSquare] ==&gt; BTC/ETC[Hitbtc]</b>	
SUM of daily profit	316.13610635352427
SUM of daily loss	-7.7661910505113925
Number of daily profit	1013
Number of daily loss	75

<b>ETC/BTC[BitSquare] ==&gt; BTC/ETC[Livecoin]</b>	
SUM of daily profit	7440.764616328014
SUM of daily loss	0
Number of daily profit	1348
Number of daily loss	0

Obrázek 5 Výsledky simulace ex-post



**Selected article from**

**Tento dokument byl publikován ve sborníku**

**Nové metody a postupy v oblasti přístrojové  
techniky, automatického řízení a informatiky 2019  
New Methods and Practices in the Instrumentation,  
Automatic Control and Informatics 2019  
27. 5. – 29. 5. 2019, Zvíkovské Podhradí**

**ISBN 978-80-01-06617-1**

Web page of the original document:

<http://iat.fs.cvut.cz/nmp/2019.pdf>

Obsah čísla/individual articles:

<http://iat.fs.cvut.cz/nmp/2019/>

Ústav přístrojové a řídicí techniky, FS ČVUT v Praze, Technická 4, Praha 6