OST Eastern Switzerland University of Applied Sciences

Blockchain (BICh)

HTLCs, Cross-chain Atomic Swaps

Thomas Bocek 18.11.2021

- A Showcase of Cross-chair Atomic Swaps
 - Either swap happens or becomes void





- Use case: I want to exchange my 1 BTC to 37 ETH
 - Obvious approach: use a centralized exchange, such as Binance, Bitstamp, or Kraken

 English 🧹 Crypto Markets	Continue Trade •	X Earn •											Log In
Binance	Will List COTI (C	OTI) - Deposit COT	I Fast for a	(02-25)	Binance La	unches 50,000 BNB Commur	nity Giveaway (02-21)	Binance V	Will List Commu	inity Coin V	ote Round 6 Winner	· (02-21)	
ETH / BTC		ast Price		24h Change		24h High	24h Low	24h Volum		<u>×</u> (🛧 M BNB	BTC ALTS V	FIAT
Ethereum	0	.026692 \$250.21		-0.001022	-3.69%	0.027772	0.026631	5,524.35	BTC		Q Search	 Change 	O Volume
	droups	6 decimals 🔻	Time m	▼ 1H ▼ 1D	1W 1M			Original Trad	lingView Dept	h 55	Pair 🔺	Price	Change
									Guine Dobe		ADA/BTC	5x 0.00000607	-0.82%
	Amount (ETH)	Total(BTC)					0.027799 >			0.027800		0.00000951	-3.74%
0.0267 50	30.000	0.80250000				é a l	i i i i i i i i i i i i i i i i i i i				AE/BTC	0.00002145	-2.94%
0.0267 49	0.692	0.01851031					·····································			0.027600	☆ AGI/BTC	0.00000254	-6.62%
0.0267 46	0.161	0.00430611			. i i i i i i i i i i i i i i i i i i i						☆ AION/BTC	0.00001321	-8.52%
0.026745	5.082	0.13591809				┶╇┸╋╲┙┷	₽₽₽ ₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽			0.027400	☆ ALGO/BTC	0.00004269	-15.67%
0.026744	7.982	0.21347061	1.1		TT		U U '' TT.				☆ AMB/BTC	0.00000189	-9.13%
0.0267 39 0.0267 36	85.500	2.28618450							NT ++-	0.027200	☆ ANKR/BTC	0.00000021	-4.55%
0.026735	13.679 78.000	0.36572174		₩				' II.			☆ APPC/BTC	0.00000430	-8.12%
0.026735	1.951	2.08533000 0.05215803								0.027000	☆ ARDR/BTC	0.00000580	-4.92%
0.026733	7.488	0.20017670						!'	· · · ·		☆ ARK/BTC	0.00002161	-10.74%
0.0267 27	0.403	0.20017870						· · · · · · · · · · · · · · · · · · ·	Ti	-0.026800	☆ ARN/BTC	0.00001497	-5.61%
0.026726	6.060	0.16195956							1	0.026692	☆ ARPA/BTC	0.00000121	-9.02%
0.026721	8.116	0.21686764							0.026631 >	-25324.21	☆ AST/BTC	0.00000227	-10.28%
0.026720	2.007	0.05362704								-25324.21	🟠 ATOM/BTC (50 0.0004356	-9.34%
0.026719	0.497	0.01327934								11454.15	∧ RAND/RTC	0 00003388	-12 2/%
0.026718	0.297	0.00793525	an a		- Later H	alalaa ahalala				11454.15	Trade History		
0.026717	0.393	0.01049978									0.026692	3.581	17:42:10
0.026708	0.149	0.00397949									0.026703	0.449	17:42:09
0.026707	0.171	0.00456690	P					TAXABLE PARTY	[[]	-0.000000	0.026703	1.923	17:42:09
											0.026704	3.986	17:42:09
0.026692		More III	16:00	2/23	8:00	16:00 2/24	8:00 16:00	2/25 8:0	0 16:00	5	0.026705 0.026704	0.496	17:42:09
0.026702	2.000	0.05340400							-			0.014 2.000	17:42:08 17:42:06
0.0267 01	2.466	0.06584467	Exchang	e Margin					Tra	ding Rules	0.026709	0.768	17:42:08
0.0267 00	26.000	0.69420000	Limite	Market							0.026704	3.761	17:42:04
0.026699	4.000	0.10679600	Limit	Market	Stop-limit 🕜	·					0.026701	0.344	17:42:03
0.026691	0.024	0.00064058									0.026700	2.446	17:42:03

- There was also Mt.Gox and BTC-e
 - You loose control over your funds (Mt. Gox)

Available for ev	rt The Guar veryone, funded by reade Subscribe ->			Search jobs	esign in Q search ~ T		
News	Opinion	Sport	Culture	Lifestyle	More~		
	ironment Science Cloba	-		24 			

World UK Environment Science Global development Football Tech Business Obituarie

Bitcoin

• This article is more than 5 years old

MtGox files for bankruptcy in Japan after collapse of bitcoin exchange

The bitcoin exchange has debts of £38m and assets of just £22.6m, it reported on Friday



▲ MtGox CEO Mark Karpeles bows in apology at a press conference at the Justice Ministry in Tokyo Friday night, Feb. 28, 2014. Photograph: I/AP

MtGox filed for bankruptcy protection in Tokyo on Friday, with the world's former biggest bitcoin exchange blaming "a weakness in our system" for its collapse.

ARCHIVE Published: January 17, 2019 12:21 PM UTC

Please Do Not Store Crypto on Any Exchange, Warns CEO of Major Crypto Exchange Kraken

Jesse Powell, the CEO of a major crypto exchange Kraken, warned users of digital assets to not store funds on trading platforms. The warning of Powell follows a high profile security breach suffered by Cryptopia, a New Zealand-based crypto exchange known for its listing of...

Author: Joseph Young @iamjosephyoung



Kraken CEO Jesse Powell listens to the people, delists Bitcoin SV | Source: World Government Summit/YouTube

Save

bunc

DON'T MISS:

Crypto Trading Is the New Wall Street: Kraken Pro Trader

Winklevoss Twins Foster Mainstream Adoption with Bitcoin Giveaway

Crypto Mom Bemoans 'Regulatory Escape Room' Feel for Crypto

Gemini Exchange Expands into Windy City to Capture Institutional Wave

New York Kraken Ex-Employee Sues Crypto Exchange Over Failure to Pay \$900,000



Why the feds took d

Tracing Mt. Gox's stolen coins led feds to

By Russell Brandom and Sarah Jeong | Jul 29, 2017, 10:00am E

SHARE

Illustration by Alex Castro / The Verge

largest exchanges

This week, one of Bitcoin's largest and most notorious coin exchanges was brought down by law enforcement — and police and prosecutors are now beginning to explain why. On Thursday, the Department of Justice unsealed an indictment against Alexander Vinnik — thought to be the operator, or one of the operators of Bitcoin exchange BTC-e — charging

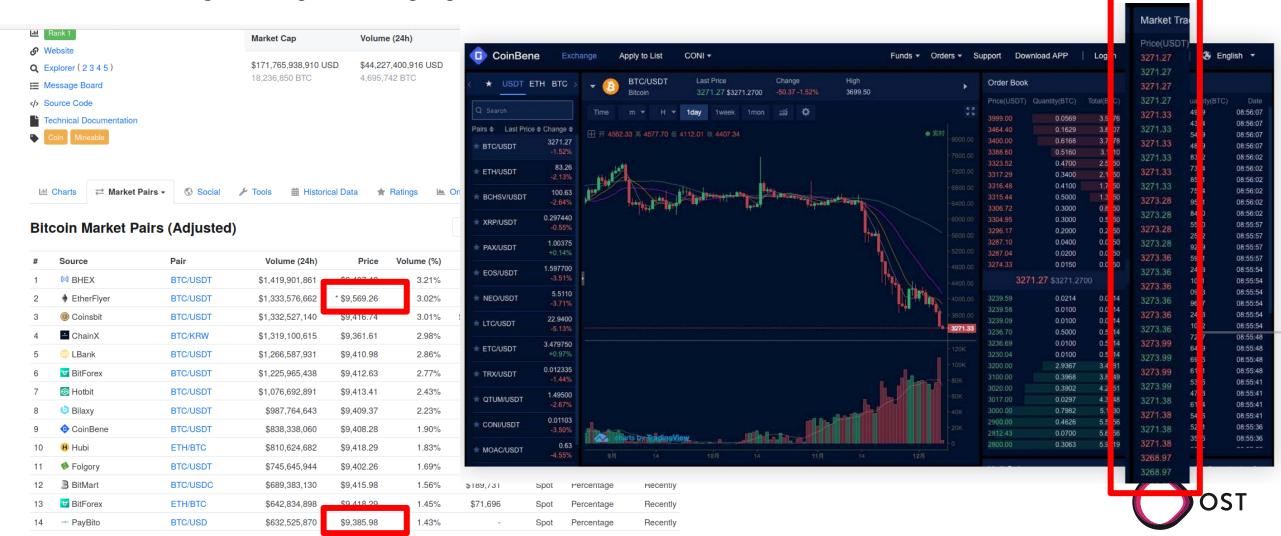
Mt. Gox

- Mt. Gox (short for Magic: The Gathering Online Exchange)
 - July 2010 reused domain name, started Bitcoin trading platform
- April 2013, handled 70% of Bitcoin trades
- November 2013, users reported payout delays
 - Exchange rates different from other trading platforms
- 7. February 2014, suspended all BT withdrawals
 - "Bug in the Bitcoin system": transaction malleability
- 20. February, suspended all withdrawals

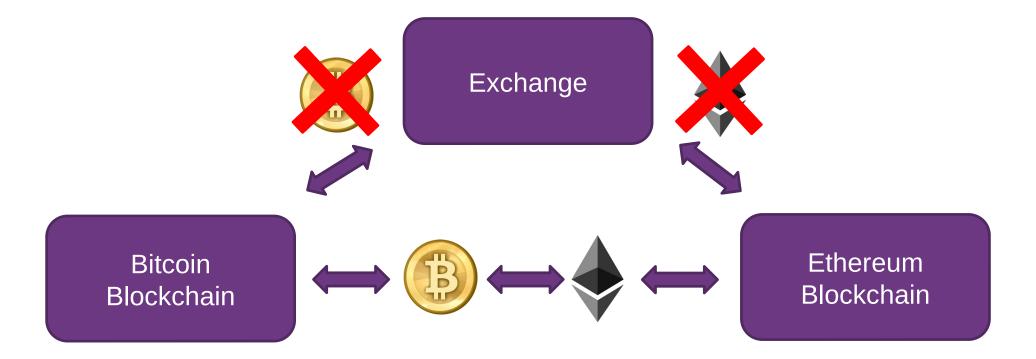
- 24. February, all trading suspended, blank page
- 9. March 2014, filed for bankruptcy
 - 850k Bitcoins missing
- 16.11.2021: Mt. Gox rehabilitation plan is now 'final and binding' [link]
 - Compensate creditors, \$460 million at the time, repaying 150k BTC (from lost 850k BTC)



• Exchanges caught trading against their customers - to boost their numbers



• With Atomic Swaps no trust in a centralized platform is needed





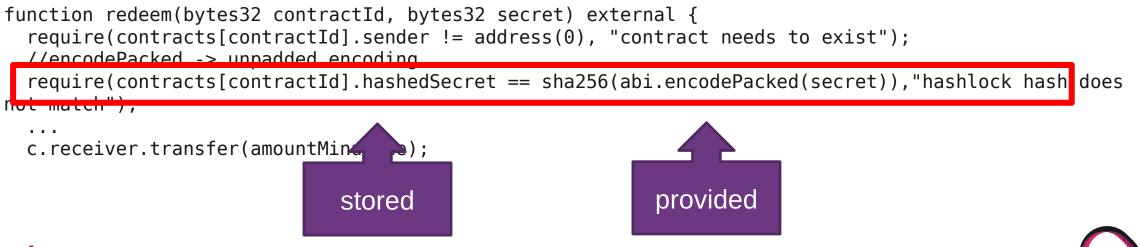
- Building Blocks of Cross-chain Atomic Swaps
- Cryptographic hashing:
 - one-way function computationally efficient in one way, computationally highly expensive the other way
 - deterministic same input same output
 - collision resistant highly expensive to find two inputs that hash to the same output

SHA256 Hash

Data:	aceuaceuac
Hash:	8698bce64d5c921046ce61e7fd0f538ad44c8f5a44e0b7789daf660d653544d8



- Building block for cross-chain atomic swaps and payment channels
- Hash lock:
 - store hashed secret publicly stored in a smart contract
 - unlock only if secret is provided (publicly)



- Building block for cross-chain atomic swaps and payment channels
- Hash time lock:
 - store hashed secret publicly stored in a smart contract
 - unlock only if secret is provided (publicly) before timeout

Or

• unlock – after timeout

function recover(bytes32 contractId) external {

require(contracts[contractId].lockTime <= now, "refundable: timelock not yet passed");</pre>

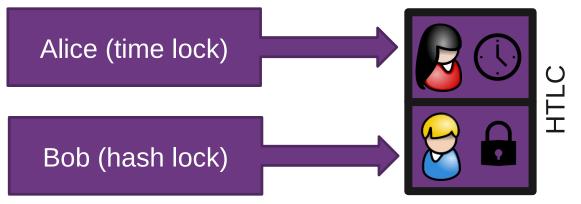
c.sender.transfer(c.amount);

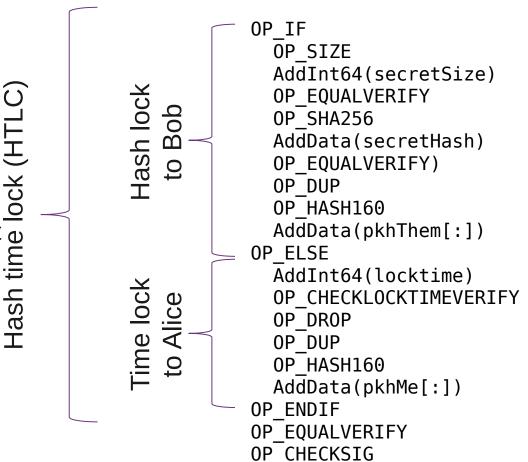


- Building block for cross-chain atomic swaps and payment ch.
- Hash time lock:
 - store hashed secret publicly stored in a smart contract ٠
 - store hashed secret publicly stored in a smart contract unlock only if secret is provided (publicly) before timeout unlock after timeout ٠

Or

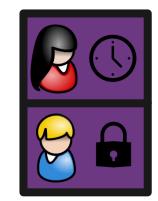
٠







- Now we are ready to do an atomic swap with Alice and Bob
 - 1 BTC for 37 ETH





Atomic Swaps

- Now we are ready to do an atomic swap with Alice and Bob with HTLC
 - Alice (initiator) creates "secret", shares with Bob, hash(secret)

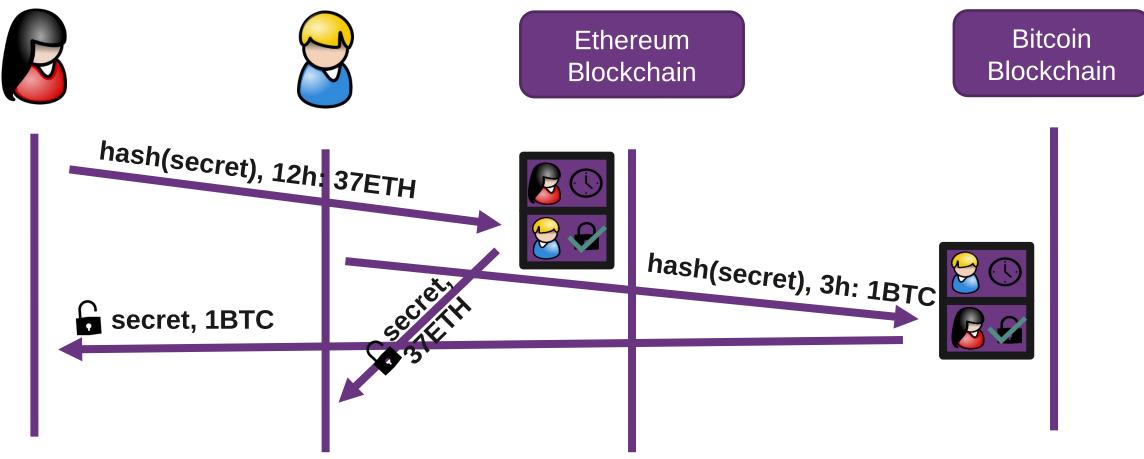


Blockchain BTC

Blockchain ETH



Atomic Swaps - Alice reveals secret to redeem 1 BTC





Atomic Swaps - Bob goes offline (worst case)

