Atomic Swaps, Early Pioneers, and Komodo

A More Specific History

Abstract: This document is intended for researchers, analysts, and other interested parties wishing to discover more about the history of atomic swaps. The following research and commentary is assembled by members of the Komodo team. The commentary is intended to be an informative launching point into one’s own research and commentary.

A Brief Description of DEX's and Atomic Swaps

For readers who are familiar with the concepts of blockchain, decentralized exchanges, and atomic swaps, the material on this page is not necessary to read. Instead, skip forward to the next main section.

Komodo Whitepaper Part I: A Primer for Blockchain Technology

If the reader is generally not familiar with blockchain technology, **Part I** of the Komodo Whitepaper is a ~30 page description of what blockchain technology is and why it is worthy of industrial attention.

Link to Komodo Whitepaper Here

Simple Explanation of Atomic Swaps and DEX Software

For readers who are already familiar with the concept of a blockchain, but are less familiar with decentralized exchanges (DEX's) and atomic swaps, Komodo has several resources available.

For a quick explanation, complete with a list of the step-by-step process of an atomic swap, read the following blog post on the Komodo website:

Link 1

For another quick discussion, the following yet-to-be-published Komodo DEX API documentation discusses the problems that DEX and atomic-swap technology solve:

Link 2

For a complete and thorough discussion on the nature of atomic swaps and the need for DEX technology, read **Part III** of the Komodo Whitepaper:

Link 3

A Timeline of Atomic Swaps

The procurement of today's modern atomic-swap protocols cannot be attributed to just one person, nor to one single moment. Many people placed ideas on public forums, recruited feedback, tested concepts, and challenged each other's ideas.

Thankfully, because a large portion of this endeavor was conducted using extant online forums and code repositories, one can trace the general thread of innovation with sufficient accuracy. The most popular online discussion hub during the incubation period was BitcoinTalk.org. This old-fashioned website features useful timestamps and user-profile overviews that allow the researcher to browse complete histories of user postings in an organized fashion. Also, the popular code repository, Github.com, features timestamps and other useful indications to display when specific collections of code and commentary were made available.

Sergio Damien Lerner: The First Known Proposer of an Atomic Swap

The first known online post regarding what we now call an "atomic swap" was made by one, Sergio Damien Lerner. He posted the idea to BitcoinTalk.org (BTT):

> *I want to describe a new P2P protocol I´m implementing for an alternate cryptocoin as a proof of concept.*
>
> *The protocol allows cross-coin p2p trading without a central point. It seems to me that it is the "holly grail" of alternate crypto coins. And this is an idea that can change the cryptocoin ecosystem for good, where all coins trade against each other. The benefit for alternate chains is enormous: they don´t need to provide an exchange site, they can trade automatically against Bitcoin. It also means that alternate cryptocoins will rely on Bitcoin and will support Bitcoin because they need it to enter the cryptocurrency game.*
>
> *This is short explanation:*
>
> *Suppose that there are two crypto-coins, XC and BTC. Each coin XC and BTC has its own blockchain and client. The user A has some XC and want to buy some BTC in return. User B wants the opposite. First both parties find each other (in a central directory or by a P2P protocol) and fix the trade price (A pays "a" XC and B pays "b" BTC back). There are two payments A->B (in XC) and B->A (in BTC). We well call these payments first and second payment, respectively. Both users have an address in the XC system and an address in the Bitcoin system.*
>
> *The protocol works as follows:*

1. User A commits to the first payment of "a" XC to the address of user B in the system XC. This is a special payment with a "contract" that is automatically allowed if a certain "proof" is published as a special transaction in a limited interval after the publication.

2. User B sends b BTC to A via Bitcoin in a standard way. This is the second payment.

The contract specifies that a piece of the Bitcoin blockchain (a branch) should be copied into a special transaction called "proof" into the XC blockchain to prove the second payment has actually taken place.

The contract also specifies:

- *The chain branch size (N). This is how much effort in terms of confirmations (PoW) must be added after the block where the second payment is published.*
- *The hash of the block where the branch should start (root block). The root block should be chosen to be some blocks in the past to avoid choosing a block that will be discarded by a competing branch. For example, if current block is BLK and the previous block of BLK is Prev(BLK), parties can choose a root in Prev^3(BLK) with a length of at least 9 blocks (6 confirmations after current block)*
- *The maximum number of blocks after the root block where the second payment can appear. This is to prevent the payment being done just after the XC contract interval has expired, thus making the trade one-way only.*

3. When the proof transaction (that matches the contract) is published in an XC block, clients automatically accept the first payment (that specifies the contract), thus paying "a" XC from A to B.

[...omitted for brevity…]

I have a proof of concept of this protocol working. I will release the code when it's ready. The system is implemented in a way to understand contracts for all other alternate currencies and unknown ones. The user specifies a "template" for the second payment message, with placeholders for the fields that are unknown (the transaction signature) and fixed values for the remaining fields (amount of money, public key of recipient,etc.). And also a template for the block format (field of linkage, hash algorithm, etc.).

Best regards,

Sergio.

PS: I named the protocol P2PTradeX, because there was no result when I googled that word.

Click Here for a Link to the Full Discussion

Sergio states in his announcement that he has a proof of concept for this atomic swap working. He does not post a link to this code, however, and at this time we have not yet reached out to him for comment and proofs.

His sparse description does not allow us to ascertain his code's reliability. From what little he does say, he did not try to implement this directly on Bitcoin at the time, due to several technical difficulties, including Bitcoin's "timelock" and "prevouts" aspects. Rather, Sergio created a separate type of blockchain coin that allowed for transactions to be refunded if certain conditions were not met.

Setting aside the issue of using the Bitcoin blockchain, Sergio's attempts at conducting an atomic swap were likely among the earliest attempts, if not the earliest, regardless of their rate of success and reliability.

The discussion thread started by Sergio received little interest from the community and was sporadically active for a period of about one year. Perhaps the community simply did not yet see the value of the idea.

One of the last comments given on Sergio's original BitcoinTalk discussion is by user @ripper234. This comment was made on May 21, 2013, a full year after the thread's inception. @ripper234 informs us that he collected both Sergio's proposal and the proposal of Tier Nolan (featured in the next section) to create a new page on the Bitcoin Wiki:

Link to Bitcoin Wiki: Atomic Swaps

A view of this Bitcoin Wiki page's historical timestamps confirm that this is the birth of this Bitcoin Wiki page.

@ripper234 also states on Sergio's discussion thread that the idea of an atomic swap is merely a proposal at this time (2013) and that no one has yet released a working prototype for Bitcoin.

This Bitcoin wiki link would later be the resource that would inspire Komodo's own lead developer, JL777, to conduct his first atomic-swap proofs of concept in 2014.

Another user from this thread to mention is @XertroV. This user states towards the end of the discussion, on June 21, 2013, that they too were working to create a decentralized exchange that is compatible with atomic swaps. Their thesis and code proofs are provided here:

Link to XertroV's MarketCoin

Like Sergio's own early attempts, XertroV's early proofs were not met with proactive response from the community, and XertroV's interest in the project would appear to be abandoned sometime in 2014.

Sergio Damien Lerner's interest in atomic swaps appears to be limited after his initial thread. He seems to have turned to conducting security audits, and also to his work with the RSK blockchain, which he is still supporting. He is available for questions at the following user profiles:

Link to Sergio's BTT Profile

Link to Sergio's Twitter Profile

Tier Nolan: The Champion of Atomic Swaps

In April 2013, users were beginning to realize that blockchain technology had true value, and that governments would soon want to be proactive in this space. This drove the conversation on BitcoinTalk.org to the concept of a DEX, and posts were made daily with new ideas about how a proper decentralized exchange could and should work.

A tech-savvy user by the name of @TierNolan gained interest in the topic at this time, and one month later posted the famed solution, the atomic swap.

Link to Tier Nolan's Original Proposal

After feedback from user @iddo, who provided a (now defunct) link to user @gmaxwell's discussion of Bitcoin "locktime" feature, Tier was able to create the basic outline for atomic swaps, which is remarkably similar to the way they are used today (including in Komodo's own atomic-swap DEX technology).

> *A picks a random number x*
>
> *A creates TX1: "Pay w BTC to <B's public key> if (x for H(x) known and signed by B) or (signed by A & B)"*
>
> *A creates TX2: "Pay w BTC from TX1 to <A's public key>, locked 48 hours in the future, signed by A"*
>
> *A sends TX2 to B*
>
> *B signs TX2 and returns to A*
>
> *1) A submits TX1 to the network*
>
> *B creates TX3: "Pay v alt-coins to <A-public-key> if (x for H(x) known and signed by A) or (signed by A & B)"*
>
> *B creates TX4: "Pay v alt-coins from TX3 to <B's public key>, locked 24 hours in the future, signed by B"*

B sends TX4 to A

A signs TX4 and sends back to B

2) B submits TX3 to the network

3) A spends TX3 giving x

4) B spends TX1 using x

This is atomic (with timeout). If the process is halted, it can be reversed no matter when it is stopped.

Before 1: Nothing public has been broadcast, so nothing happens

Between 1 & 2: A can use refund transaction after 48 hours to get his money back

Between 2 & 3: B can get refund after 24 hours. A has 24 more hours to get his refund

After 3: Transaction is completed by 2

- A must spend his new coin within 24 hours or B can claim the refund and keep his coins

- B must spend his new coin within 48 hours or A can claim the refund and keep his coins

For safety, both should complete the process with lots of time until the deadlines.

Today, the formula can now be described more simply, but the concept is the same. The following is an excerpt from Komodo's own content, provided for clarification purposes:

Step 0

Bob posts a trade order on the DEX. This is listed as Step 0 because, technically, it's not part of the atomic swap process. However, it must take place before the atomic swap can begin.

Step 1

Alice sees Bob's offer and accepts it. She commits to the trade by paying the atomic swap fee, which is only 0.15% of the total trade amount. The purpose of the atomic swap fee is to make sure Alice, and all other users, don't spam the network with rapid requests. Note that Bob does not have to pay any transaction fees for the trade.

Also, note that this transaction fee must be a separate UTXO from the one Alice will swap with Bob. If you'd like to learn more, read Komodo's guide to UTXOs here.

Once Alice has paid the fee, the atomic swap has officially begun.

Step 2

Bob sends a deposit of funds to a secure address. The decentralized nature of atomic swaps guarantees that no one— neither Bob, nor Alice, nor any third-party administrators— has access to these funds until the trade times out or has been completed.

Bob's deposit must be 112% of the amount of the order that he originally posted. If Bob is an honest actor, this is not a concern because those funds will be returned to him. Whether the atomic swap fails or whether the atomic swap is complete, Bob's deposit will be returned. The deposit simply removes any incentives to cheat.

As with Alice's transaction fee, Bob's deposit must be a separate UTXO from the one that he intends to swap with Alice.

Step 3

Alice then sends her KMD to a second secure address. Just as before, nobody— not Bob, not Alice, not even Komodo Platform admin— have the ability to touch these funds until the swap ends.

If, for any reason, the trade fails at this point, then the atomic swap would be timed out and get canceled. At that point, Bob's BTC deposit would be released back to him and Alice's KMD would be returned to her, too.

Step 4

Bob sends his BTC payment to Alice, finishing his part of the deal. Recall that this sum of BTC is a separate from and additional to the deposit of BTC paid in Step 2. Only Alice is able to claim Bob's BTC payment.

Step 5

Alice now accepts Bob's BTC payment. Once Alice has claimed Bob's BTC payment, Bob gains the ability to claim Alice's KMD payment.

Step 6

Bob accepts Alice's KMD payment. At this point, both parties have obtained the funds they were hoping to trade for. The atomic swap is a success. Hooray!

Step 7

> *Now that both parties have exchanged funds, Bob is allowed to reclaim his deposit of BTC. At this point, the atomic swap process is complete.*
>
> *That's all there is to it! This process is designed to incentivize each party to continue on to the next step of the trade. It is also an atomic process, which literally means that either: (a) the swap occurs exactly as Bob and Alice agreed, or (b) nothing takes place and both Bob's and Alice's funds are returned to them (except the atomic swap fee).*

As mentioned earlier, user @ripper234 now took stock of the information regarding this concept and posted it to the Bitcoin Wiki, as it was clearly a brilliant idea.

On August 2, 2013, Nolan states that he would like to prove the method his invented, and this is probably the beginning of the community's earnest attempts to conduct atomic swaps using Bitcoin-based blockchains.

While Nolan was experimenting with atomic swaps, user @socrates1024 took the concepts put forth by both Tier Nolan and Sergio Damien Lerner and optimized them on the Bitcoin Wiki page for contracts.

Sergio Damien Lerner appears in the discussion thread at this time (October 2013) and states that he can see no drawback to the optimized version, as put forth by @socrates1024.

On February 13, 2014, when asked if there was any progress, Nolan states that one challenge in particular is forestalling positive results. This challenge was known as the "Transaction Malleability" issue. In short, at this time the Bitcoin protocol allowed for a transaction to change between the time it was submitted to the mempool and the time it was included in a block. This would allow an attack vector for a malicious user. Therefore, while "dummy" atomic swaps could be performed on the BTC chain, they were otherwise useless for industry-related purposes.

In March 2014, @k99 proposed a concept that would alleviate some of the issue and Tier Nolan thought favorably of the idea.

> *I created a thread about a similar method. You method is simpler.*
>
> > *Quote from: k99 on March 22, 2014, 03:11:37 AM*
> >
> > *I think the extortion problem due malleability could be solved in the way that Bob pays in a deposit so there is a balanced risk situation.*
> >
> > *So both pay in the same amount, Alice payment move over to Bob and he gets his deposit back after the trade:*
> >
> > *Tx1:*

input 1: x BTC from Alice

input 2: x BTC from Bob

output:

if clause: MultiSig <Alice, Bob>

else clause: 2x BTC to Bobs address and redeemer needs to solve H(x)

<snip>

Tx1 is first signed by Bob then sent to Alice and then she signs her input.

Alice selects a transaction output of value x that she owns as input 1 and sends it to Bob.

Bob creates the transaction, as above, signs it and sends it back to Alice.

Alice signs the transaction and gets it hash.

Alice creates the refund transaction.

Input

2x from TX1 signed by Alice, locked 24 hours in the future

Output

x to Bob

x to Alice

Bob signs and sends it back to Alice.

Alice now has a refund transaction.

She is then supposed to publish TX1.

If Alice stops here, then she can hold Bob's money to ransom.

Worst case, she gets her money back after 24 hours.

OTOH, her hand is weakened, since her x BTC is tied up in the process.

> *Quote*
>
> *The fact that Alice is the redeemer who reveals the secret and therefore control if the trade will executed or be canceled (refund), might need additional protection (offer fees, reputation system?).*
>
> *Automated trades with micropayments might be another option (break down a bigger volume to smaller chunks).*

This might be a general solution, especially with malleability. If you have traded with someone before, you are willing to trust them for up to 1% of the trade or 1% of the total trades that you have done with that person before.

The concept proposed by @k99 allowed for an increased measure of security. If Alice and Bob could establish trust outside of the blockchain, then it would be possible from that point forward to have a certain amount of trust built-in to future trades. While this was a helpful and encouraging solution, it did not yet meet the full requirements for an atomic-swap based DEX.

Following this discussion, Nolan came to the conclusion that new features would be required in Bitcoin for atomic swaps to become a viable and consistent feature. He assembled a formal "Bitcoin Improvement Proposal" (BIP), and submitted it here:

Link to Nolan's BIP

At the heart of the BIP is the simple idea that the Bitcoin protocol should include a method to lock funds for a given amount of time and execute rudimentary scripts on their behalf when certain rules and conditions are met. As the script would be able to verify that the transaction that was sent to the mempool was the same transaction that was included in the block, this would remove the aforementioned attack vector.

While this specific BIP was not accepted into the Bitcoin protocol, it did provide useful conversation and thought provoking material for another BIP that was pioneered by many Bitcoin aficionados: OP_CHECKLOCKTIMEVERIFY (CLTV)

Link to OP_CHECKLOCKTIMEVERIFY BIP

The list of contributors in the CLTV BIP is impressive, including Peter Todd, @Luke-Jr, and many other early pioneers in blockchain technology.

For this BIP to be included in the Bitcoin protocol, it would require a hardfork, wherein the majority of the Bitcoin-miner community would support a change in the code at a set time. Before proceeding to this final stage of the inception of secure atomic swaps, we first turn to Komodo's own atomic-swap endeavors.

JL777: Pioneer of Downloadable Atomic-Swap DEX Software

Komodo claims that of the early pioneers in atomic-swap technology, Komodo's lead developer, James Lee (JL777 or James), deserves to be mentioned due to his relentless and successful efforts to bring atomic-swap technology to the common user. His blockchain efforts began in 2013; his atomic-swap efforts began in 2014; he performed his first insecure cross-chain atomic swap in 2015; he performed his first secure atomic swap upon the release of the CLTV BIP in early 2016; he created fully automated atomic-swap software in late 2016; between August 2017 and early 2018, his software uniquely led to over 120,000 atomic swaps performed by hundreds of anonymous users on the open Internet. Most of these users were non-technically trained, and only followed step-by-step instructions along with downloadable executable files. Komodo is not aware of any other atomic-swap pioneer that can claim a similar feat.

In late 2013, James was making his first experiments with blockchain technology. Little is known about James at this time, as he prefers to keep his anonymity for security reasons. The basic information that he provides the public is that he arrived in the blockchain industry with approximately twenty years of experience in the C programming language, with an emphasis on coding for core-level Graphics Processing Units (GPUs) and on coding for the finance sector. His initial interests were primarily speculative and revolved around NXT and XRP, and involved

gateway services. However, by January of 2014 his interests shifted to blockchain-based software development, and by February 2014 he was pioneering DEX technology.

In April of 2014, James felt prepared to publicly announce his first decentralized exchange (DEX), which he called, InstantDEX. At this time, the idea of a DEX was still revolutionary. The initial frenzy that spurred Nolan's creation of the atomic-swap theory was exciting, but as yet unrealized. Likewise, XertroV's attempts had also not yet proved viable to the community, and did not clearly articulate their relationships to atomic swaps.

It deserves to be mentioned that while the name "InstantDEX" is no longer active, much of the code that JL777 authored to power InstantDEX is still active in Komodo technology to this day, making Komodo's DEX technology among the oldest of DEX initiatives. For example, the popular extant DEX, BitShares, would begin construction later in the year. Another popular DEX, EtherDelta, appears not to have begun construction until sometime in 2016. One of the few extant DEX's that was in production at the same time as InstantDEX is Bisq, as shown on their Github repository.

The original goal for InstantDEX was to create a decentralized gateway that would allow for on-chain trading of tokenized digital assets. For an in-depth discussion, the reader may turn to this material regarding DEX technology and review the section on decentralized gateways. This model was a commonly proposed solution at the time, and it is now made familiar by the aforementioned BitShares project.

While James was building the beta version of InstantDEX he encountered the "Atomic Swap" Bitcoin Wiki page collected by @ripper234, and thereafter discovered Tier Nolan's original proposal via Google. In April 2014, James announced his intentions to perform a modified version of an atomic swap, purely between NXT assets. (NXT assets are similar to the ERC20 colored tokens of Ethereum.)

James understood at this time that core blockchain technology was not sufficiently mature for pure cross-chain atomic swaps. His goal here was to include a demonstration of atomic-swap capabilities as a proof of concept. The endeavor lasted several days, during which time several anonymous users on the Internet were able to perform automated on-chain atomic swaps, as reported in the same NXT Forum discussion linked above.

The code for this public atomic-swap endeavor is found in this repository. The commits dated between April and May 2014 should prove fruitful for any reader that wishes to verify these claims for themselves.

This was the beginning of James's interest in bringing atomic-swap technology to the masses, but it was certainly not the climax.

James finished the beta version of InstantDEX in June of 2014. From this point forward, James focused on making interoperable blockchain technology available to the common user. His many endeavors during this time period are beyond the scope of this discussion; in summary,

he sought to create a network of blockchains that worked together, rather than relying on a single blockchain. He again declared his intention to connect blockchains using atomic-swap technology in September of 2014, and as a part of his larger initiatives.

On September 6, 2014, James reached the infamous “Transaction Malleability” problem that plagued Nolan and other user’s attempts. With the exception of the “timelock” necessities, he was able to conduct a cross-chain atomic swap between NXT and BTC. Like other pioneers, this solution was only useful for “dummy” atomic swaps, and would not withstand public pressure.

Tier Nolan responded on James’s discussion thread with the following clarifications:

> *There is also a plan to introduce a new OP_CHECKSIG (and VERIFY) opcode. One of its properties is that it will replace all the txids in a transaction to the n-txids that would have been used if n-txids had been used since block 0.*
>
> *This closes the malleability problem, since everything else is signed by the creator of the transaction.*
>
> *OP_CHECKLOCKTIMEVERIFY will solve the problem too. It also removes the need for refund transactions to create the timelocking.*

And later:

> *OP_CHECKLOCKTIMEVERIFY is intended "soon". The plan was for deployment to happen immediately after the last soft fork.*
>
> *The block size debate has slowed deployment.*

As is clear from this and many other discussions, there was a multitude of Bitcoin enthusiasts at this time that had reached the same testing levels as JL777 in conducting atomic swaps.

Without the CLTV feature, all atomic-swap progress on BTC-based blockchains was purely theoretical. Like many other early pioneers, James continued developing his atomic-swap technology while waiting for the CLTV to be released.

The Long-Awaited Feature is Released: OP_CHECKLOCKTIMEVERIFY

In November of 2015, the long awaited feature, “OP_CHECKLOCKTIMEVERIFY”, was finally included in the update to the Bitcoin protocol, and there was much rejoicing among atomic-swap enthusiasts. User @spartacus posted this linked thread, which was filled with a “Who’s Who” of early pioneers. Of note is user, @CIYAM, who also built his own atomic-swap DEX software while waiting for this feature to be released.

At this point, one must imagine a flood of technically proficient blockchain engineers seeking to be “the first” to use the CLTV feature to perform a secure cross-chain atomic swap. It is not

possible for Komodo to ascertain who was officially “first” without those who performed the swaps coming forward with their transaction histories. Perhaps, at some future date, these early enthusiasts will bring their evidence to the discussion.

For James, his attention at the time was on large-scale user adoption. He was battling ideological differences with the core NXT developers and had come to the conclusion that in order to achieve his goals, the users of his software would require independence from any particular blockchain. James announced his “Declaration of Independence” and the Komodo project in February of 2016.

While this was ongoing, Tier Nolan, JL777, CIYAM, and several other atomic-swap enthusiasts worked together to problem solve the integration of BTC-fork based alt-coins into the atomic swap process. This marked the beginning of bringing a modern, secure, automated version of an atomic swap to the masses. Their conversation begins in this thread and continues in this thread. JL777 relied on Tier Nolan’s generous support and experience, and also on the support of @TPTB_need_war and other users, as they worked together to clarify and elucidate many of the finer security considerations of atomic-swap technology. Some of the attack vectors clarified included the “Slippage Attack,” and problems due to “Cut and Choose,” which affected alt coins that did not yet implement CLTV.

In September 27, 2016, James finished his beta release of his fully automated and secure atomic swap software, and announced this accomplishment in this linked post.

> *I have been working on getting atomic cross chain swaps fully working for quite a while. The protocol details are described in: https://bitcointalk.org/index.php?topic=1364951*
>
> *With help and inspiration from Tier Nolan, today was the first automated atomic swap including redeems via the following transactions triggered by:*
>
> *curl --url "http://127.0.0.1:7778" --data "{\"agent\":\"InstantDEX\",\"method\":\"request\",\"vals\":{\"source\":\"BTCD\",\"amount\":0.1,\"dest\":\"BTC\",\"minprice\":0.004}}"*
>
> *alicefee:*
> *https://www.blockexperts.com/btcd/tx/867775f455c22930fa9bc0a48cd41d56fbdf043cd735f3d34a6f8dbdcfed200b*
>
> *bobfee:*
> *https://blockchain.info/tx/b4d1d3eab856547209f950ca36ac5c0f3c6b8791036962200c784b9dcea660be*
>
> *bobdeposit:*
> *https://blockchain.info/tx/f4aa6a34f07cb2bad90aca79f2fc8e51b55c23d78d53e3035f156de1a7faf2a3*

alicepayment: https://www.blockexperts.com/btcd/tx/a7e27e540b19a1225796c89de75955279e06600c2cf04462c786d158fdc269c8

bobpayment(*): txid 87b6a1e9896c1da28c1e20f421cdac1ad5233f7925962bee107147ed621a12d2

alicespend of bobpayment(*): txid 69f690d5201e1d7dabf69ea6c1bc810df843bac3a5092738a60d0410d921c9e6

bobspend of alicepayment: https://www.blockexperts.com/btcd/tx/4575c92c93459738543918ecc1871f8c27348b2006354c699401304c08ec816b

bobrefund of bobdeposit: https://blockchain.info/tx/52a3bf49eca2b49346812458ee96b242e643ae2a59080fde4b52e06d110a97df

(*)The bobpayment and alicespend of it was from a different test run

Now there are still the timeout cases to get working, but the hardest part has been to get all the mainstream spends of the custom transactions working. Now it is ready for a GUI to be made for it so end users can submit conversion requests to the LP nodes from the browser.

On the Liquidity Provider side, there is more work to do but the framework is in place for any node to signup to be an LP node with a customizable profit margin for each coin.

curl --url "http://127.0.0.1:7778" --data "{\"agent\":\"tradebot\",\"method\":\"amlp\"}"

curl --url "http://127.0.0.1:7778" --data "{\"agent\":\"tradebot\",\"method\":\"liquidity\",\"targetcoin\":\"BTCD\",\"vals\":{\"profit\":0.005}}"

A cool thing is all during this "weekend's" testing of the atomic swaps, I didnt have to reset the notary nodes at all. They ran all the time and properly handled all the comms.

The blockchain explorer addresses above link to James's first atomic-swap transactions that were performed using fully automated software. The code for these experiments can be found in the FSM branch of this linked Github repository and can be verified by any interested party.

While the core technology was ready, bringing this to the average user would require a basic GUI interface (the graphics to make trading more user friendly), support manuals, a team of support agents, and an established community. For the next eight months, the Komodo community worked together to develop these necessities.

In August of 2017, public testing of Komodo's DEX software using a GUI interface began in earnest. Most of the conversation took place in the #tradebots channels of Github, which can be downloaded and studied using this link. Throughout this time period, non-technically trained users performed atomic swaps on a frequent basis.

These events occurred during the late "bubble" period of 2017, when many newcomers to blockchain technology were rushing into the space looking for unrealized speculative opportunities. The interest surrounding atomic swaps suddenly took flight when Litecoin, one of the highest price-ranked blockchains on the market, and Decred announced "The first LTC < --> DCR" atomic swap. With the prominent market position of Litecoin and the concept of atomic swaps being completely new to the average cryptocurrency journalist, many crypto-news agencies inaccurately described this as the "first ever atomic swap." For example, here is Ethereum World's article on this subject. The Komodo marketing team reached out to many news agencies at the time to correct the record, but did not receive a large response.

Komodo continued marketing efforts for the atomic-swap DEX software and the community grew into the thousands of users. Approximately 77K Twitter followers joined by early 2018, and the Komodo subreddit community grew to nearly 10K. The Komodo Slack channel became too crowded for the service to suffice, and Komodo switched to Discord and Riot.

Over the course of the next six months, Komodo's atomic-swap DEX software facilitated hundreds of users in performing approximately 120,000 atomic swaps. Due to the way the software functions, and its lack of KYC requirements at that time, it is impossible to know exactly how many users were involved in these events. Based on download and usage activity, Komodo estimates that the total number of unique users during this time period was between 100 and 1000.

Around the time the Komodo community reached 120,000 atomic swaps, the cryptocurrency market became uncertain, and Komodo pulled back on marketing efforts for this software. In result, activity on the DEX fell.

Since this time, Komodo has worked to build v2.0 of the Komodo DEX software. Komodo developer, Artem, leads this initiative. v2.0 takes into account much of what Komodo learned during v1.0. The new version is now available for public testing.

If you would like to perform your own first atomic swap, please reach out to the Komodo team on discord at this link. Ask for the #MM2 channel and someone should be available to assist you. Please also reach out to @SHossain on Discord; he is the head of our support team.

This concludes the discussion of the timeline of atomic-swap adoption and Komodo's participation therein. The content herein is provided for research purposes, and to serve as a launching point for additional commentary.