Modernizing IOLTA using bitcoin's blockchain technology

by Pamela Morgan, Esq., Empowered Law

published March 2014; revised June 2015; revised February 2016, revised June 2021

When I became aware of bitcoin as a technology, and not just a currency, I was inspired by how it might be used to replace custodial IOLTA or client trust accounts. As most of you know, in simple terms, an Interest on Lawyer Trust Account (IOLTA) is a specific type of trust account where an attorney holds client funds, until the money is earned. Retainer is sometimes an ambiguous term. In this article, it means prepayment of legal fees for specific work that will be done in the future, not payment for an attorney to be "on-call" for whatever legal matter might arise during the month. Once the attorney has completed all or part of the work, the money is earned and the attorney must transfer the earnings out of the IOLTA account and into the attorney's personal or business account. Although the procedure might seem straight-forward at first, it's actually a complex and confusing process and many attorneys get it wrong. According to, Lawyer Trust Account Mistakes - 3 Common Lawyer Trust Account (IOLTA) Mistakes, three common mistakes are (1) "Borrowing" money from the trust account, (2) Commingling attorney funds with client money, and (3) Failing to properly track client funds. Attorneys are disciplined and disbarred every year for making these "mistakes"[1].

With blockchain technology and programmable[2] money, we no longer need custodial IOLTA accounts; we can simply use bitcoin or another cryptocurrency to facilitate transparent, instantaneous transfer of value which protects both the client and the attorney. Cryptocurrencies also enable "watch only" features where a trusted third party, such as an accountant, can be given credentials to view the account transactions but not initiate transactions.

Before we explore the blockchain solution, let's look at how and why IOLTAs were created and what problems they attempt to solve. The first issue is client protection, the second is ensuring attorneys get paid for legal work.

Governments, attorneys, and bar associations have been concerned about protecting client funds for many years. According to the American Bar Association (ABA) article, A History of the Client Protection Rules, the development of the laws surrounding client protection seemed to be historically tied to depressed economic times when client funds were misappropriated. Today, the ABA model ethics rules, and the ethics rules adopted in virtually every jurisdiction, clearly state that it is unethical for attorneys to commingle client funds with firm or attorney funds. Additionally, ABA Model Rule 1.15 requires attorneys to keep client funds in a client trust account. The IOLTA solution, while better than nothing, does not

[1] See the following articles as examples: Ex Michael Jackson Lawyer Disbarred for Commingling Funds to Evade Creditors, Attorney Disbarment Warranted When Funds Commingled and No Legal Services Provided, Disciplinary Actions from the Most Recent Law Journal (North Carolina)

[2] Learn about the concept of programmable money: https://youtu.be/_0jxX84mzts

adequately protect clients. IOLTAs are still custodial accounts, with little oversight, and no client control.

What's wrong with custodial accounts? Custodial accounts, particularly those with little oversight, create an environment that seems to invite confusion, misuse, and misappropriation. Remember the the Madoff case where investors lost millions of dollars? Custodial accounts with little oversight. For those of you familiar with bitcoin, remember Mt Gox? Custodial accounts with little oversight. How does this relate to IOLTA? IOLTA exhibit the features of typical custodial accounts with little oversight by outside parties and no client control.

Many firms have one single IOLTA where all client funds are deposited and managed. Why? Because having a separate account for each client would be too cumbersome for the bank and the firm. Who watches over these accounts? The owner of the account - the law firm. While the firm may have audit procedures in place, there is no third party watching out for individual clients in real time. More importantly, individual clients cannot verify their own balances independently. Clients are not provided with aggregate IOLTA information; it would be of limited value to clients as the account contains information for all clients and not just one. In order to see the status of their account, clients must usually request an "accounting" from their attorney. The accounting is typically derived from the firm's internal accounting system and should show all financial activity relating to that client. Obviously the accounting could be manipulated by the one party who creates all of the data, the one party who provides all of the information to the client, the one party who is entrusted with protecting the funds from misuse by the one party who has access to them - the attorney or firm. I'm not suggesting that most attorneys or firms would manipulate the data, nor am I suggesting that an attorney would intentionally set out to steal client funds. I am, however, suggesting that the system is both inefficient and ineffective at protecting clients and attorneys and there is a better way.

How could we do it better? If misappropriation is such a problem, why allow attorneys to hold client money in the first place? Why not create a service first, pay later model? Attorneys typically require a retainer because: (1) attorneys want assurance that they will be paid for their work, as we know non-payment of fees is a huge issue for lawyers, (2) clients who pay up front are typically more willing to take action when asked, like requesting records or otherwise participating in the legal action, and (3) attorneys need access to client funds to pay expenses like filing fees. Without client funds either the attorney assumes the financial risk for the client's case, potentially causing ethics issues, or the client must be immediately available to pay court costs and filing fees in the appropriate manner when needed.

What other options are available? Currently, there are four viable alternatives to IOLTA, all using cryptographic ledgers or the bitcoin blockchain technology.

Option 1: Use bitcoin, or an alt coin, for payment of legal fees when they become due. Why is this a better solution to protect clients and attorneys? It eliminates the need for custodial accounts. When using traditional payment methods, such as checks or even credit cards, there is a significant delay between the payment request and the time the client pays. Have you seen your firm's most recent accounts receivable aging report? In my experience, my bitcoin clients pay within thirty minutes of receiving an invoice - yes, minutes, not days. Currently it takes about ten minutes for a bitcoin transaction to be verified and about an hour for me to rely on it. Additionally, payment requests can be processed using SMS, smart phone, or traditional computer/laptop. Also "opening" a bitcoin account is faster, more convenient, and less expensive than opening a traditional bank account. For the examples in this article I'm using Copay, a multi-signature wallet from BitPay, a wallet provider but there are many excellent services available.[3] Admittedly, the risk shifts from the client to the attorney using this method and it may not be appropriate for all practice areas. It does, however, encourage frequent communication between attorney and client, which is likely to increase overall client satisfaction.[4] (Clients commonly complain in grievances that their attorney was non-responsive. If communication necessitates payment attorneys are incentivized to communicate more frequently with clients.)

Option 2: Replace the current system with the exact same system, on the blockchain, for increased transparency. How? The attorney and the client both create bitcoin wallets.[5] The attorney creates two addresses within the wallet, one for client funds, one for firm operating expenses or earned funds. The client can have one address or more, depending on their preference.[6] When the client retains the attorney, the client simply transfers bitcoin from their wallet to the attorney's client account address. When the attorney has earned the funds, the attorney transfers them from the custodial account into the firm or personal account. This is the same process we currently use with two important distinctions: transparency and convenience. Clients can view the balance in the custodial account at any time, from the privacy of their home or from anywhere in the world. Confidentiality is maintained because while the transactions are public, the ownership of the accounts generally is not. This protects the client because it provides real-time convenient oversight, by the client. The challenge with this option is that the client will see all transactions in the account, not just those relating to their own funds.

Option 3: This is essentially the same as Option 2 above but instead of a single client account the attorney creates an account for each client. Bitcoin addresses can be created for free, with the click of one button, in less than ten seconds (depending on internet speed, of course). With the wallet I've selected, I can use my phone or laptop to create new addresses. Each address can and should include a client name, matter, or some other identifier. Using the example below, I've created an account called

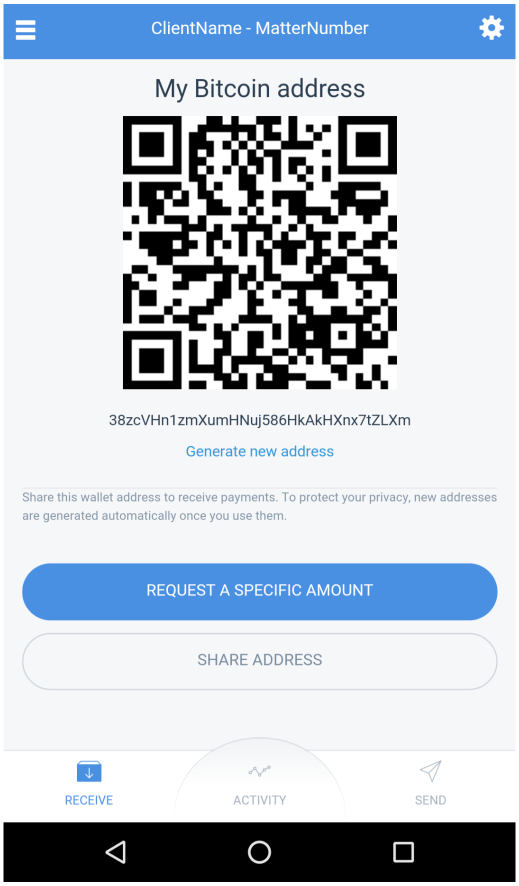
[3] Multisignature wallets are an industry best practice. They provide backup and recovery options should a signer become unavailable, they also help to prevent embezzlement.

[4] Clients commonly complain in grievances that their attorney was non-responsive. If communication necessitates payment attorneys are incentivized to communicate more frequently with clients.

[5] For an explanation of the process, try https://www.weusecoins.com/en/.

[6] It's worth noting that "opening" a bitcoin account is faster, more convenient, and less expensive than opening a traditional bank account. Creating an address is even easier. I create new addresses for free, in seconds, by clicking one button. I don't need to know, use, or understand computer code.

ClientName-MatterNumber. Within that account I can create more than two billion unique bitcoin addresses.



38zcVHn1zmXumHNuj586HkAkHXnx7tZLXm

Share this wallet address to receive payments. To protect your privacy, new addresses are generated automatically once you use them.

The long string of numbers below the QR code, beginning with a "3", is the unique bitcoin address I've created for this example. This is the "account number" that would be provided to the client. It's best to provide both the QR code and full address to the client. When using this method use care to document this address in the client file or elsewhere and be sure to securely backup the wallet.

When the attorney provides the address to the client, the client deposits the retainer into the given address. The client can then see each outgoing transaction related to that address, in real-time, from any internet connected device. There's no need to ask the attorney for an accounting, it's available in real-time anytime. Again, this benefits clients by encouraging open frequent communication and client oversight. This allows clients to monitor their own funds without seeing the entire trust account holdings. [7]

Option 4: Creating a digital escrow or multi-signature account with the client and a third

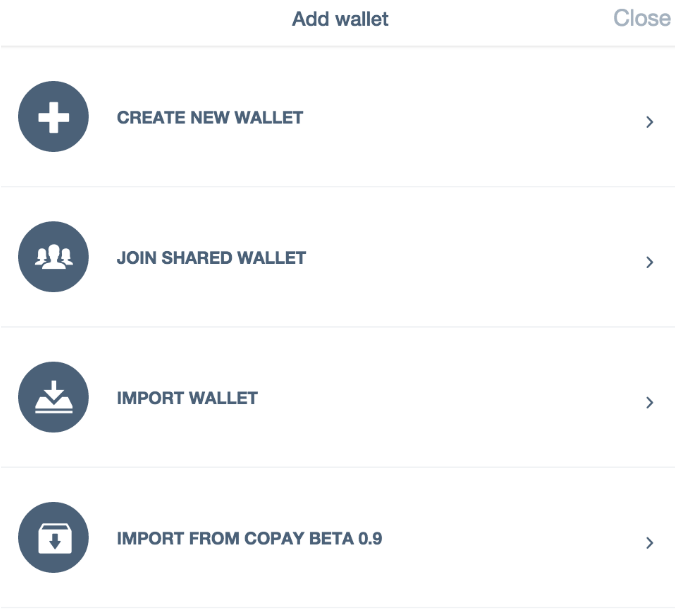
[7] Industry best practice requires testing of an address prior to full funding.

party.[8] While this option might sound complicated at first, it's really almost as simple as the other options above with two main differences: (1) a third party is optionally brought into the transaction to resolve any disputes and (2) the attorney does not have custody of the funds. Bitcoin has the ability to include some conditions on transaction execution including dates and signatures. The technology enables us, for the first time, to have the equivalent of non-custodial escrow accounts. The conditions must be put in place prior to funding, which makes sense because it should be part of the retainer discussion.

Let's consider an example of this implementation. We'll walk through the creation of a wallet (account), initial account funding, and workflow of a payment transaction. In this example Alice is the attorney; Bob is her client; Pamela is the arbitrator/third party.

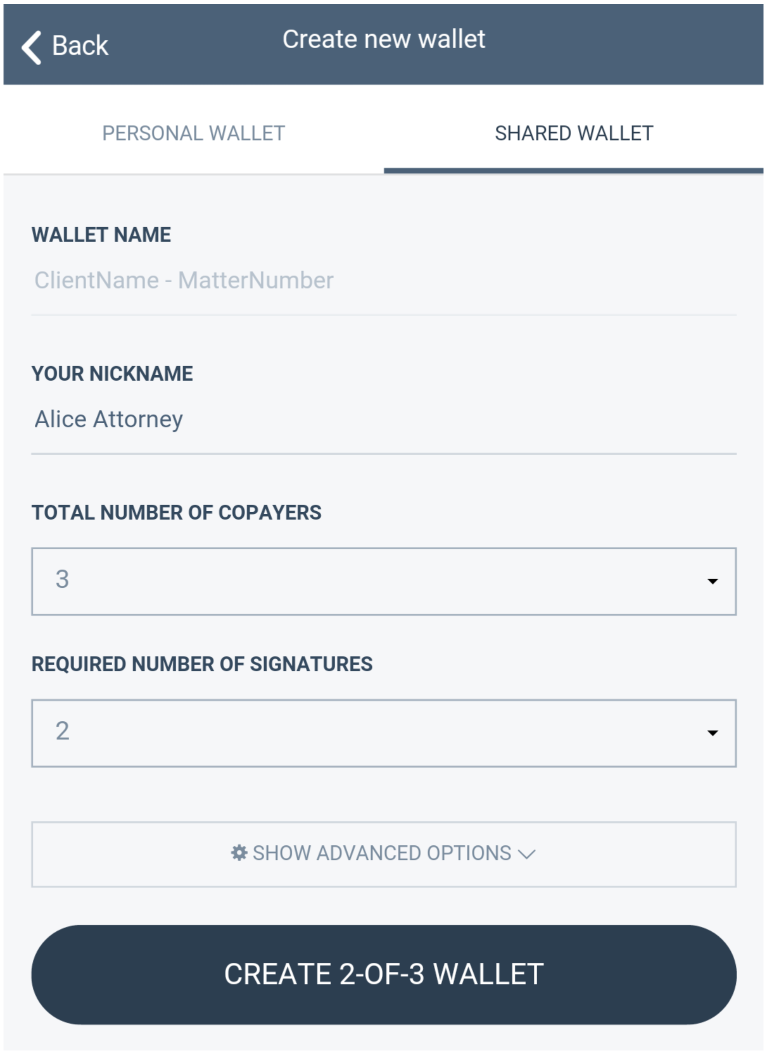
Creating a Wallet:

Alice initiates the wallet creation using her Copay.io account. Instead of creating a new address, Alice creates a new wallet, which is as easy as selecting the "Create New Wallet" option. This allows her to designate Bob, Alice, and Pamela as signers on the account.



For this example, Alice names the wallet "ClientName-MatterNumber" to distinguish it from other wallets and clients. Then Alice adds her Nickname, "Alice Attorney", which will be seen by all other signers on this account. Alice selects 3 as the total signers with 2 required signatures. This means that two of the three signatures are needed to release any funds.

[8] Multisignature addresses can (and should) be used for bitcoin holdings of law firms for governance and separation of duties. Learn more about bitcoin and corporate governance: https://empoweredlaw.wordpress.com/2014/05/25/multi-signature-accounts-for-corporate-governance/



WALLET NAME

ClientName - MatterNumber

YOUR NICKNAME

Alice Attorney

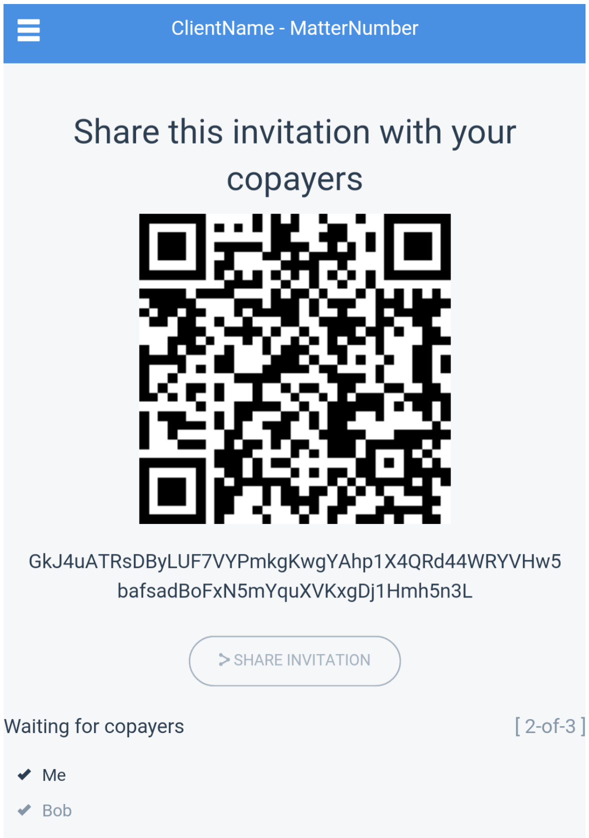
TOTAL NUMBER OF COPAYERS

3

REQUIRED NUMBER OF SIGNATURES

2

When Alice selects “CREATE 2-OF-3 WALLET” the wallet is created and an invitation to join the wallet is created. Alice then sends Bob and Pamela the invitation, again either by sharing the QR code or by sending the long string of numbers and letters below the QR code.



Share this invitation with your copayers

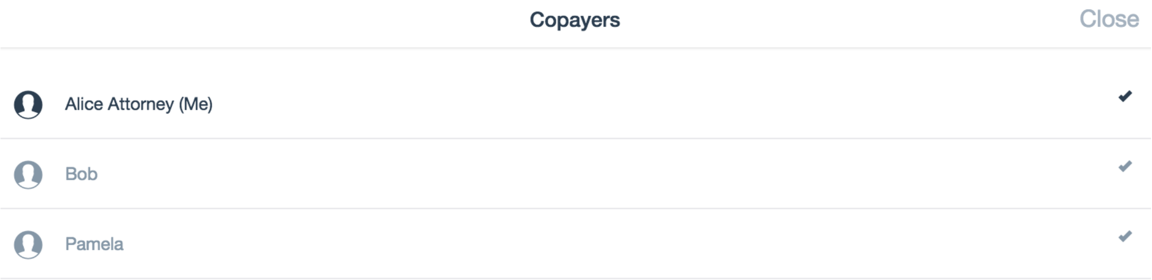
GkJ4uATRsDByLUF7VYPmkgKwgYAhp1X4QRd44WRYVHw5bafsadBoFxN5mYquXVKxgDj1Hmh5n3L

Waiting for copayers [2-of-3]

✓ Me

✓ Bob

Once Bob and Pamela respond to the request, the wallet is ready for use.



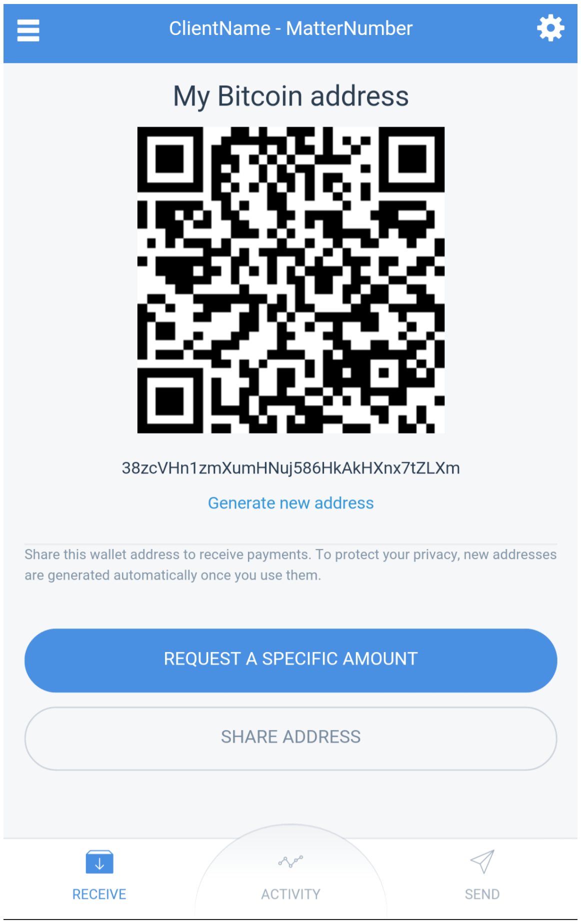
Alice Attorney (Me) ✓

Bob ✓

Pamela ✓

Funding the Wallet (retainer):

Alice then sends Bob a request to fund the account with a retainer payment. To do this, Alice selects "RECEIVE" from the options at the bottom of the screen and a receive address will appear. Typically Alice will send the request to Bob with a copy of a signed retainer agreement, in email. It is not a security risk to transmit payment requests, including QR codes and bitcoin addresses, in open unencrypted email, though retainer agreements should be appropriately secured.

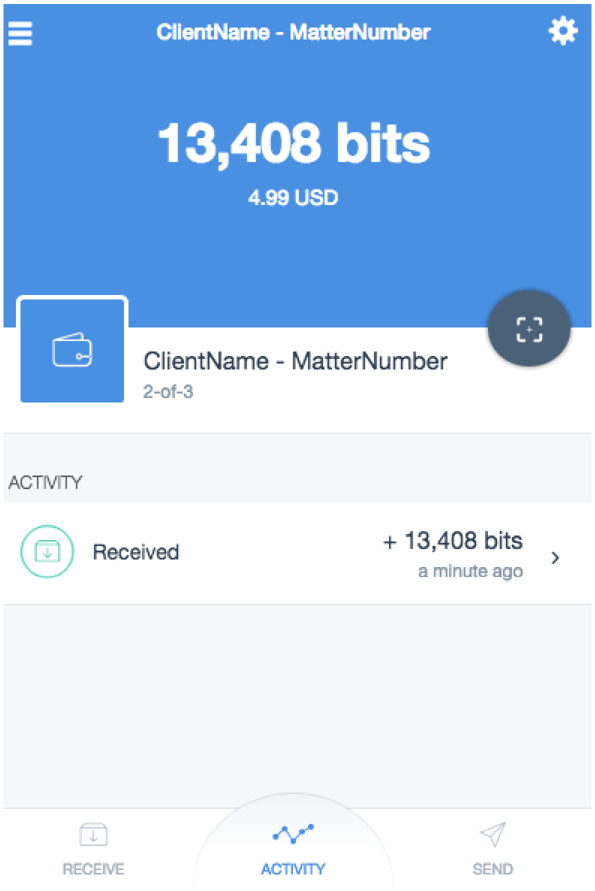


My Bitcoin address

38zcVHn1zmXumHNuj586HkAkHXnx7tZLXm

Share this wallet address to receive payments. To protect your privacy, new addresses are generated automatically once you use them.

Bob then can respond to the request and fund the wallet. For purposes of this illustration a small amount of bitcoin was used to fund, however there are currently no value limits on transfers. One could fund thousands, millions or more in a single transaction. Importantly, however, before fully funding any new address, the spending function should be tested to ensure the address was set up correctly and everyone knows how to use the system. When the account is funded it looks like this:



ClientName - MatterNumber

13,408 bits

4.99 USD

ClientName - MatterNumber

2-of-3

ACTIVITY

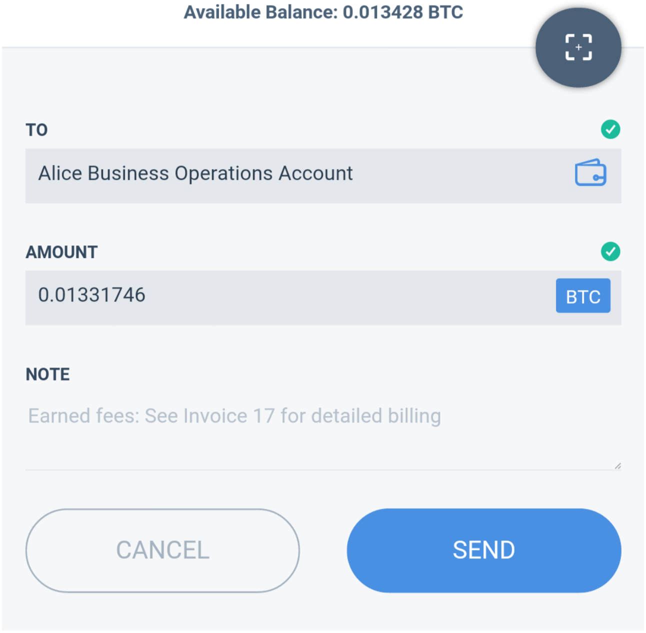
Received + 13,408 bits

a minute ago

Notice that neither Alice nor Bob can move funds without the others approval, unless they get Pamela involved. Alice knows the funds are available for payment when needed. Bob knows that he will be informed and involved in payments to Alice.

Client Billing and Payments:

When Alice has earned some fees, she initiates a request to Send funds to her personal or business operations account by selecting the “Send” button and completing three fields.



Available Balance: 0.013428 BTC

TO

Alice Business Operations Account

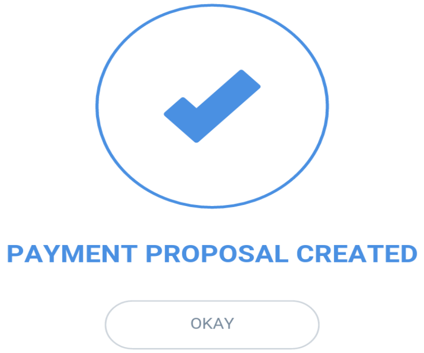
AMOUNT

0.01331746 BTC

NOTE

Earned fees: See Invoice 17 for detailed billing

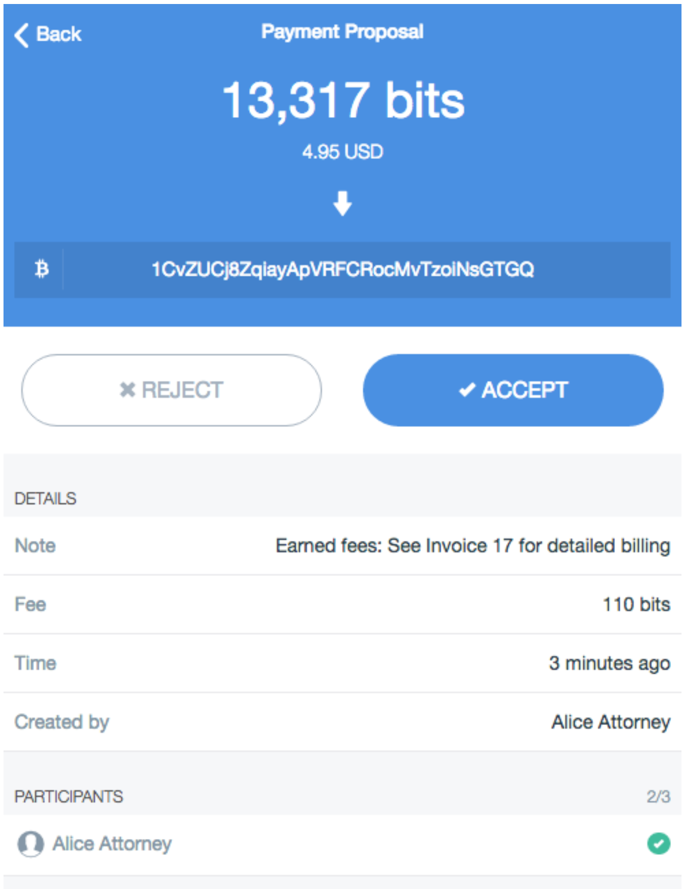
She then selects “SEND” and sees this screen:



PAYMENT PROPOSAL CREATED

Alice selects “OKAY” and waits for Bob or Pamela to sign. Bob and Pamela will both receive notifications that a transaction is pending. In this instance, for policy reasons, Pamela would not sign unless she was also notified of a dispute.

Bob will review the pending transaction in his wallet software.



Payment Proposal

13,317 bits

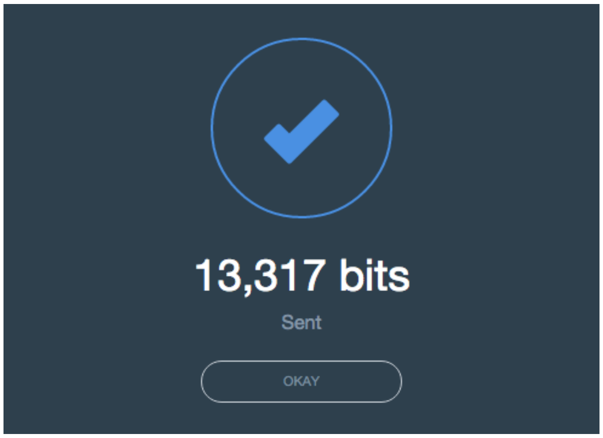
4.95 USD

฿ 1CvZUCj8ZqiayApVRFCRocMvTzoiNsGTGQ

DETAILS	
Note	Earned fees: See Invoice 17 for detailed billing
Fee	110 bits
Time	3 minutes ago
Created by	Alice Attorney

PARTICIPANTS	2/3
Alice Attorney	✓

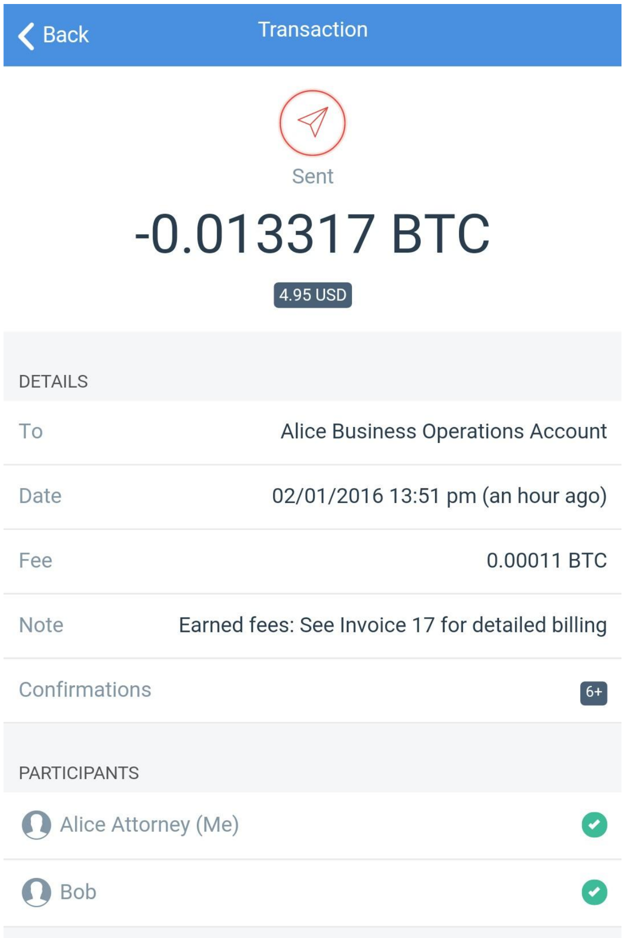
Bob's notification allows him to review the transaction details including who created the transaction, the amount, the receiving address, detailed notes, and what signers have approved the transaction. He has the option to accept or reject.



13,317 bits

Sent

By selecting "ACCEPT" the 2 of 3 signature requirements are met and the transaction is sent to the network. Note, only Alice and Bob need to sign the transaction to release the funds to Alice. Pamela, the third party, is uninvolved.



Transaction

Sent

-0.013317 BTC

4.95 USD

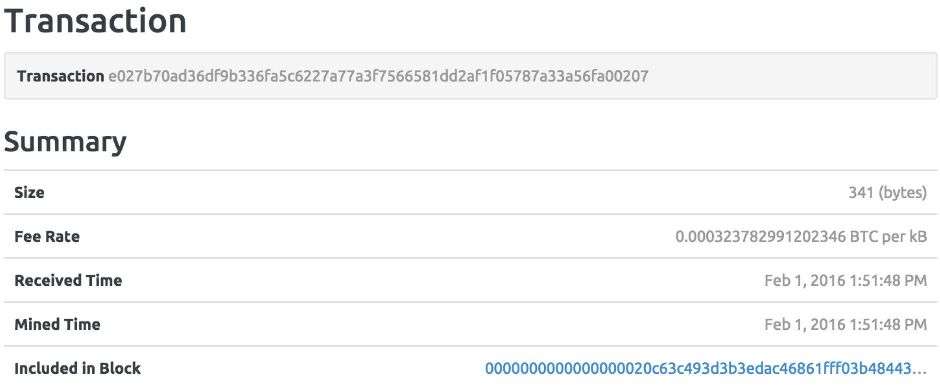
DETAILS

To	Alice Business Operations Account
Date	02/01/2016 13:51 pm (an hour ago)
Fee	0.00011 BTC
Note	Earned fees: See Invoice 17 for detailed billing
Confirmations	6+

PARTICIPANTS

Alice Attorney (Me)	✓
Bob	✓

An immutable public ledger is created with the transaction, in the public bitcoin blockchain, and the account transaction history is recorded within the wallet itself.



Transaction

Transaction e027b70ad36df9b336fa5c6227a77a3f7566581dd2af1f05787a33a56fa00207

Summary

Size	341 (bytes)
Fee Rate	0.000323782991202346 BTC per kB
Received Time	Feb 1, 2016 1:51:48 PM
Mined Time	Feb 1, 2016 1:51:48 PM
Included in Block	0000000000000000020c63c493d3b3edac46861fff03b48443...

Dispute Resolution:

If Bob is unhappy with Alice's representation he could decide to reject the transaction. Alice then has two options, Alice could (and should) talk to Bob about the representation and resolve the issue directly with him. If that doesn't work, Alice can contact Pamela and begin the dispute resolution process.

Today there are no independent standards for third party blockchain dispute resolution. Each third party can set their own rates, response times, requirements, procedures and law to apply[9]. If Alice can convince Pamela that she has earned the money and should receive it, Pamela and Alice can sign the transaction. Two of three signatures will release the funds to Alice. However, if Bob can convince Pamela that Alice has not earned the money or has failed to deliver adequate services to Bob, then Bob and Pamela can sign the transaction, releasing the money to Bob (a refund). This solution protects both parties while avoiding third party intervention in most cases. If a dispute arises, both parties can present the dispute to their chosen third party for quick, inexpensive, binding resolution.[10][11] Interestingly, Pamela could find that Alice is entitled to partial payment and Bob is entitled to a partial refund. If she can get one of the parties to agree to this distribution then it will happen, if not the money just sits in the account until two of the parties are willing to sign a transaction.

This is the ideal IOLTA replacement because it provides oversight not only by the client but by a third party, if needed. It provides an easily auditable, unforgeable, transparent trail. It protects both parties and eliminates many problems with traditional custodial accounts.

Why might the legal community be reluctant to replace IOLTA? First, many states require attorneys to deposit custodial funds into an IOLTA. Options two and three above might violate this rule. Options one and four above would not appear to violate the rule because the attorney is not taking custody of the funds. However, states could disagree with that interpretation. Second, interest bearing IOLTA fund state pro-bono legal systems. While this a good and worthy cause, this funding can be accomplished by simply reallocating bank fees that firms would have paid using the old system to those pro-bono causes.

Multisignature in practice. Today, using multisignature in practice takes some effort and some technical knowledge. Not many wallets offer native multisignature support. However, in the summer of 2021, the bitcoin network agreed to an upgrade (colloquially called Taproot).[12] Taproot will make using multisignature less expensive and should encourage more development in this area. Over the next few years we should see more user-friendly

[9] Of course the effectiveness of this dispute resolution is highly dependent upon jurisdiction and process.

[10] Binding in the sense that once the funds are released any aggrieved party would have to seek recourse outside of the blockchain, typically from the legal system of their local jurisdiction.

[11] As an aside, this area is ripe for mediation and arbitration experts to expand their practice areas and offer services in this capacity.

[12] https://www.coindesk.com/taproot-bitcoin-upgrade-improve-technology-software

multisignature enabled wallets and we may even see some additional programmable money features, like time-locks[13], implemented in an easy-to-use way.

Other considerations. There are many other considerations, such as currency volatility, exchange, taxation, and credit that are not addressed in this article. I'm sure there are others that have yet to be discovered. This article is meant to provide enough information to spur an open discussion about changing the way we view IOLTA, custodial accounts, how clients are served, transparency and other relevant issues. The bitcoin technology provides an opportunity to rethink, reimagine, and redesign systems - including the legal system. We don't have to settle for "that's how we've always done it" anymore. We can do better and we should.

Contact: Pamela Morgan, Esq.;
Twitter: @pamelawjd
Email: pamela@empoweredlaw.com
Web: www.empoweredlaw.com

[13] Time-locks are exactly what they sound like, adding time constraints on the ability to move funds. For example, I can create a multisignature time-lock that allows instant access to funds with 2 of 3 keys but also allows a single key to unlock funds only after one year has passed.