UX draft for a bitcoin wallet

for the 99%

Design guidelines.

Bitcoin is still in phase of collectible/ store of value, and not yet in medium of exchange (no-one spends their coins). So may be this work is for the future but the future is built today. Also, if it's not bitcoin it will be another coin: the future is crypto.

The purpose of this document is to share some ideas for a wallet that would include **simple contracts** like multi-signature and time locks but is aimed at **consumer users**. Simple enough so my mum can use it (not my grandma though)

- Embrace users' current mind models and standards. Be clear.
- Establish hierarchy; hide non vital detail.
- Make users' mistakes hard to happen.
- Tell a story.

Alice doesn't do crypto

The target user…

- uses a smart phone fluently
- isn't interested in running a full node **(non politics)**
- doesn't know what UTXO means **(non technical)**
- has crypto and uses it (as opposed to just hodling)

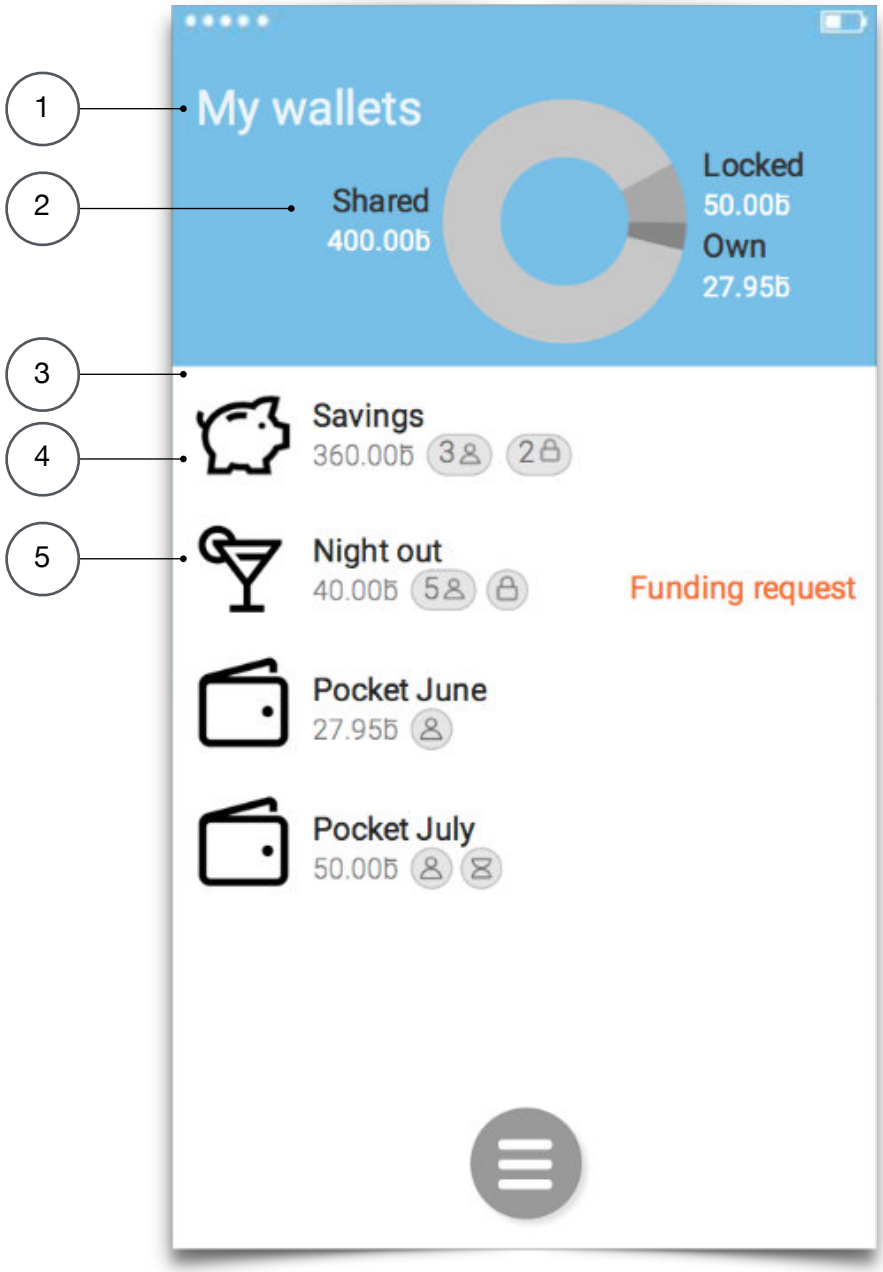
The first three describe almost every human on Earth. People forgetting this is why UX in the space has such a bad press.

Regarding the fourth, I don't have data, but the number will grow with adoption. In fact, consumer oriented products like this general purpose, easy to use wallet should help adoption.

This is not:

- **Visual design.** Wireframes are ugly and things don't align. Its purpose is to describe the information architecture and task flows. They are also handy to make cheap paper user tests.
- **A complete wireframe spec**. Never waste time working on something that nobody wants. That means publishing incomplete work.
- **Branding**. The fact that this wallet doesn't have a name will give you a clue about how lazy (focused) I am.
- **Code**. Not a line.

This is a sketch: ideas **to be explored** and expanded further. As you know, the devil is in the details and there is plenty of space in this document for him to lurk.

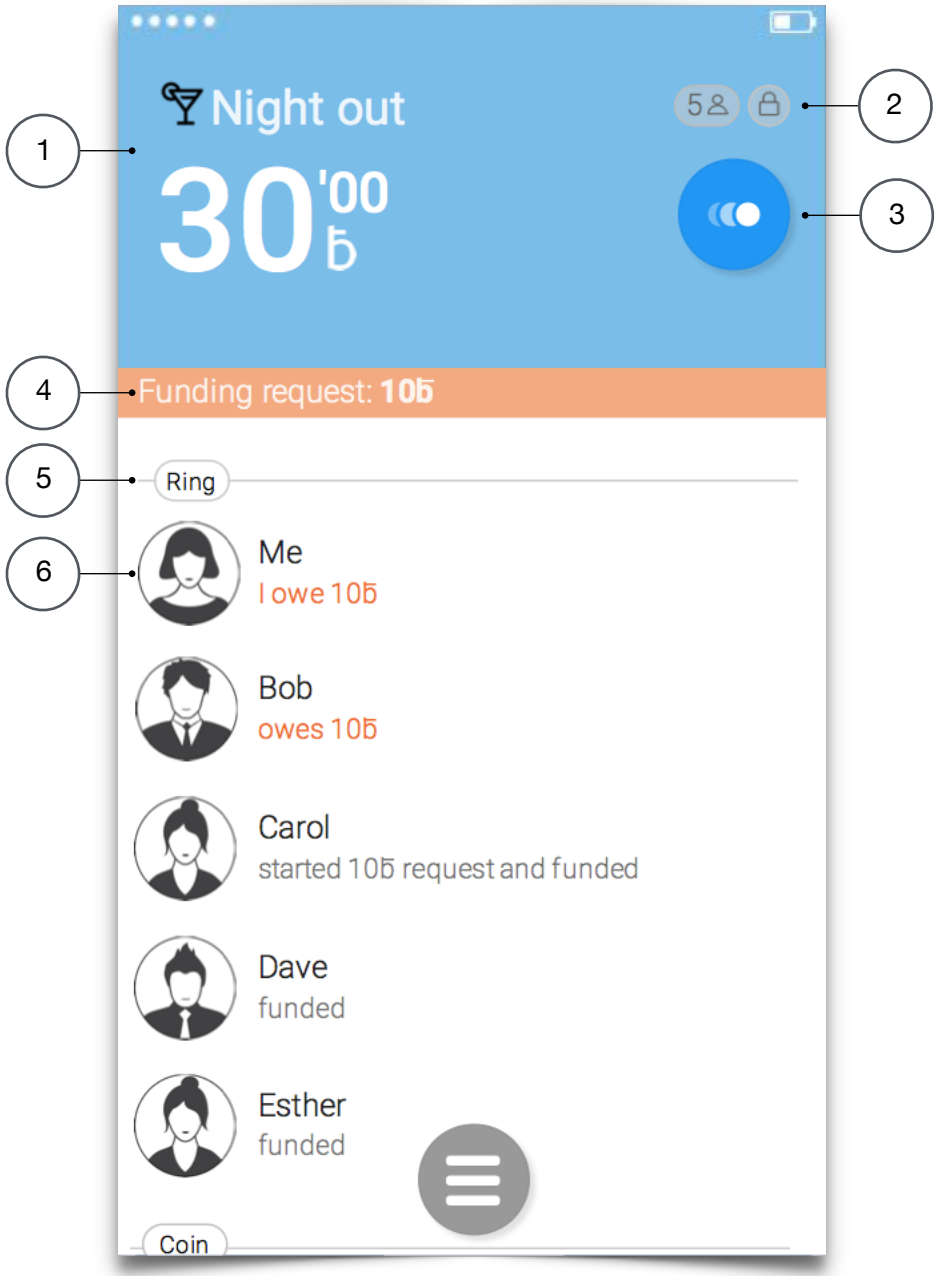


Home

High level view of a user's wallets.

1. Here there will be a logo / brand.
2. A donut chart to aggregate my wallets. Different users could need different visualisations; more research should be conducted to explore options.
3. List of wallets. Each line leads to the details. Alice has four of them.
4. Each line shows its icon (or user picture), name, holdings and a visual summary of the wallet's properties.
5. This one shows an alert: someone in that **ring** started a funding request.

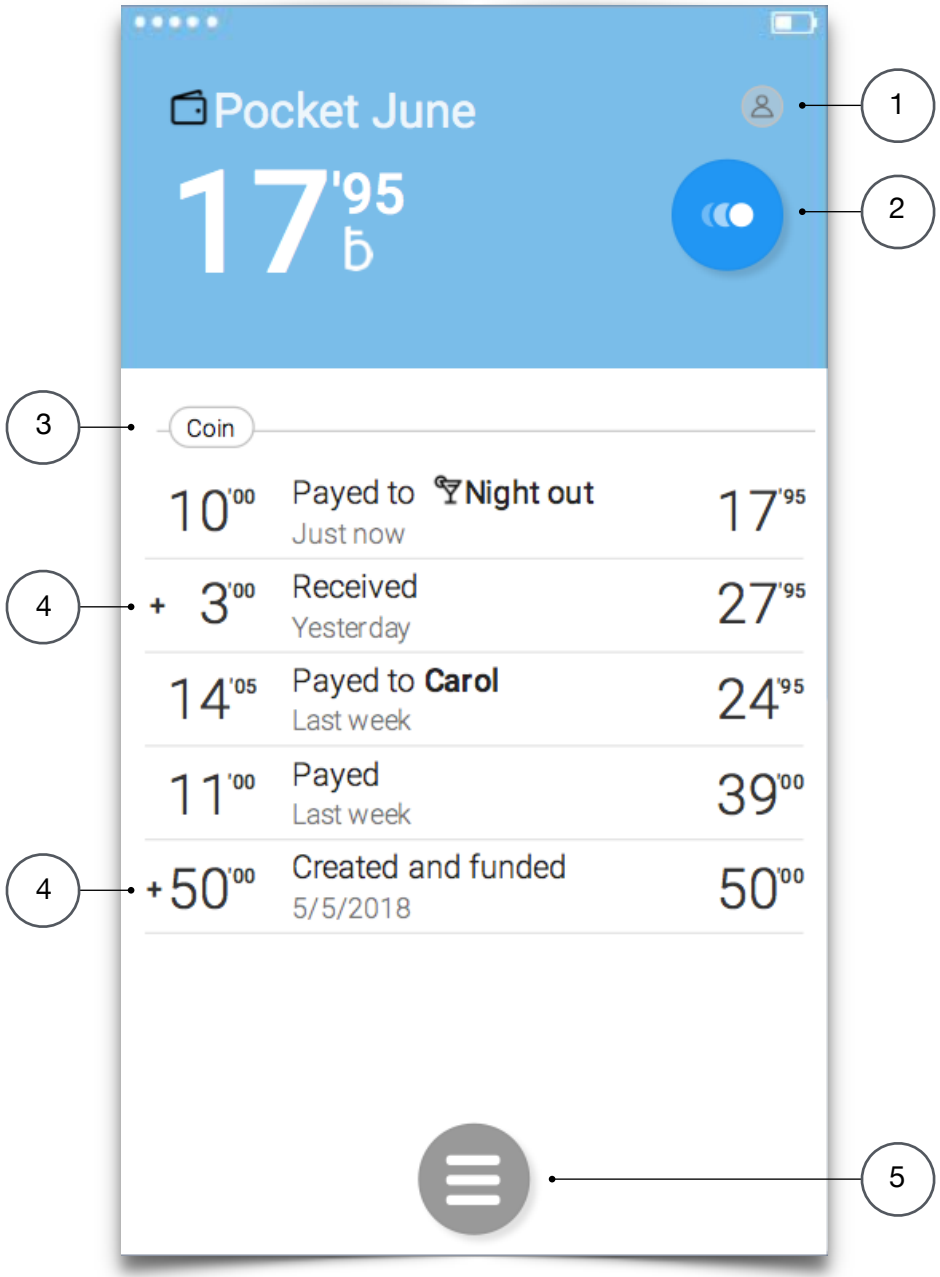
Note: I like the word "ring" for the group of entities that share a wallet. Rings are interesting. They use **hard rules** (contracts) and **soft rules** (social/UX) to shape themselves. You can model different social/economic relationships like the examples offered, based on the ruleset. It's fun to explore other possible use cases. For instance: How would be a ring with differently weighted votes?



Wallet detail

"Within" the user's wallet.

1. Icon/image, title, amount. The amount of funds is the most important element of the screen.
2. This ring has 5 members. Only one signature is needed to spend the funds. They are long time friends and they trust each other with this amount of money. This makes paying for the group drinks more convenient. A physical version of this arrangement is commonly used by many people, though there is usually only one bearer of the cash. In my hometown it is called "*bote*" (=pot)
3. "Pay" button. It starts a payment flow.
4. Carol created the wallet and made a funding request.
5. A list of the persons sharing the wallet.
6. Alice should transfer 10 units from her other wallets. This is an example of the "soft" rules I mentioned before. The warnings make clear who contributed and who didn't. Transparency and peer pressure enforcing honesty.

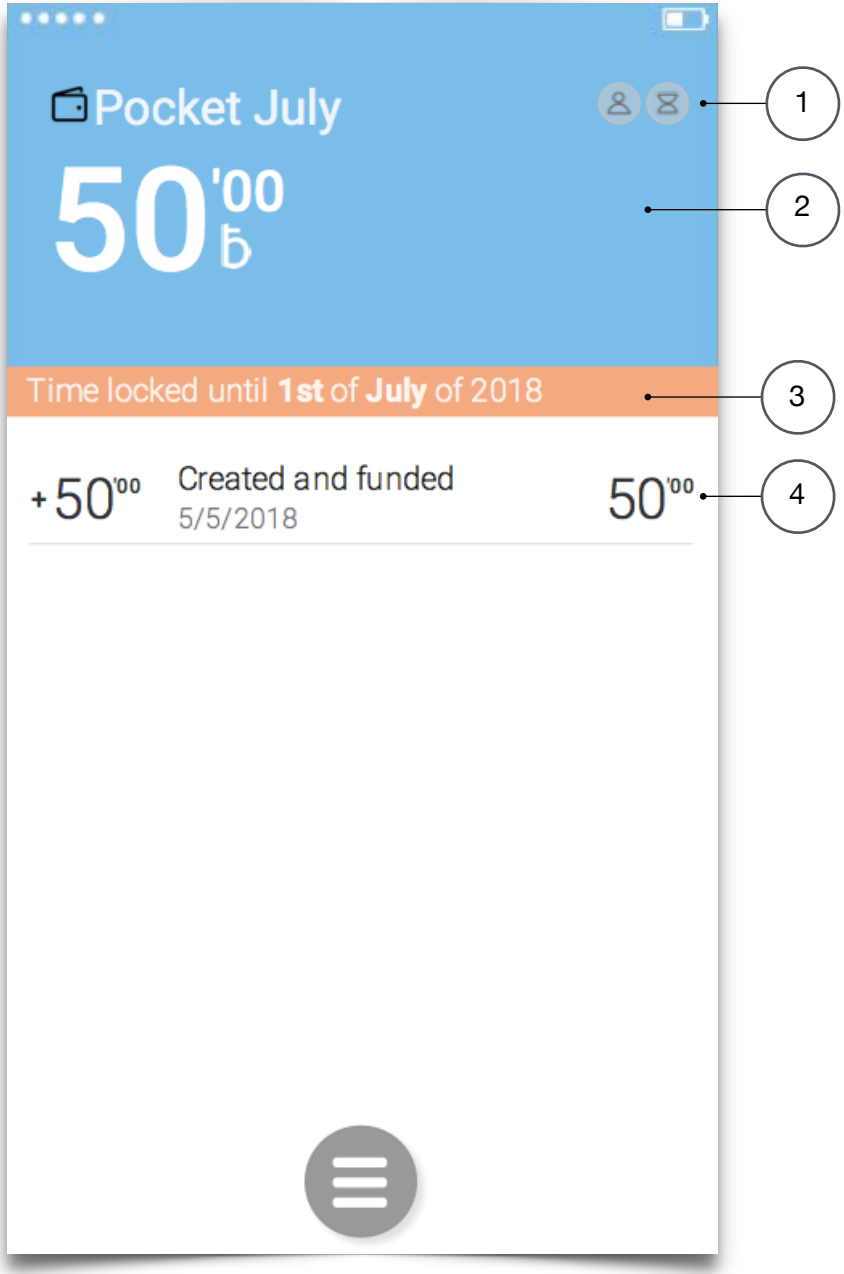


Personal wallet

A classic wallet fits the model

1. The user is sole owner of the money. No need for # of signatures icon because it is redundant.
2. “Pay” button without a currency symbol. Designing this icon was fun. It stresses the fact that the money is going away: “Think before you spend” Purists, please forgive me for using a gradient.

3. Classic list of operations and balance. Every line opens to show details.
4. Incomes visually separated from spendings. Add some colour in visual design but keep it colourblind safe.
5. The hamburger button is a contextual menu, grouping “everything else” functionality.



Future money

Time locked wallet

This wallet will become a normal personal wallet in July. This is another use case that fits nicely within the general model.

1. The user is sole owner of the money, but it is not available yet. The second icon would like to be a sand clock but my visual design skills.
2. No “Pay” button
3. “Warning” explains the situation.
4. Creating and funding a wallet can be only one operation in the user’s mind model if done one after the other. In fact, a wallet of this type should be created automatically upon receiving a time locked payment.

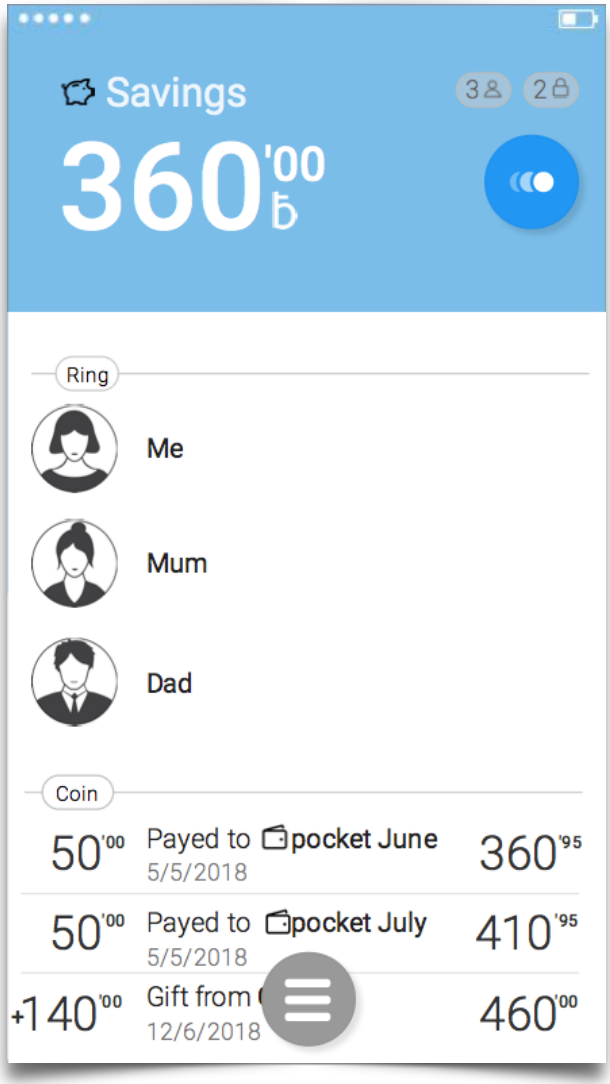
Payment

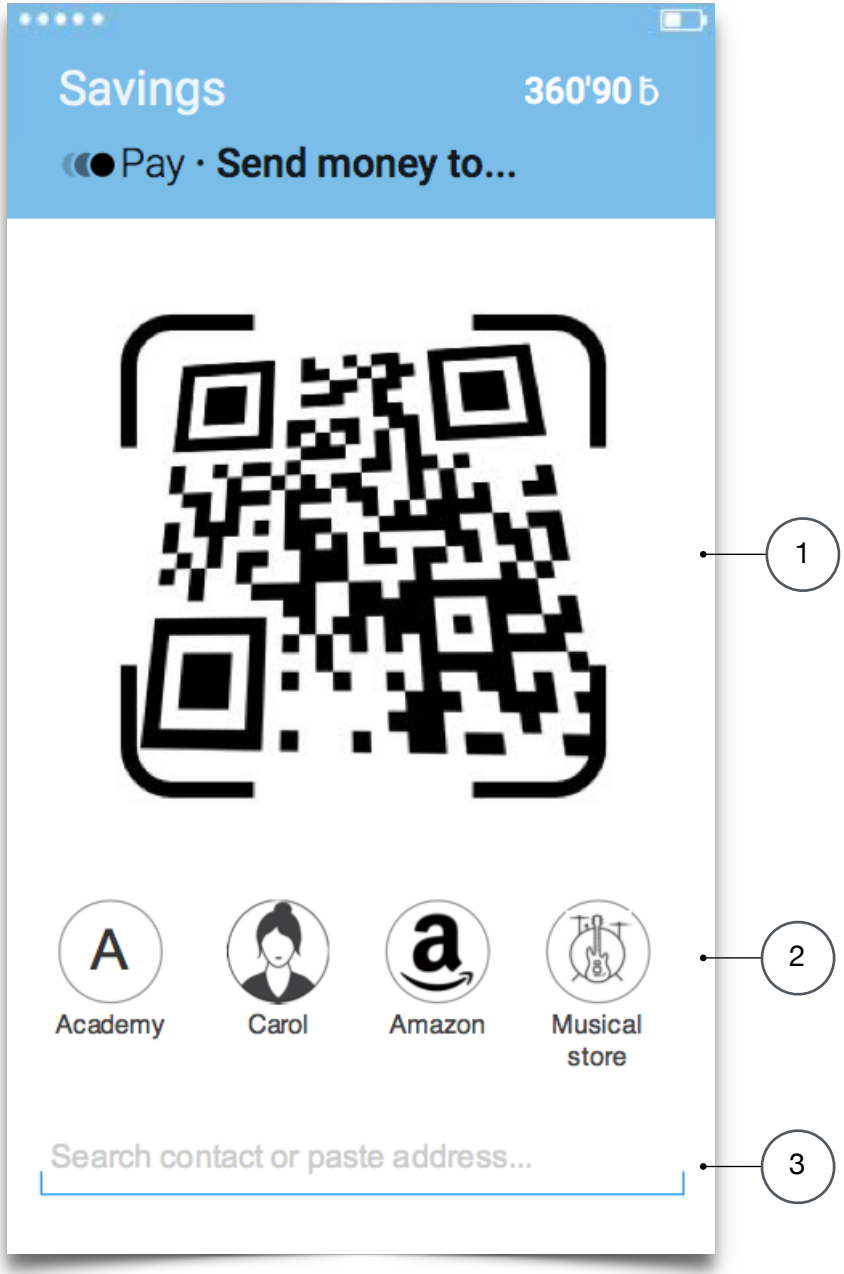
Multi-signature user story

Alice's old guitar is a cheap toy. Now that she is in a band she needs a new one. She has been in every shop in town looking for the perfect one…

This is a "Savings" wallet. Multisig 2 of 3. Alice needs either her mum or her dad to sign along with her for any payment. Both parents together could also spend.

Alice taps the button to start a payment.





Send money to...

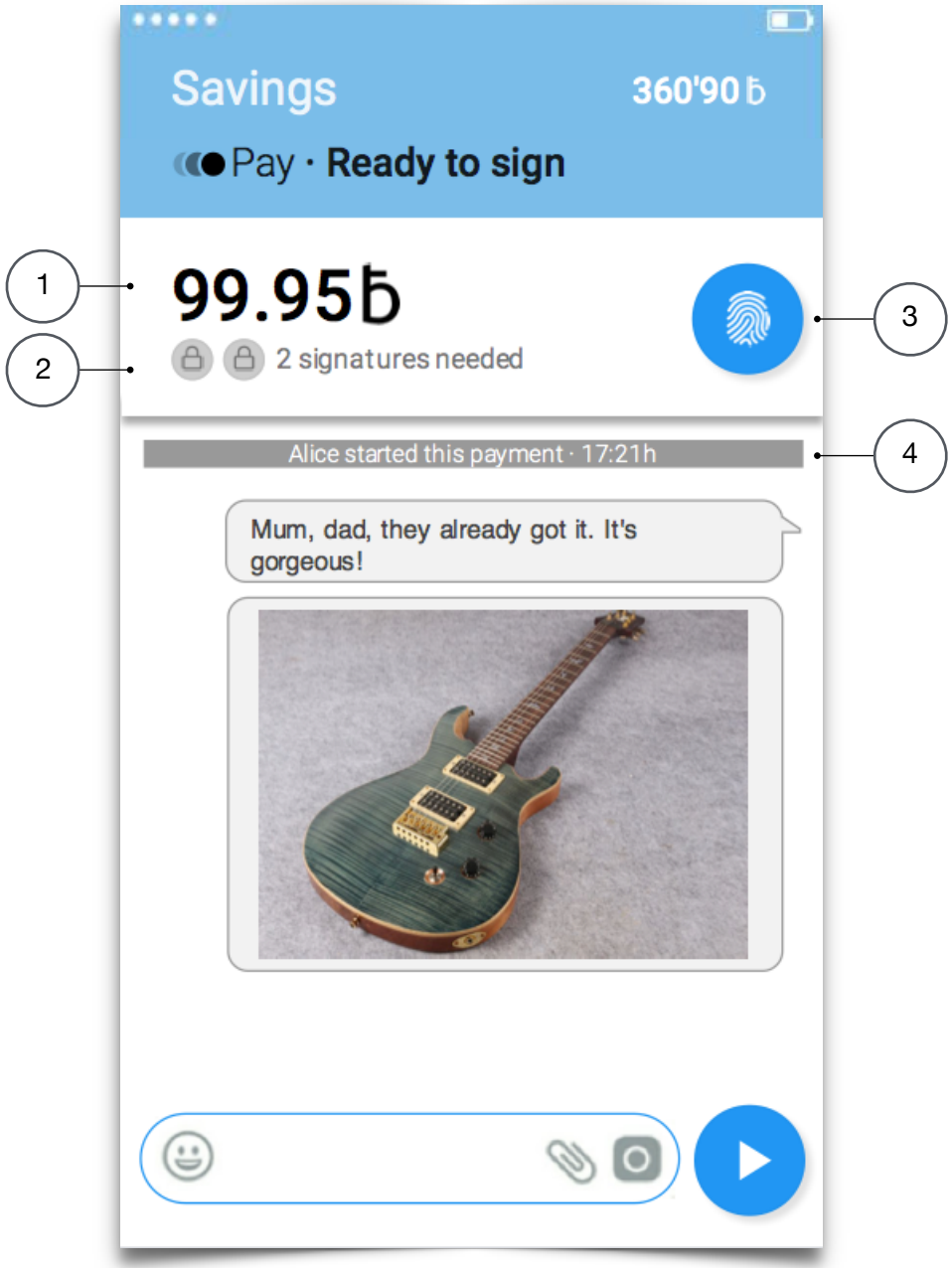
Payment 01

The task of starting a payment is a pain point. The long list of symbols of an address is intimidating for most people: Is it right? Will I lose my money? Give me my glasses!

People pay to other people and business, not to a list of symbols. Crypto digital identities will probably solve this problem. Meanwhile, is there a way attach metadata to an address? Can we have a list of identified addresses without having the user entering the data?

1. QR scanner is on by default.
2. Last contacts payed from this pocket.
3. Text input to search for a contact or and address. When tapped it opens the keyboard and closes the QR scanner.

The paths 2 and 3 need another screen after this one to input the amount to pay.



Ready to sign...

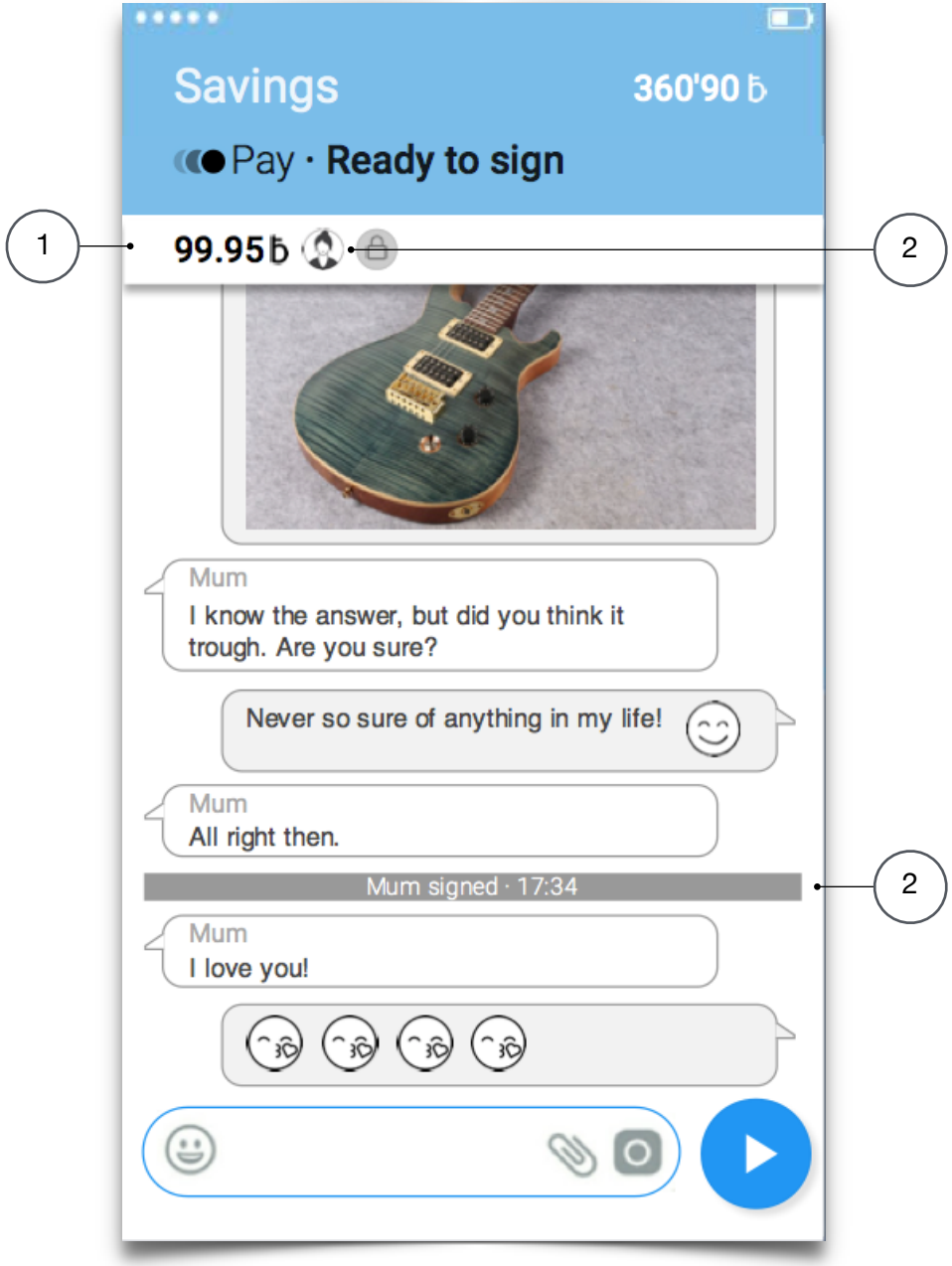
Payment 02

1. Amount to pay. If we had name and/or image of the receiver they should be part of this group. The address is not shown here; it is be available in a deeper view.
2. # of signatures needed to send the payment.
3. “Sign” button
4. If this looks like WhatsApp is because I copied it.

Messaging platforms already have or will have payment systems. They are a natural fit because payments are communication. Also controlling a payment network can be very lucrative. It should be obvious why wallets need a chat.

Here we show a conversation within the ring, but buyer/seller is equally relevant. That raises the question about the scope of the conversation: Is it tied to a transaction? Is it more general? How public? The whole market? (That’s Twitter’s turf)

My view: attach it to transactions, like in this example.

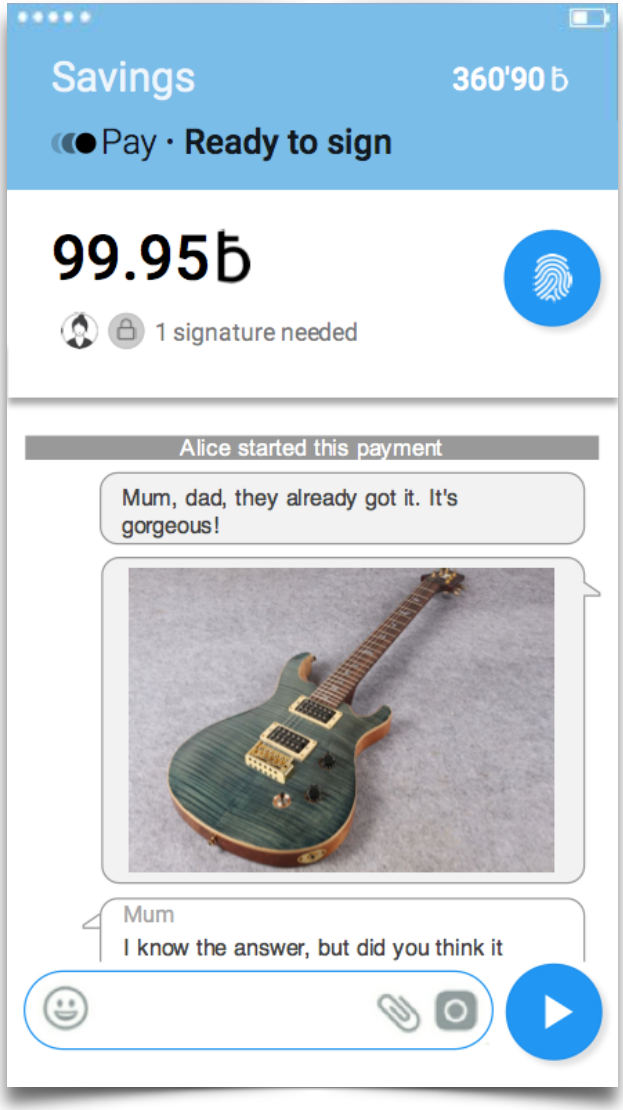


First signature

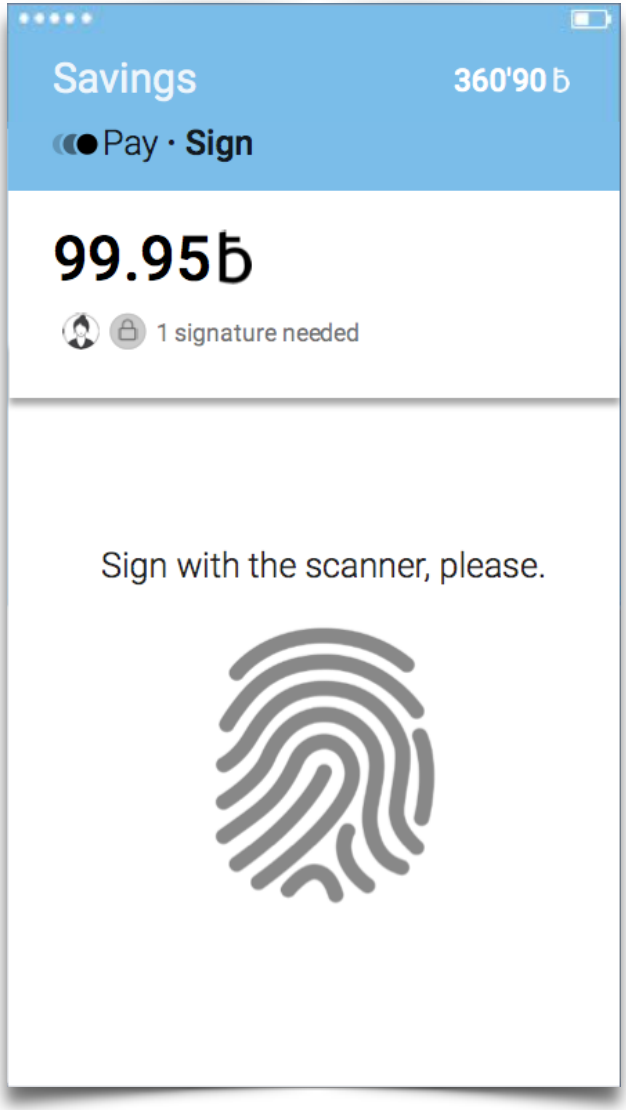
Payment 03

Thinking of the chat as metadata of the transaction opens other rabbit holes. Metadata makes sense of past payments; it helps to understand and improve user's financial decisions. It could also help protecting the user from scams. The wallet could automatically store other data tied to the transaction: GPS location, a picture of the QR code and surroundings, a register of a relevant conversation… you see were this is going? The privacy issues is something that belongs to a wider conversation.

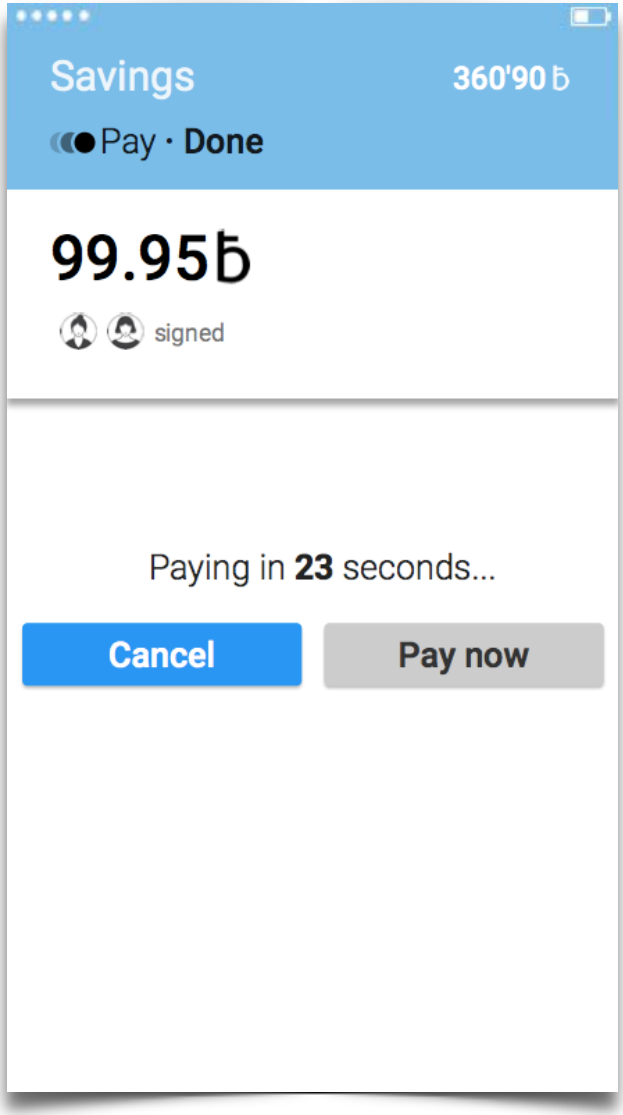
1. The sub-header can collapse to give space when the chat is used.
2. Mum just signed.



Alice swipes up to reveal and press the sign button.



Biometrics may be not safe enough but they are human; passwords are not. Can they be trusted when combined with multi-signature? Are there other solutions? Bash me on this one.



Irreversible actions must always ask for confirmation but this delay feels more natural than the clumsy:

"Are you sure: YES NO"

The payment will be sent in 22, 21, 20…

Thank you for sharing your thoughts!

@luna1999

/99-wallet