System Architecture

Modified bitcoin client which sends API PUSH messages for every newly mined block.

The backend server keeps track of user account balance and any pending transactions. Pending transactions are synced with the full node server. Future-proof so that more currencies can be supported.

Bitcoin Full Node Server

Scala Back-end Server

Notifies server of newly mined blocks and their transactions

Back-end server notifies the node of new transactions to be broadcasted

Mobile Wallet

1*

2*

An wallet application capable of generating new private and public bitcoin keys. communicates with Back-end regarding account balance and transaction statuses.
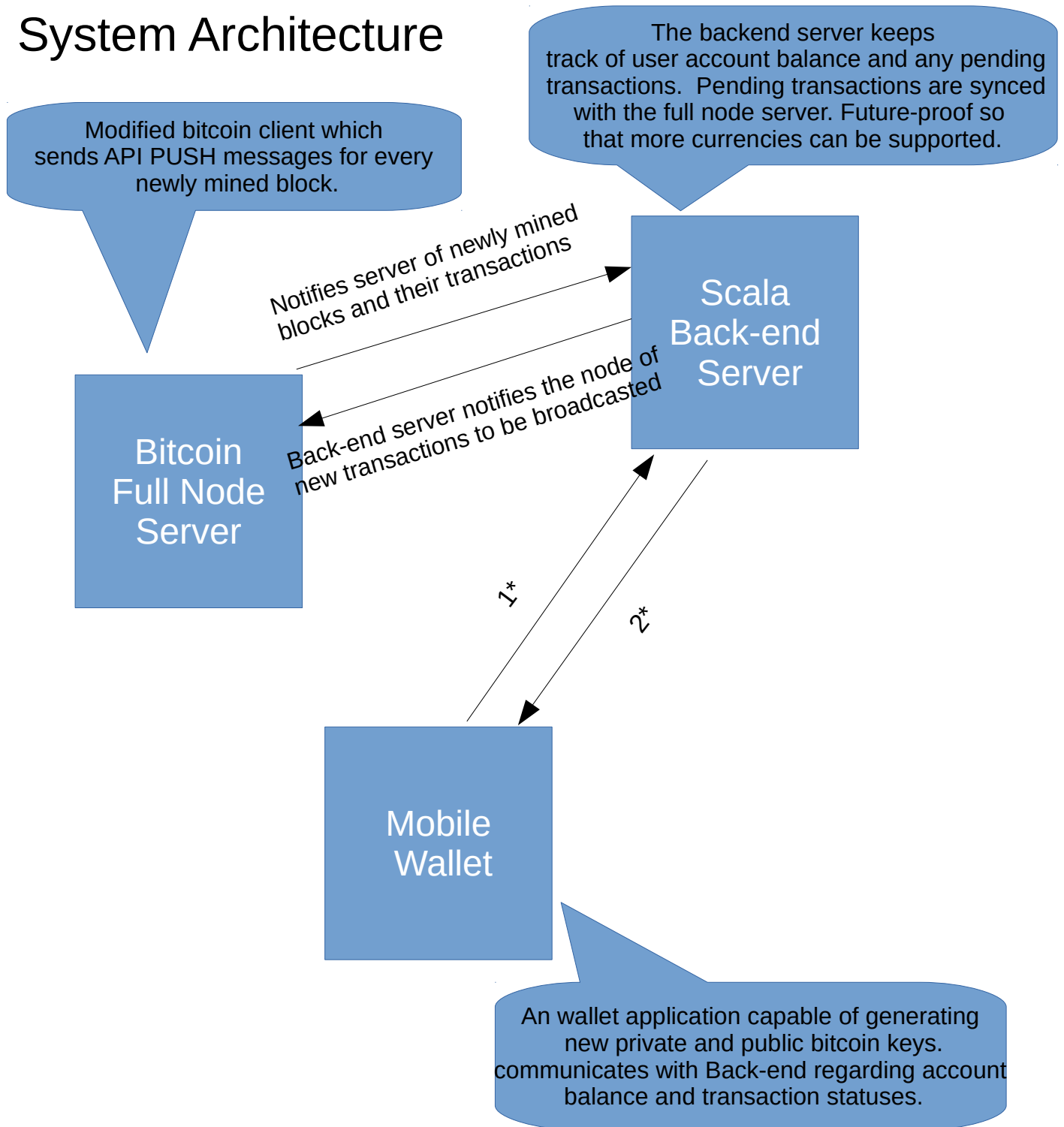
1*: Client does PULL reqeusts regarding: account balance, transaction statuses, initialization of a new payment (so that full payment information can be displayed by the phone wallet).

2*: Client sends PUSH requests during new key generation. Backend server is notified about new public keys and the hash of the private key so that only one account can be associated with the given private key. Client also sends PUSH requests when committing/signing a new transaction (the signed transaction is sent to back-end server so that the account balance can be deducted and so that the new transaction can be broadcasted.