Philanthropy on the Blockchain

Danushka Jayasinghe, Sheila Cobourne, Konstantinos Markantonakis, Raja Naeem Akram, Keith Mayes

Philanthropy On The Blockchain

Danushka Jayasinghe, Sheila Cobourne, Konstantinos Markantonakis, Raja Naeem Akram and Keith Mayes

Smart Card & IoT Security Centre, Information Security Group,
Royal Holloway, University of London, Egham, Surrey, UK, TW20 0EX
{Danushka.Jayasinghe.2012, Sheila.Cobourne.2008}@live.rhul.ac.uk,
{K.Markantonakis, R.N.Akram, Keith.Mayes}@rhul.ac.uk

Abstract. One of the significant innovations that came out of Bitcoin is the blockchain technology. This paper explores how the blockchain can be leveraged in the philanthropic sector, through charitable donation services in fiat currency or Bitcoin via a web-based donor platform. The philanthropic model is then used for a case study providing humanitarian aid for a community living in a challenging geographical environment with limited internet availability. An SMS based mobile payment system is proposed for provisioning the received donations using the existing GSM network, very basic mobile phones and One Time Password (OTP) security tokens. The proposed scheme is finally evaluated for security while discussing the impact it has on charities and donors.

Keywords: Blockchain, Bitcoin, Rootstock, Philanthropy, Smart Contract, Multi-signatures, Hosted Wallet, SMS, Charity, OTP, Security Token.

1 Introduction

Bitcoin is a decentralised cryptocurrency system which works on a peer-to-peer network, using blockchain technology [8, 18]. Blockchain technology has gained rapid interest due to its decentralised nature and strong security properties [22, 23]. However, blockchains are not limited to decentralised cryptocurrencies, but can also be applied to other innovative ideas such as smart contracts, recording asset ownerships, cross-border payment solutions, trade finance, etc. [21, 22].

A report by the UK Charities Aid Foundation [10] identifies that for charities, blockchains can increase transparency, openness and trust whilst reducing transaction costs and providing new opportunities for fundraising. We explore this by introducing a generic blockchain based philanthropic model that uses a web-based donation platform where donors can choose which charity projects to support, through donations in Bitcoin or fiat currency [17]. In the proposed scheme, the charity will maintain hosted Bitcoin Wallets for registered users: back-end payments are done via multi-signature Bitcoin transactions to enhance security: more advanced services can be offered using Smart Contracts via the Rootstock platform [2]. This allows the charity to provide feedback on how each individual donation was used (donation transparency), along with secure, cheap and speedy transactions and an infrastructure that can be used for donation provisioning. This generic philanthropic model is then applied to financial aid distribution in offline geographical environments such as warzones, disaster areas and economically deprived areas of the world where the basic technological infrastructure necessary for a blockchain solution is not available. In these challenging conditions, conventional internet-based money transfer may not be possible and physical cash handling may be fraught with danger. Using our solution, Bitcoin payments can be done using basic mobile phones, an SMS mobile payment system utilising an existing GSM network and low-cost security tokens.

The main contributions of the paper are: 1) a new philanthropic model that leverages the Bitcoin blockchain/ Smart Contract Platform for charitable donations/ provisioning and 2) an SMS based Bitcoin mobile payment system that can be used in an offline environment. The paper is structured as follows. Benefits of Blockchains are identified in Section 2. Our philanthropic model is introduced in Section 3, and in Section 4, this is applied to a use case of humanitarian aid in a disconnected environment. The proposed scheme is evaluated in Section 5, and the discussion is concluded and future research directions outlined in Section 6.

2 Benefits of Blockchain Solutions for Charities/ Donors

Blockchain solutions can provide advantages when used in conjunction with charitable giving [10, 11, 15]. For example, the Royal National Lifeboat Institution (RNLI) in the UK has accepted Bitcoin since August 2015 [7]. BitGive Foundation's (GiveTrack) allows donors to trace Bitcoin transactions (donations) in real time [5] Bitcoin solutions can benefit both charities and donors as follows:
1. Donation transparency: by using Bitcoin addresses for donations there is a publicly available audit trail detailing exactly where a particular donation went.
2. Reducing transaction costs: Low International transaction fees are a feature of blockchain payments as seen in Table 1. Bitcoin Currency (BTC), United States Dollar (USD), Great British Pound (GBP).

Table 1. Comparison of transaction fees

Transaction Method	**Fee BTC**	**Fee USD**	**Fee GBP**	**Speed**
Bitcoin(average 645 bytes)[a]	0.0001	\$0.25	£0.20	roughly 50 minutes [9]
Western Union[b]	-	\$14.83	£8.90	less then 1 hour
Western Union[b]	-	\$11.50	£6.90	next day
MoneyGram[b]	-	\$16.50	£9.90	less then 1 hour
Ria[b]	-	\$10.00	£6.00	same day

[a] Bitcoin transaction fees are calculated on transaction size, not monetary value [8].
[b] Based on remittance transfer of 120 GBP from the United Kingdom to Uganda [20].

3. Donation speed: All Bitcoin transactions are broadcast immediately. Each transaction that is included in a valid mined block and added to the blockchain is called a confirmation which takes just over seven minutes [8, 9]. With each subsequent block mined, the number of confirmations for that particular transaction increases by one. It is common practice to wait until at least six confirmations [18], taking roughly fifty minutes [9]. Some transactions could be considered to be complete after only one or two confirmations. This is fast compared to existing methods which could take several days [23]: see Table 1.

4. Donation provisioning: Provisioning the donations to beneficiaries can be challenging. For example, humanitarian financial aid distribution in warzones can be hindered if the country's banking system is subject to sanctions. Bitcoin payments bypass the banking system and donations can reach their intended target, without requiring the charity to transport large amounts of cash [10].

3 The Blockchain Philanthropic Model

We propose a system where a donor can make their donation in Bitcoin via a Donor Platform. Each charity/project on the donor platform has a Bitcoin address, with the 'granularity' ranging from one Bitcoin address per project through to a central Bitcoin address for the charity. These standalone Bitcoin addresses can be funded by donors using a standard pay to address (Pay To Public Key Hash) Bitcoin transaction. Bitcoin donors can use any Bitcoin wallet/client to donate, or use fiat currency that gets converted to Bitcoin automatically by using an online exchange. Once a donation is made, the donor can query the blockchain to see whether the donated funds have been used or not. The charity then uses the donations to allocate financial aid to individual beneficiaries. Beneficiaries can then perform Bitcoin transactions for day-to-day activities.

3.1 Bitcoin Transaction Methods

We propose that donations can be used by the charity for donation provisioning and subsequent SMS payment processing via one of two Bitcoin payment methods: Multi-Signature Addresses and Smart Contracts.

Option 1: Multi-Signature Addresses are derived using a multi-signature process, where more than one private key is needed to authorise a transaction. For example, a 2-of-3 multi-signature is when a Bitcoin address is associated with three private keys and at least two out of the three private keys are needed to authorise a Bitcoin transaction. In our proposal, we use 'Pay To Script Hash' (P2SH) transactions to process multi-signatures. To generate a multi-signature, a Full Redeem Script which includes details of the three public keys is hashed to generate a hashed Redeem Script which becomes the P2SH multi-signature. The Full Redeem Script is shared between all key-holding entities. The Redeem Script can be used to verify the transferred amount and whether its being sent to the correct multi-signature address. It also gives details about how many signatures are needed to make a payment. The recipient needs to provide the full redeem script to spend the received Bitcoins.

Option 2: Smart Contracts can be defined as a set of instructions represented in computer code published on a distributed network, that receives inputs, executes instructions and provides outputs. It can enable a charity to offer additional features such as: routine provisioning of donations when beneficiaries are low in cash, issuance of small micro-finance loans, record keeping, donation requests to donors and automatic audit reports of a charity activity. Running advanced smart contracts on the Bitcoin network is not possible, however, a suitable platform would be Rootstock (RSK) [2], which is a sidechain that is based on a 2-Way peg mechanism. The 2-Way peg is a method to convert BTC into Smart Bitcoin Currency (SBTC) and vice-versa. When a user intends to convert BTC to SBTC, some BTC are locked in Bitcoin and the same amount of SBTC is unlocked in RSK and vice-versa [2]. Provisioning of donations, payments between beneficiaries and transaction fees to execute instructions are paid using SBTC. The smart contract is then published in the RSK network i.e. the contract exists on every node joining the network, including miners. To execute an instruction in the smart contract, the charity broadcasts a message to the RSK network. A small transaction fee is paid for this process ("Gas"). A smart contract can be instructed to receive two or more signatures (similar to multi-signature functionality) via programmable logic before a transaction can be executed and broadcast to the peer-to-peer network.

4 The Philanthropic Model in an Offline Environment

Blockchain based schemes have constraints, such as requiring Internet and compatible devices: computers, tablets or smart phones that can perform cryptographic processes. People in a geographical area without reliable Internet facility would find it difficult to use the hosted wallet based transactions. There is more GSM network coverage than Internet access in most countries around the world [16], and the use of mobile phones within the GSM network coverage is considerably higher compared to other communication technologies [16], so this points us to consider an Short Message Service (SMS)-based solution.

4.1 SMS Payments and Bitcoin

SMS m-payment systems have been extremely successful in the developing world, most notably M-PESA in Kenya [6]. The SMS approach has been extended to perform Bitcoin transactions [1,3]. However, all these schemes require the user to have initial online access to set up and maintain their Wallet. Attempts to integrate Bitcoin directly with M-PESA in Kenya have largely been unsuccessful due to business pressures [24]. Other proposals need smartphone apps to interact with online Bitcoin wallets e.g. BTC Wallet [12]. As none of these existing solutions is suitable, we propose a novel SMS based mobile payment system which acts as a gateway to transact with the blockchain, using Bitcoin wallets hosted on beneficiaries' behalf by the charity (Hosted Wallet). Offline beneficiaries can then make and receive Bitcoin payments using SMS messaging on basic mobile phones along with a One Time Password (OTP) security token, that provides some assurance that only a genuine user can send an SMS to make a transaction.

4.2 Security Requirements and Adversarial Model

The proposed scheme must satisfy the following security requirements. **Confidentiality**: sensitive information should not be disclosed to unauthorised parties. **Integrity**: information must not be tampered with by unauthorised parties. **Authentication**: all participants in a transaction must be authorised and all transaction data must be genuine. **Non-repudiation**: none of the participants

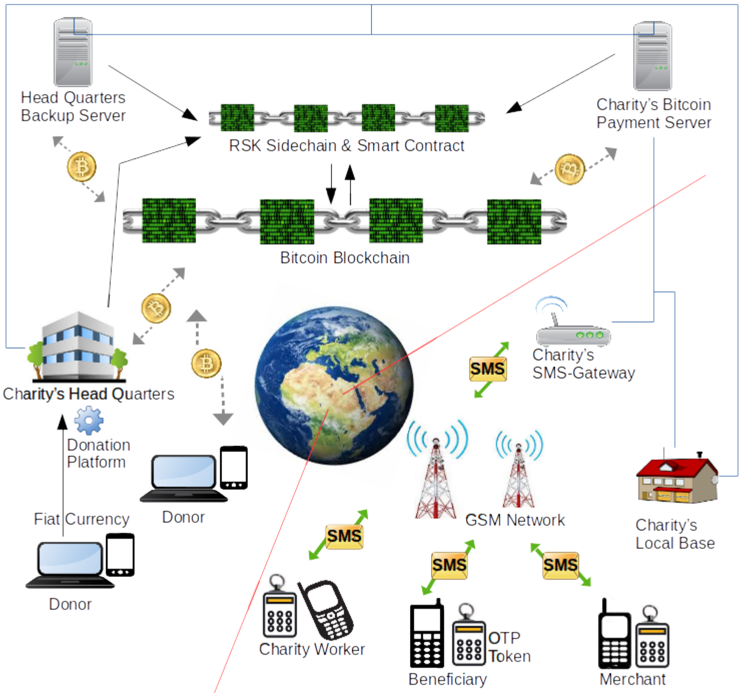

Fig. 1. Philanthropic Model and SMS Payment System Architecture

in a transaction can subsequently deny taking part in it. **Availability**: services should not be denied to authorised users (distributed denial of service - DDoS).

In a humanitarian aid setting, the adversarial model is as follows [14]. **State Level Attackers (SL):** high levels of skill/resources, employed by government agencies to attack commercial/government systems. State sponsored cyber attacks on humanitarian operations have been recorded. **Cyber Criminals (CC):** are organised groups who attack systems for money, who also have high levels of skill and resources. **Hacktivists (Ha):** have moderate skills and resources and use digital tools to mount attacks for ideological reasons. **Insiders (In):** may have low levels of technical skill and resources, corrupt users, charity workers or merchants can be particularly dangerous if they have privileged access to data.

4.3 Proposed SMS-Based Bitcoin Payment Scheme

The charity creates Hosted Wallets for beneficiaries, and during a secure registration process at the local office, issues OTP tokens that will be used to make payment requests. Our proposal involves interactions between a number of entities, described below: the relationship between entities is illustrated in Figure 1.

Bitcoin Payment Server (BPS): manages hosted Bitcoin Wallets on behalf of beneficiaries, securely holds Bitcoin keys for each account holder and is connected to the Bitcoin/RSK peer-to-peer network. **Charity Local Office (LO):** located at the disconnected environment, registers phone numbers of users and manages distribution of OTP tokens. **Charity Head Quarters (HQ):** geographically distant from the aid environment, and has online access/secure servers: the HQ holds relevant Bitcoin private keys for all payers. **Charity Head Quarters Backup Server (HQB):** backup server which also holds relevant Bitcoin private keys for all payers. **One Time Password (OTP) Token:** cheap Hash-based One Time Password (HOTP) security token used with every SMS transaction. **SMS-Gateway:** server that sends and receives SMS transmissions[1] to and from the telecommunication network, and is connected to the BPS. Additionally, we make the following assumptions: **Charity Head Quarters (HQ):** The charity operates on an international level while providing humanitarian aid for offline beneficiaries. It is a reputable and trusted entity, with secure premises and online access/ backup servers which may be geographically distant from the aid environment. **Donors:** Potential donors must have online access to use the donor platform. **Donor Platform:** Hosted on a secure web server adhering to industrial standard security controls to prevent attacks (such as: Denial of Service, website defacing, content manipulation, etc.). **Bitcoin Payment Server (BPS):** Secure server managed under industrial standard security controls to prevent attacks. All security keys are kept encrypted and stored securely to minimise the risk of data breaches. **Phones:** All users of the system possess simple mobile phones ('feature phones') that are protected by security code/access PINs, and the local existing GSM network can be used for SMS messages. **Secure Registration:** At the LO, all users of the system must register their mobile numbers and be issued with cheap Hash-based One Time Password (HOTP) security tokens. Mobile numbers are assigned an OTP identifier and Bitcoin wallet. All registration details are sent to the BPS (encrypted using the LO's private key), in batches if the LO's internet connection is intermittent

Security Token: This is a cheap hardware security token that generates HMAC-Based (HOTP) passcodes when the user requests ("event-driven"). These codes remain valid until used by the authenticating application. Typical OTP lengths are 8 digits or 6 alphanumeric characters, and are generated by standardised algorithms e.g RFC4226 [19]. The BPS can generate a user's transaction OTP using the same algorithm. **Trust:** SMS-Gateway and BPS are trusted & secure. Mobile phones are not. **Bitcoin wallet addresses:** All the Bitcoin wallet addresses and Bitcoin transactions use a 2-of-3 multi-signature process. The key holding entities are the BPS, charity HQ and HQB. So when the BPS receives a payment request, it cannot broadcast a valid Bitcoin transaction to the Bitcoin peer-to-peer network without it being authorised by one of the other keyholders.

4.4 Processing a Bitcoin Payment Request

Payments can be made from charity worker to beneficiary, beneficiary to merchant, or merchant to merchant [2] , and the message flow is shown in Figure 2. The notation used is shown in Table 2, security credentials for each entity are shown in Table 3 and the content of each SMS messages used is shown in Table 4. For simplicity of exposition, the following description shows the Head Office (HQ) providing the second Bitcoin key.

[1] All SMS messages used in the proposal are within the standard 160 character length.

[2] Merchants could use an existing Bitcoin address, registered and associated with a short Merchant ID by the BPS, used instead of Ph_P/ Ph_R in transactions.

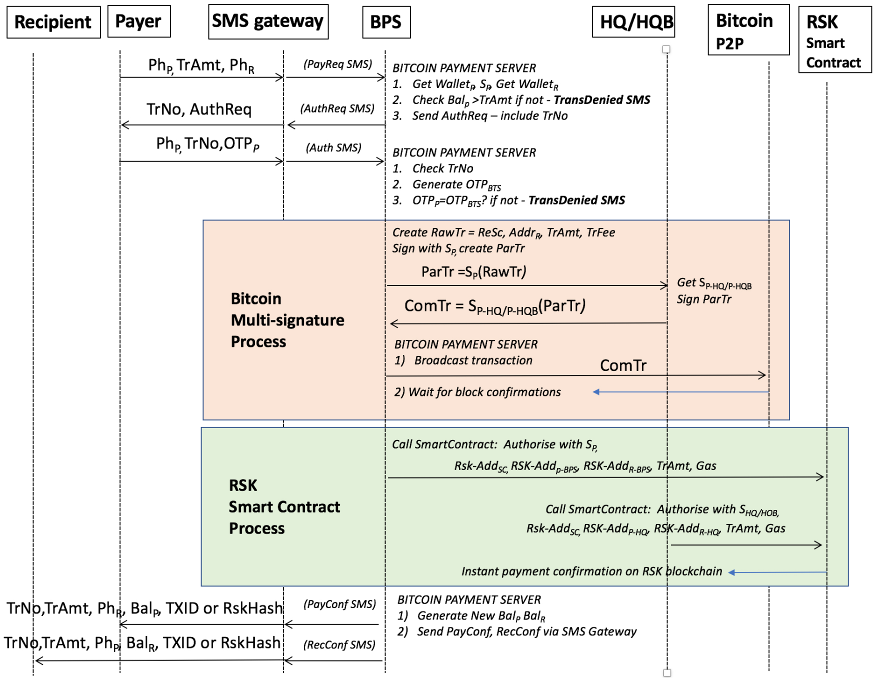
Recipient
Payer
SMS gateway
BPS
HQ/HQB
Bitcoin P2P
RSK Smart Contract
Ph_P, TrAmt, Ph_R
(PayReq SMS)
BITCOIN PAYMENT SERVER
1. Get $Wallet_P$, S_P, Get $Wallet_R$
2. Check Bal_p >TrAmt if not - **TransDenied SMS**
3. Send AuthReq – include TrNo
TrNo, AuthReq
(AuthReq SMS)
Ph_P, TrNo,OTP_P
(Auth SMS)
BITCOIN PAYMENT SERVER
1. Check TrNo
2. Generate OTP_{BTS}
3. OTP_P=OTP_{BTS}? if not - **TransDenied SMS**
Bitcoin Multi-signature Process
Create RawTr = ReSc, $Addr_R$, TrAmt, TrFee
Sign with S_P, create ParTr
ParTr =S_P(RawTr)
Get $S_{P-HQ/P-HQB}$
Sign ParTr
ComTr = $S_{P-HQ/P-HQB}$(ParTr)
BITCOIN PAYMENT SERVER
1) Broadcast transaction
ComTr
2) Wait for block confirmations
RSK Smart Contract Process
Call SmartContract: Authorise with S_P,
$Rsk\text{-}Add_{SC}$, $RSK\text{-}Add_{p\text{-}BPS}$, $RSK\text{-}Add_{R\text{-}BPS}$, TrAmt, Gas
Call SmartContract: Authorise with $S_{HQ/HOB}$,
$Rsk\text{-}Add_{SC}$, $RSK\text{-}Add_{P\text{-}HQ}$, $RSK\text{-}Add_{R\text{-}HQ}$, TrAmt, Gas
Instant payment confirmation on RSK blockchain
TrNo,TrAmt, Ph_R, Bal_P, TXID or RskHash
(PayConf SMS)
TrNo,TrAmt, Ph_P, Bal_R, TXID or RskHash
(RecConf SMS)
BITCOIN PAYMENT SERVER
1) Generate New Bal_P Bal_R
2) Send PayConf, RecConf via SMS Gateway

Fig. 2. SMS Payment Message Flow

Table 2. Notation used in Proposed SMS Payment Scheme

Notation	Description
$Addr_X$	Bitcoin Multi-signature Address for entity X
BPS / Ph_X	Bitcoin Payment Server(entity) Phone Number of entity X
BAL_X	Bitcoin balance in Account AC_X for entity X
E_K(Z) / X→Y	Encryption of data Z with key K / Message sent from X to Y
HQ / HQB	Head Quarters (entity) / Head Quarters Backup Location (entity)
LO / P / R	Local Office (entity) / Payer(entity) / Recipient(entity)
OTP_X	One Time Password generated by entity X
PK_X/ SK_X	Public/ Secret Key pair of entity X
S_X / $TrHash$	Bitcoin Private Key of entity X (signing key) / Transaction Hash
$TrAmt$ / $TrNo$	Transaction Amount / Transaction Number
$TXID$	Unique Transaction ID of a transaction recorded in the blockchain. Also referred to as the Transaction Hash (TrHash)
(Z)$Sign_K$	Signature on data Z with signature key K
$TrFee$	Transaction Fee paid to the Bitcoin miner
$RawTr$	Raw Transaction created for signing
$ParTr$	Partial Signed Transaction created after signing $RawTr$
$ComTr$	Complete Signed Transaction created after signing $ParTr$
$ReSc$	Full Redeem Script used for the Bitcoin multi-signature address
$RSKHash$	Rootstock Transaction Hash
$RSK\text{-}Add_{SC}$	RSK Smart Contract Address, unique for the contract and never changes
$RSK\text{-}Add_{X-Y}$	RSK public key (RSK address) of entity X kept securely with entity Y
$S_{RSK-X-Y}$	RSK private key of entity X kept securely with entity Y
Gas	Transaction fee paid to execute instructions on the smart contract

Stage 1: Payment Request: to make a payment, the Payer (P) types an SMS with payment instructions (*PayReq SMS*), and sends it to a local phone number provided by the charity, to be forwarded to the charity's BPS via the SMS-Gateway. The BPS retrieves Bitcoin wallets for both Payer and Recipient, checks *TrAmt* is not greater than BAL_P, pseudo-randomly generates a three-digit number, unique per transaction *TrNo*, and then sends *AuthReq SMS* asking for Payer's OTP. The Payer presses a button on the OTP token, then sends *Auth SMS* containing the resulting OTP to authorise the transaction. The BPS checks the TrNo, generates OTP_{BPS} and compares to the received OTP_P. If any checks fail, *TransDenied SMS* is sent to the Payer. If all checks are passed then the BPS proceeds to making a Bitcoin payment, using one of the two proposed options.

Stage 2: Bitcoin Transaction Processing

Option 1: Multi-signature Process: The BPS first generates a Raw Transaction (*RawTr*) which includes the Full Redeem Script (*ReSc*), the new multi-signature address associated for the receiver where the payment is going to, *TrAmt* and *TrFee*. The *RawTr* then needs to be signed by minimum 2 participants in turn to generate a valid Bitcoin transaction. The BPS first signs the *RawTr* using the corresponding Payer private key S_P and forwards the Partial Signed Transaction (*ParTr*) to the HQ for signing.
BPS→HQ: ParTr = $(ReSc, Addr_R, TrAmt, TrFee)Sign_{S_P}$

To authorise the payment request, HQ first verifies the *ParTr* to check the payment amount and number of signatures needed. Once satisfied, HQ signs this using its private payer Bitcoin key S_{P-HQ} to generate the Complete Signed Transaction *ComTr* and sends this back to the BPS.
HQ→BPS: ComTr $=(ParTr)Sign_{S_{P-HQ}}$

The BPS then broadcasts the *ComTr* to the Bitcoin peer-to-peer network. Once broadcast, a unique transaction-id (TXID) or the recipient's Bitcoin address can be used to trace the transaction on the blockchain. The Bitcoin miner who first publishes the valid block in the blockchain that also includes our Bitcoin transaction is paid the *TrFee* for the payment. This is the first confirmation for the transaction. The BPS then waits for the transaction to be confirmed in the agreed number of blocks before generating the SMSs.

Option 2: Smart Contract Process: The BPS calls the Smart Contract and authorises the *TrAmt* and the *Gas* is paid by using the $S_{RSK-P-BPS}$.
BPS→RSK: $RSK\text{-}Add_{SC}, RSK\text{-}Add_P, RSK\text{-}Add_R$, *TrAmt*, *Gas*

Once the message gets broadcast in the RSK network, the HQ or the HQB calls the smart contract which act as the second set of instructions needed by the smart contract to execute the transaction. HQ/HQB uses the $S_{RSK-P-HQ/HQB}$ to authorise the paid amount *TrAmt* and the transaction fee *Gas*.
HQ/HQB→RSK: $RSK\text{-}Add_{SC}, RSK\text{-}Add_{P-HQ}, RSK\text{-}Add_R$, *TrAmt*, *Gas*

Table 3. Credentials Used in Proposed SMS Payment Scheme

Entity	**Keys and Other Assets**
Payer/ Recipient	No keys, PIN for phone, HOTP token (no PIN) for making payments
BPS	S_{P-BPS},$Addr_{P-BPS}$, $Addr_{R-BPS}$, PK_{LO}, Ph_X, OTP_X
HQ	S_{P-HQ}, S_{RSK-HQ}, ReSc
HQB	S_{P-HQB}, $S_{RSK-HQB}$, ReSc
LO	SK_{LO}, Physical OTP tokens, phone numbers (payers/recipients), plus registration details/ OTP allocation details
Donor	S_{Donor}/ V_{Donor}
Donor Platform	$Addr_{Project}$

Table 4. SMS Payment Messages

Message	**Content**
PayReq SMS	Ph_P, TrAmt, Ph_R
AuthReq SMS	TrNo, AuthReq
Auth SMS	Ph_P, TrNo,OTP_P
TransDenied SMS	Ph_P, TrNo, Ph_R, Denied
PayConf SMS	TrNo,TrAmt, Ph_R, BAL_P, TXID
RecConf SMS	TrNo,TrAmt, Ph_P, BAL_R, TXID
PayConfRSK SMS	TrNo,TrAmt, Ph_R, BAL_P, RskHash
RecConfRSK SMS	TrNo,TrAmt, Ph_P, BAL_R, RskHash

When instructions are received from both BPS and HQ/HQB, the Smart Contract executes a transaction to transfer the value *TrAmt* to the recipient. The unique transaction details are recorded instantly on the RSK blockchain in the format of a hash (RskHash). The BPS does not need to wait for a transaction confirmation as there is instant confirmation when using the RSK platform.

Stage 3: Payment Finalisation: Once the payment is done, the BPS updates the payer/recipient balances and sends confirmation messages via the SMS-Gateway: *PayConf SMS* or *PayConfRSK SMS* to the Payer and *RecConf SMS* or *RecConfRSK SMS* to the Recipient. TXID/RskHash are included as unique IDs that can be used to trace the transaction on the Bitcoin/RSK blockchains.

5 Analysis

In this section, we discuss SMS security and analyse the proposal against security requirements shown in Section 4.2. A summary of targets that adversaries may attack along with suggested countermeasures is shown in Table 5.

SMS Security Issues: SMS messages are not encrypted by default and the SMS service is vulnerable to man-in-the-middle attacks and spoofing [4]. Attack methods include interception/redirection using false base stations in GSM networks, eavesdropping at the Short Message Service Centre (SMSC), and SS7 hacking [13]. Adversaries who might target the SMS system are *SL*, *CC* and *In*, aiming to create fraudulent transactions. Although these issues are not addressed directly in our proposal, measures have been included which provide some deterrent to would-be attackers. The use of the OTP means that replay

Table 5. Attack Targets, Adversaries and Countermeasures

Target	**SL**	**CC**	**Ha**	**In**	**Countermeasure**
Donor Platform	y	y	y		Hosted on a secure web server adhering to industrial standard security controls to defend against : DDoS, website defacing, content manipulation
HQ/HQB/BPS (DDoS)	y		y		HQ/HQB has secure premises and backup servers: BPS managed under industrial standard security controls and best practices to prevent attacks.
HQ/HQB/BPS (privilege escalation)	y	y		y	Use of security controls such as: access control, routine web-application vulnerability assessment/patching and storing keys encrypted
SMS (MNO/GSM)	y	y			GSM/SMS security issues partially mitigated by OTP 2FA and TXID/RSKhash on confirmations
SMS spoof	y	y		y	OTP/TXID/RSKhash gives some assurance that payment is genuine
SMS replay	y	y		y	OTP prevents replay attacks
Blockchain/RSK (DDoS)	y		y		DDoS attacks not viable in distributed ledger, and integrity is innate in blockchain solutions

attacks will fail, and the *AuthReq SMS* from the charity should alert users to potentially fraudulent transactions. Additional assurance comes from including both *TXID*/*RSKHash* and *TrNo* in confirmation SMSs: these can be used to cross check with the Bitcoin/RSK blockchain and in a verbal comparison between Payer and Recipient respectively, to provide an extra level of assurance that the transaction is correct. These measures provide a higher level of security than other SMS Bitcoin schemes: e.g. in Coinapult SMS, the user sends an SMS containing a security code sent by the payment service in a previous SMS, which offers limited assurance that the transaction is genuine.

Security Requirements

Confidentiality- ***Security of Bitcoin private keys:*** If a Bitcoin private key or Bitcoin wallet is lost or not accessible, then the Bitcoin value recorded to that Bitcoin address cannot be transferred. The 2-of-3 multi-signature process avoids this risk by allowing any two out of the three private key holders to recover the Bitcoins. ***Donor anonymity:*** Anonymous donations may introduce management issues for the charity, as this may need special reporting and investigation due to possible money laundering/fraud regulations. To comply with these, a charity policy may be needed requiring identification for donations over a certain amount. ***Server attacks (HQ/HQB/BPS):*** Adversaries *SL* and *CC* will aim at obtaining keys, transaction data and identity information: *Ha* may wish to find embarrassing data. Table 5 shows recommended countermeasures.

Integrity- ***Blockchain*** ensures the integrity by providing an immutable record of past transactions. ***RSK blockchain*** is mined by the same miners in the Bitcoin peer to peer network. Double-spending prevented by using proof-of-work using SHA256 hashing similar to Bitcoin and uses a checkpointing service provided by a federation of well-known and respected Bitcoin community members [2]. ***Server attacks(HQ/HQB/BPS/Donor Platform):*** the donation platform may be targeted by: *CC* to change published content by replacing the charity's Bitcoin addresses with addresses belonging to the criminals; *Ha* may aim to vandalise the content; *SL* may tamper with it to undermine the credibility of the charity. Transaction records at the BPS may be tampered with by *CC*, *SL* to make fraudulent transactions. ***SMS Replay Attacks:*** countered using the OTP in the *SMSAuth* message. Potential attackers here are *SL*, *CC* and *In*. **Authentication-** ***Authenticating the payment request SMS:*** OTP security tokens are used for two-factor authentication. The charity's BPS authenticates the user by verifying the OTP included in the SMS, so if a phone is lost/stolen, an attacker cannot make a valid transaction. The OTP is valid until it is received and processed by the BPS, so network delays will not cause adverse effects. This should give some protection against spoofing attacks by adversaries *Sl*, *CC* and *In*. ***Mobile Phones:*** The handset's PIN protection will present a barrier to attackers who steal the phone. ***Transaction Number:*** In a point-of-sale transaction, the beneficiary and the merchant can compare the TrNo received on confirmation messages before a purchased product is handed out. ***Social engineering:*** Aimed at obtaining privileged access to data at HQ/BPS, so security awareness training will be needed. However, an insider at the BPS/HQ/HQB is not able to transmit a transaction alone because of the use of multi-signatures. **Availability-** ***Recovering lost Bitcoins:*** If any one of the three Bitcoin private key holders loses their key the remaining two parties can recover the Bitcoins. ***DDoS Attacks:*** The donor platform, HQ/HQB and BPS are an attractive targets for *SL*, *Ha* DDoS attacks: see Table 5 for countermeasures. DDOS on the blockchain are not viable due to its innate security and distributed nature.

6 Conclusion and Future Work

This paper first identified the advantages of blockchains for charities, then discussed how blockchain solutions could be employed, even with their potential constraints. The first contribution is a new philanthropic model that leverages the Bitcoin blockchain. The payment system uses either a 2-of-3 multi-signature transaction process with the Bitcoin network, or a smart contract for advanced functionality utilising the RSK network. The second contribution is an SMS Bitcoin payment system that can be used in an offline environment via the existing GSM network. This proposal was then evaluated against security requirements. It must be noted that, the volatility of Bitcoin exchange value poses a financial risk for the charity. However, in an environment where the banking system/economy may have collapsed, using Bitcoin might be the only viable option. Our solution is aimed at a closed eco-system where payments are made within a constrained geographical environment, thus minimising the effects of Bitcoin price volatility. As a long-term solution to this, the charity may replace the Bitcoin blockchain with a private blockchain solution to give more control over exchange prices. Other future work include a practical implementation of the proposed scheme to identify potential limitations and take timing measurements. Also, we would like to investigate how the philanthropic model could be applied in different situations e.g. when smartphones and Internet connectivity are available or in an ad-hoc network that replaces the existing GSM network.

References

1. Coinapult SMS, https://coinapult.com/sms/info
2. Rootstock platform, http://www.rsk.co/
3. BTC For SMS (2017), http://www.btcforsms.com/
4. FlexiSpy (2017), https://www.flexispy.com/en/features/spoof-sms.htm
5. GiveTrack: Donation tracking (March 2017), https://bitgivefoundation.org/bitcoin-charity-2-0-initiative/
6. M-PESA (December 2016), https://www.safaricom.co.ke/personal/m-pesa
7. Birkwood, S.: Is Bitcoin the ideal charity currency or a cause for concern? (January 2015), http://www.thirdsector.co.uk/analysis-bitcoin-ideal-charity-currency-cause-concern/fundraising/article/1326549
8. Bitcoin.org: Bitcoin wiki (2014), https://en.bitcoin.it/wiki/Main_Page
9. Blockchain.info: Average transaction confirmation time (Visited, November 2016), https://blockchain.info/charts/median-confirmation-time
10. Charities Aid Foundation: Giving Unchained: Philanthropy and the Blockchain
11. Davies, R.: Public Good by Private Means: How philanthropy shapes Britain. Alliance Publishing Trust (2016)
12. Gautham: BTC.com Wallet App (September 2016), http://www.newsbtc.com/2016/09/19/btc-com-wallet-app-sms-bitcoin/
13. Gibbs, S.: SS7 hack explained: what can you do about it? (April 2016), https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls
14. Gilman, D.: Cyber-Warfare and Humanitarian Space (October 2014), http://commstech-hub.eisf.eu/uploads/4/0/2/4/40242315/daniel_gilman_cyberwarfare_and_humanitarian_space_eisf_october_2014.pdf
15. ImpACT Coalition: Through a glass DARKLY: The case for accelerating the drive for accountability, clarity and transparency in the charity sector. Tech. rep. (2013)
16. International Telecommunications Union (ITU): ICT Facts And Figures 2016 (Visited, October 2016), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf
17. Mankiw, N.: Principles of microeconomics, vol. 10. Cengage Learning (2006)
18. Nakamoto, S.: Bitcoin: A peer-to-peer e-cash system. Bitcoin.org (2008), http://www.bitcoin.org/bitcoin.pdf
19. RFC 4226: HOTP: An HMAC-Based One-Time Password Algorithm, December 2005. http://www.ietf.org/rfc/rfc4226.txt
20. The World Bank: Remittance prices worldwide: Third quarter 2016 (Visited, December 2016), https://remittanceprices.worldbank.org/en
21. Walport, M.: Distributed ledger technology: Beyond blockchain. UK Government Office for Science, Tech. Rep 19 (2016)
22. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014)
23. Wright, A., De Filippi, P.: Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664 (2015)
24. Young, J.: Former Kipochi CTO Explains Controversial M-Pesa Deal (January 2016), http://www.newsbtc.com/2016/01/11/former-kipochi-ceo-explains-controversial-m-pesa-bitcoin-deal/