LIFEcoin

SUPPORTING LIVES AND LIVELIHOODS

APRIL 22, 2018

LITA DAS, CONNOR MAKOWSKI, MICHAEL WINDLE

“On the first of the month

The whole family

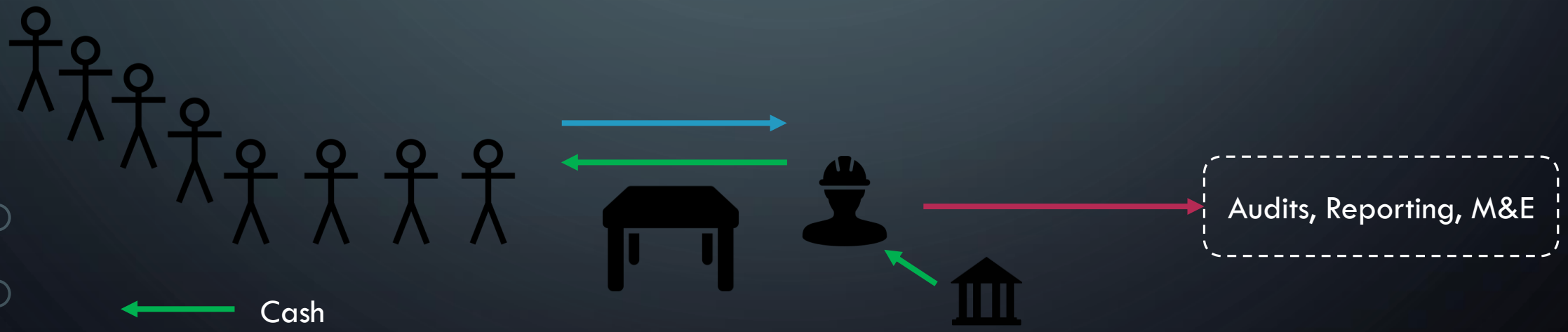
Goes to the city center

Waits in a long line

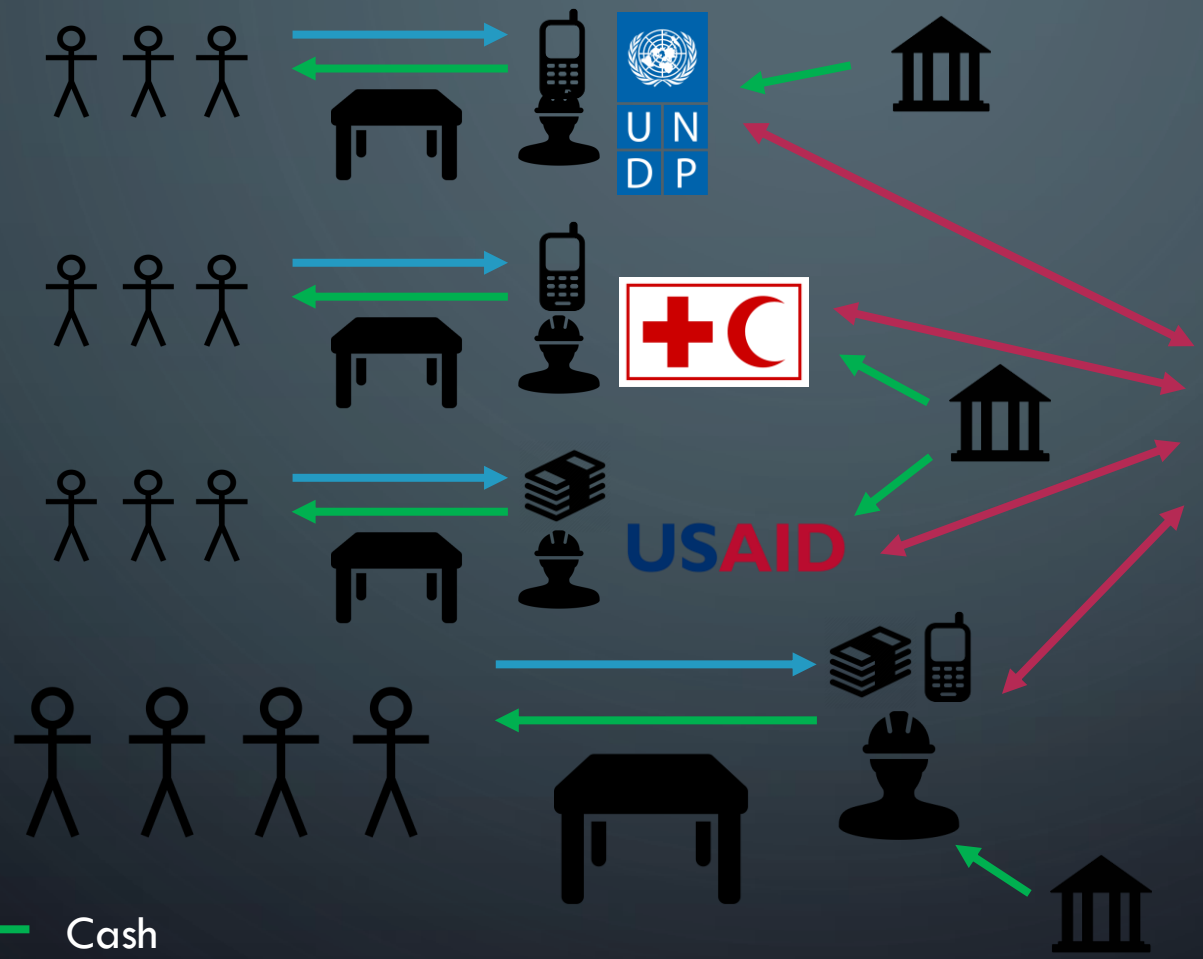
And picks up our cash envelope

Which we use until next month”

SYSTEM SUMMARY – CURRENT STATE



SYSTEM SUMMARY – WITH LIFEcoin



Blockchain Ledger

- Virtual Accounts
- Transaction History
- Balance Info
- Better Audits / M&E

Identify verification by:

- Camp ID Card
- Govt ID Card
- Retina scanning (biometric)

(Anything that can be Hashed/ Salted into a 256 bit string)

Cash

Public Information

Secure Information

CODE DEEP DIVE

- Efficient and Minimalistic Code
  - https://github.mit.edu/conmak/LIFEcoin.git
  - Can be run on any modern computer (with Intel/AMD)
- Key Code components:
  - Anonymous and Secure Data Storage
  - Transactions are Cryptographically Signed and Secure
  - Transactions Validated by all Computers running LIFEcoin
  - LIFEcoin is set up to automatically Block:
    - Overdrawing of Balance
    - Double Spending of Appropriated Funds
    - False Transactions

Current System Extensions:

1. Partial withdrawals
2. Deposits
3. Commodity tracking (tents, NFIs, not just CTPs)
4. Cryptographically integrates with Biometric Identification

```
>>> print (vars(X.Running_Balance))
{'Account_Status': {'-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCdc6lq4X2/IwMNrb6SOzVaw56Y\nVN
qRVkINlyoZI7IH48THXdLzwrRNQC2++VuaQ3lCubLKQ3uznYeR+4qK1G1W8Yfx\nRtYpSLEKje7bYU+w7A6Iq+Oemr+T4RZj5u3+37IjQM+5d+A/6sHUo
pNav4GeVf92\nEJjYujsjnGXcIrVsVQIDAQAB\n-----END PUBLIC KEY-----': 99999999999995000, '-----BEGIN PUBLIC KEY-----\nMIG
fMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCLHO8rLkUPVz2AelK7J39g4Q0K\nRhHvA2cIv2KZVGFj8OEAS3iha9rSROSuN8u6bUOWcZK85oplWtPMBf
diQlG/9cdt\nQ8RcI/5pu0JM+1rs4jE5Q24/xqUCuLvVkuqP4EbgyW8PAatkGFetP8r6OSFeY6ZZ\n5MsZuvgLK1Rbn+BL+wIDAQAB\n-----END PUBL
IC KEY-----': 4980, '-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCiV10Y9mSz7jtlh1Jzh6+JoQmu\nm9
Zxk24ctjrTXCPiFzfy7bZhfs8Z2OvREKic6i6JyE5EnDTTyYFhscMBg9WU2VX9\nfXCq4xaWO06HIfl4BsSjW/CD1SI8soFGjZSCFNQCfX56WwS8AwmF0
vlYZCPq6M1B\nJacVn0mSEbppTRZESwIDAQAB\n-----END PUBLIC KEY-----': 11, '-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQ
EBAQUAA4GNADCBiQKBgQC0CQcU4Hu1AsIG3sWb9FhBukqf\nqVlw9iBXfRa7a7PQeCkQdKGqa3hhDhToSD/R8csbOVXdnp3fHjX7G136+FuFo83J\nqn2
eFzYVRI9WiU9qdqrNTMAZjxzKmVjSmRkazC35YfKbMrI0VWh/NZTQrl1/Xnyt\nz6Bx5qrOcSkuh6/DcwIDAQAB\n-----END PUBLIC KEY-----': 0
, '-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCKF7SAN+lXwEyZlQD/8/RL630m\nRJdPw9V9h+rTF6w77Ice
7QGgzqzBu0SOuM9oP2iacg/soGFbfNKEewct7eruoorL\n97Pm2YvqL4VHT0eafwPEmmH8RFfBmzmU6LDR550Yixi4MvLeDYZWnbiG8aszVXIg\nJQ2oZ
vxp9SxE1LlXTQIDAQAB\n-----END PUBLIC KEY-----': 0, '-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg
QCx4rRO9NL4La1yL8NuY3M3O/Df\nzSkFqAjt05X9oZOZIsnOydC3zSXsWNqFnNdv8684fY7WRdDNlYYHUZ4GcIQ7m26I\n//gUGqoVSPjAUYavuvGh/t
uwreOJetjN6i0VGSdeoXPQFrzSFRr5xWqBfzU2W4ph\nzLa5NA7XmlzTlNqmXQIDAQAB\n-----END PUBLIC KEY-----': 9}}
>>>
```

313 lines (275 sloc) | 13.4 KB

Raw | Blame | History

```
import hashlib
import time
from Crypto.PublicKey import RSA
from Crypto import Random
from Crypto.Hash import SHA512

proof_of_work='000'
digits=len(proof_of_work)

def Read_Private_Key_File(key_location, account_name=""):
    private_key_file = open(key_location+r"\Private_Key_"+account_name+".txt", "r")
    PEM_private_key = private_key_file.read()
    private_key_file.close()
    obj_key=RSA.importKey(PEM_private_key.encode('utf-8'))
    return obj_key

def Determine_My_Public_Key(key_location, account_name=""):
    obj_key=Read_Private_Key_File(key_location, account_name)
    PEM_Public_Key=((obj_key.publickey()).exportKey()).decode('utf-8')
    print ('Public key stored')
    return PEM_Public_Key

class Blockchain:
    def __init__(self):
        self.Chain={}
        self.Balance_Sheet=self.Balances()
        self.Running_Balance=self.Balances()
        self.Recent_Transaction_Blocks=10
        self.Recent_Transactions=self.Recent_Transaction()
        self.Recent_Pre_Block_Transactions=self.Recent_Transaction()
        print ('Blockchain Sucessfully Created!')

    def Initialize(self, Public_Key, Funding_Amount):
        self.Block_ID=1
        Current_Block=self.Block(self.Block_ID)
        Current_Block.Add_To_Donor_Act(self.Initialization_Block(), Public_Key, Funding_Amount)
        Current_Block.Calculate_Nonce()
        Current_Block.Finalize()
        self.Chain[self.Block_ID]=Current_Block
        Next_Block=self.Block(self.Block_ID+1)
        self.Chain[self.Block_ID+1]=Next_Block
        self.Gen_Next_Block()
        Temp_Balance_Sheet=self.Balances()
```

```
>>> import LIFEcoin
>>> from LIFEcoin import Determine_My_Public_Key
>>> from LIFEcoin import Read_Private_Key_File
>>> X=LIFEcoin.Blockchain()
Blockchain Sucessfully Created!
>>> X.Balance_Sheet.Add_Account(r"C:\users\conmak\desktop\HLBC_Keys", "Funds_Account")
Account added to for Funds_Account
>>> X.Generate_Transaction(User1_Public_Key, 10, r"C:\users\conmak\desktop\HLBC_Keys", "Funds_Account")
Transaction Generated
Transaction is valid
Not a duplicate
Submitted in acceptable time frame
User balance is sufficient
Transaction Submitted
>>> X.Generate_Transaction(Org1_Public_Key, 10, r"C:\users\conmak\desktop\HLBC_Keys", "User1_Account")
Transaction Generated
Transaction is valid
Not a duplicate
Submitted in acceptable time frame
User balance is sufficient
Transaction Submitted
>>> X.Generate_Transaction(Org1_Public_Key, 10, r"C:\users\conmak\desktop\HLBC_Keys", "User1_Account")
Transaction Generated
Transaction is valid
Not a duplicate
Submitted in acceptable time frame
Insufficient Balance
>>> X.Add_Block(Org1_Public_Key)
Validation of block sequence passed
Validation of all transactions in block passed
Block Submitted
```

Create the Blockchain

Add an account

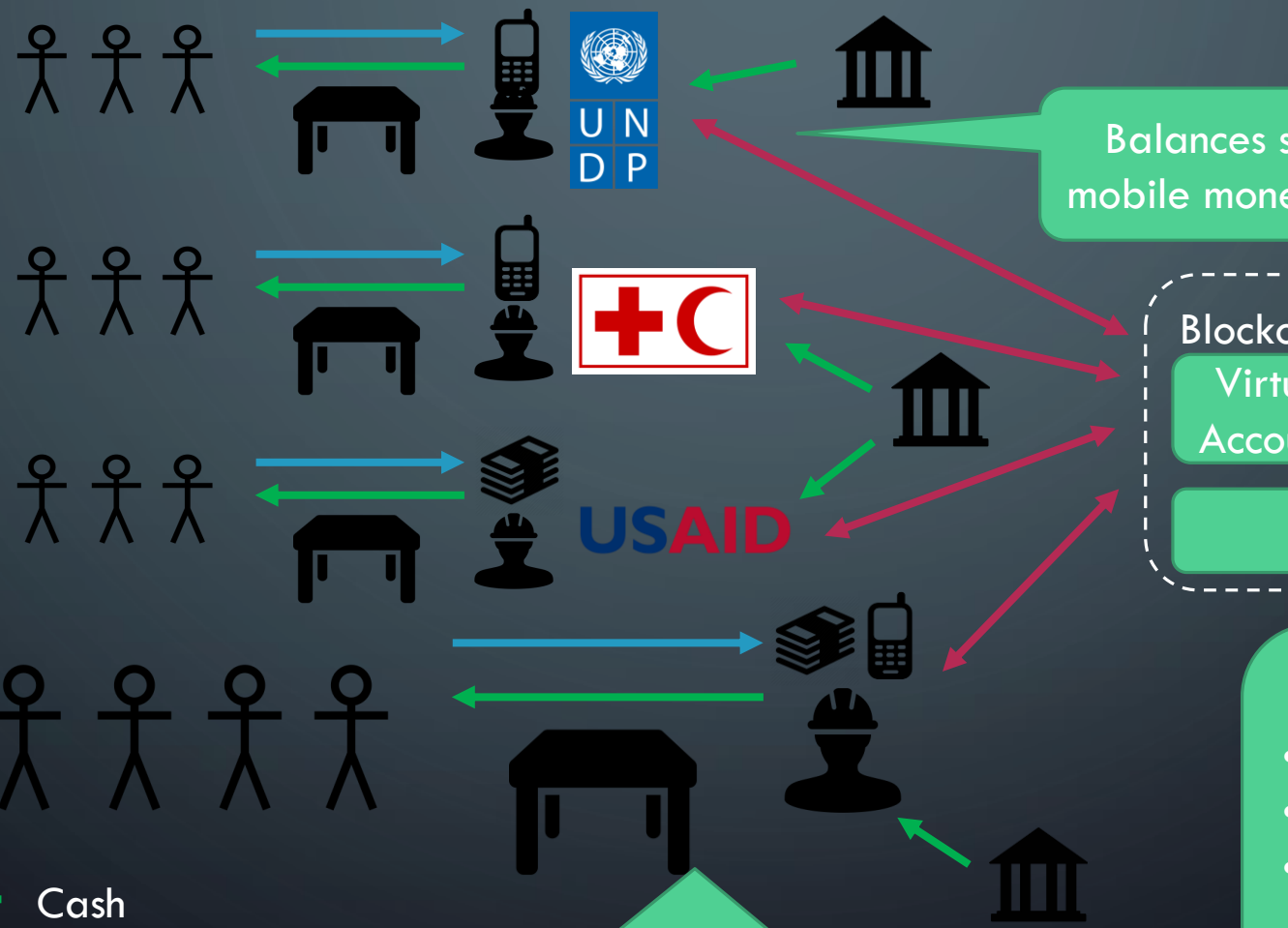
Disperse funds to users' virtual accounts

Allow users to withdraw funds

System prevents double dip

Add Block every minute to ensure consistent records across all computers

SYSTEM SUMMARY – WITH LIFEcoin



Shared virtual account visibility across locations and organizations for simultaneous distribution

Balances support cash and mobile money at each location

Blockchain Ledger

- Virtual Accounts
- Transaction History
- Balance Info
- Better Audits / M&E

Shorter Lines

Identify verification by:

- Camp ID Card
- Govt ID Card
- Retina scanning (biometric)

(Anything that can be Hashed/ Salted into a 256 bit string)

Cash

Public Information

Secure Information

System redundancy if one "table" loses intranet connectivity

FEATURES/BENEFITS WITH LIFEcoin

More efficient programs

Scalable Systems

Reduced Wait Time

Virtual Accounts

Cost Reduction

Integrated Markets

Happier Clients

Improved Personal Finance

Access to Cash

Financial Infrastructure

SYSTEM SUMMARY

BUSINESS MODEL

- Processes for **shorter response time**
- **Secure, accurate** and **trusted** service at low set-up cost
- **Robust** to loss of network connectivity

LEGAL FRAMEWORK[1]

- **Pseudonymization**: data encryption through 256 bit hash
- **Data protection by design:** built into system processes in various ways
- **Data protection officer:** Admin control feature

TECHNOLOGY ARCHITECTURE

- Blockchain (Distributed Ledger)
- Transactional Encryption
- Multi Node Validation

DEPLOYMENT PLAN

- Pilot in existing camps with CTPs
- Rollout using cash
- Subsequently add mobile money, and deposit functionality

1. Pursuant to European Union's General Data Protection Regulation (GPDR)

“On the first of the month

The whole family

Goes to the city center

Waits in a long line

And picks up our cash envelope

Which we use until next month”

"As needed

~~"On the first of the month~~

~~The whole family~~ One person

Goes to ~~the city center~~ any table

Waits ~~in a long line~~ a few minutes

And ~~picks up a set amount of cash~~

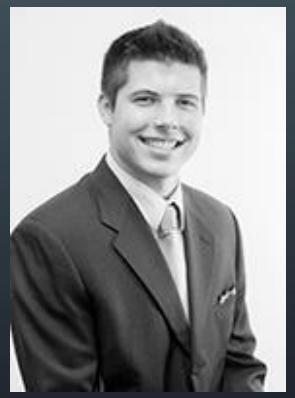
gets some amount of mobile money or cash

Which we use until ~~next month"~~

we want to go back."

Thanks for helping us make cash transfer programs more effective!

Lita



Connor

Michael