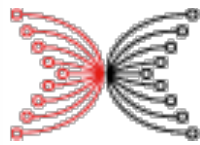


Overview of Blockchain Technology and Collaboration between Tokyo Tech and Industry



INPUT | OUTPUT



Input Output Cryptocurrency Collaborative Research Chair

Mario Larangeira

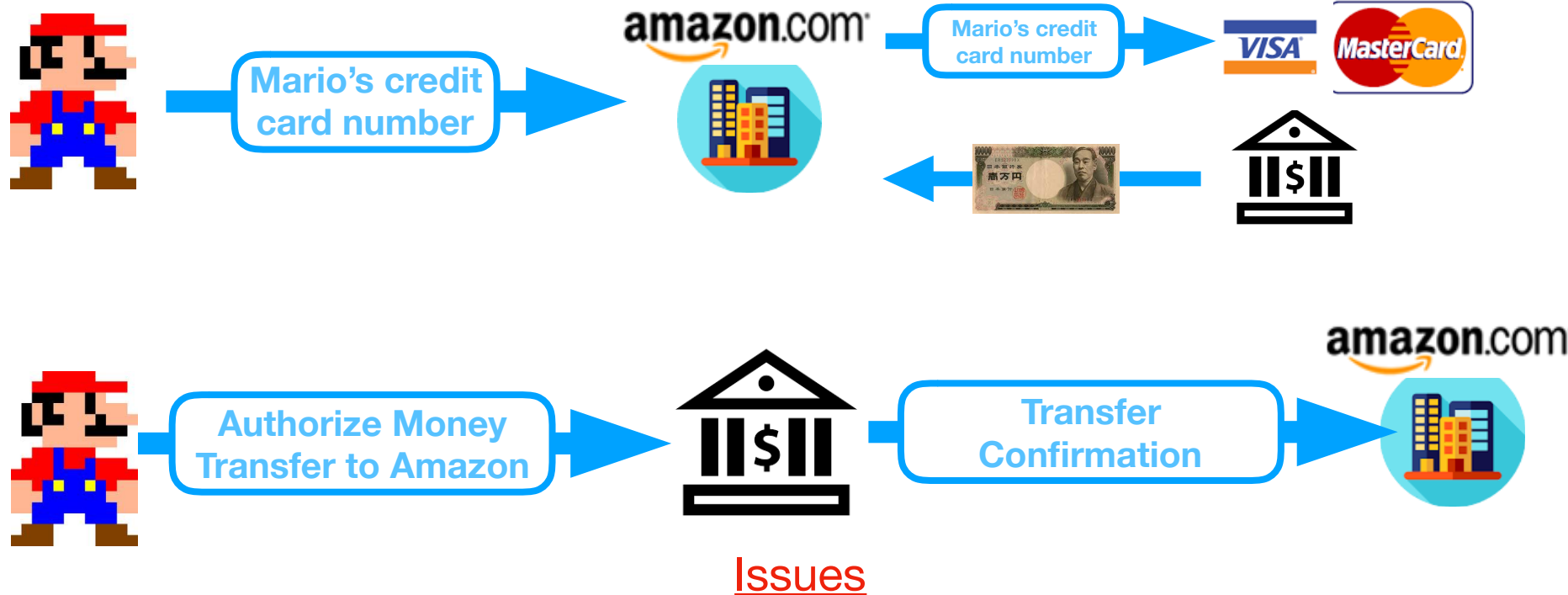
mario@c.titech.ac.jp

Overview

- **Overview of Blockchain Technology**
- **Applications**
- **Tokyo Tech/IOHK Collaboration**

Blockchain Technology

Traditional Digital Transactions



- Trusted party
- Potential High Transactions fees
- No anonymity

Anonymous E-Cash - Digicash

- Chaum's "Blind signatures for untraceable payments" [83] and "Untraceable electronic cash" [88]
- Like Fiat Currency:
 - Anonymous
 - Secure (no double spending or forging)
 - Only banks issue money (e-cash)
 - ...and centralized



"The difference between

*a bad electronic cash system
and well-developed digital cash*

*will determine whether
we will have a dictatorship
or a real democracy"*

(attributed to David Chaum)

Bitcoin Appearance

- October 2008
- Currency: Bitcoin(BTC)
- Fractions: 1BTC = 10^8 Satoshi
- Limited supply: 21 million BTC

Issues previous attempts



- Trusted party
- Transactions fees
- No anonymity
- **No** trusted party
- Low(er) fees
- “pseudonymity”

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Decentralized Ledger

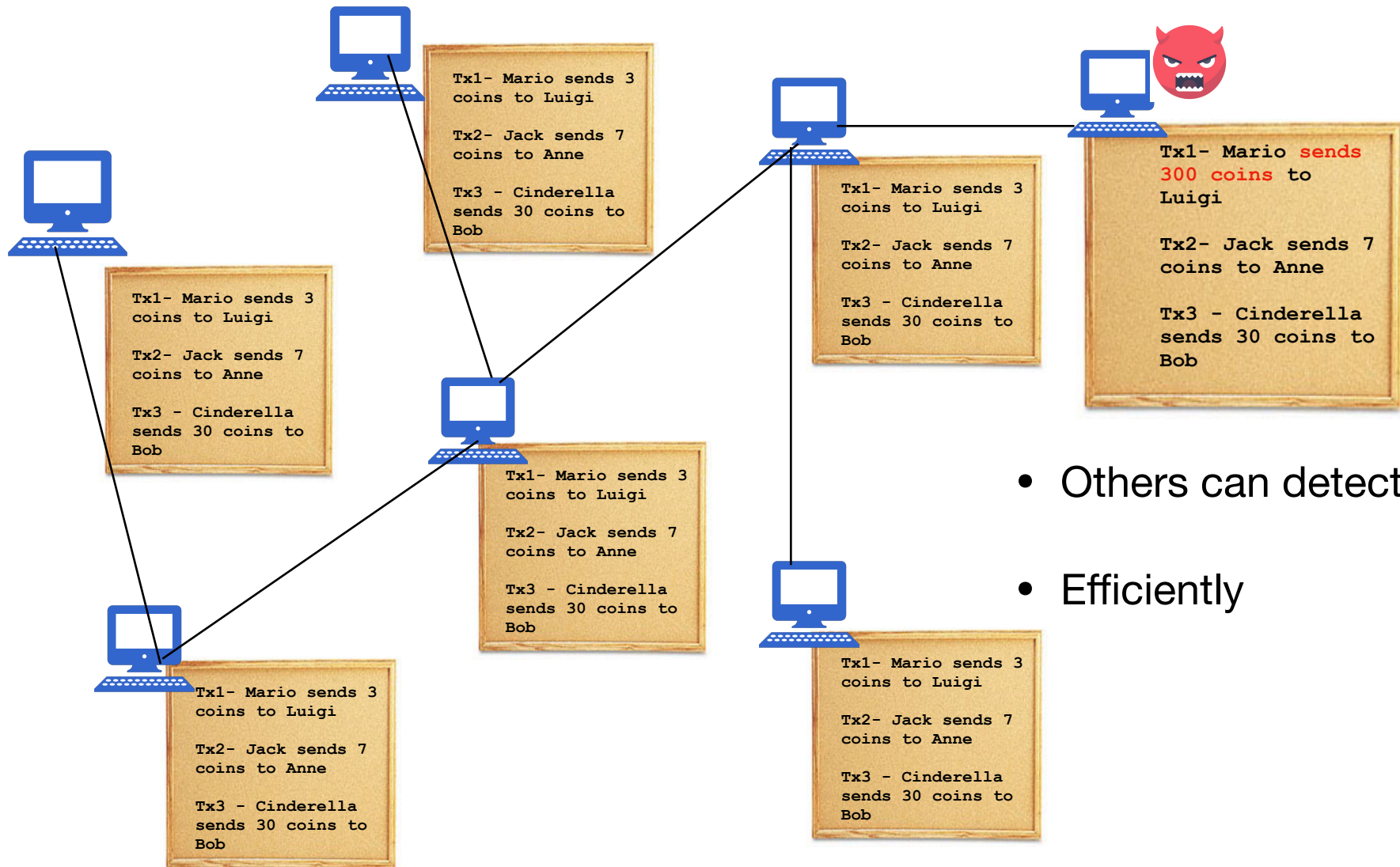
- A data structured kept by mutually distrustful players
- Special properties are needed:
 - Immutable/append only
 - add records: 
 - cannot remove or reorder: 
- Cryptographic **digest**
 - changes would affect the digest

Tx1- Mario sends 3
coins to Luigi

Tx2- Jack sends 7
coins to Anne

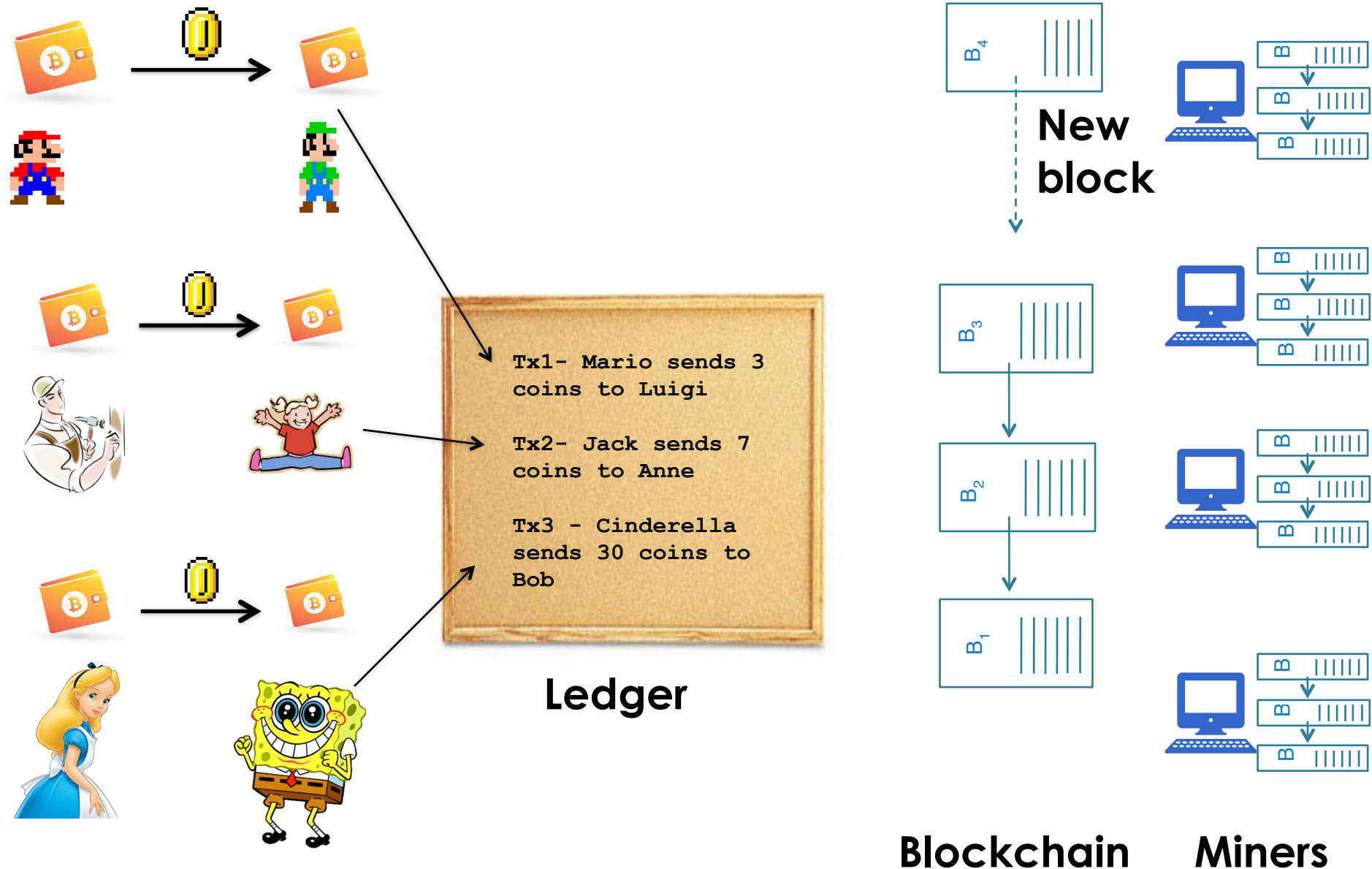
Tx3 - Cinderella
sends 30 coins to Bob

Immutability/Digest



- Others can detect
- Efficiently

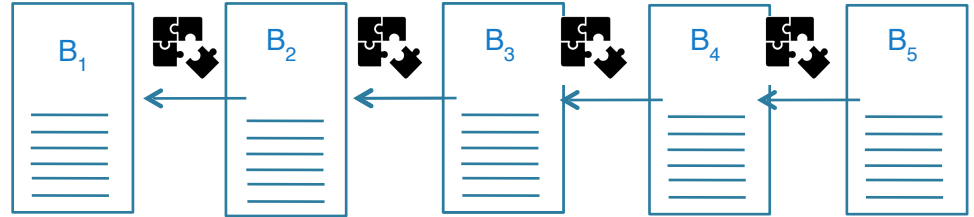
System Architecture



Consensus with PoW

- Puzzles: are mildly hard

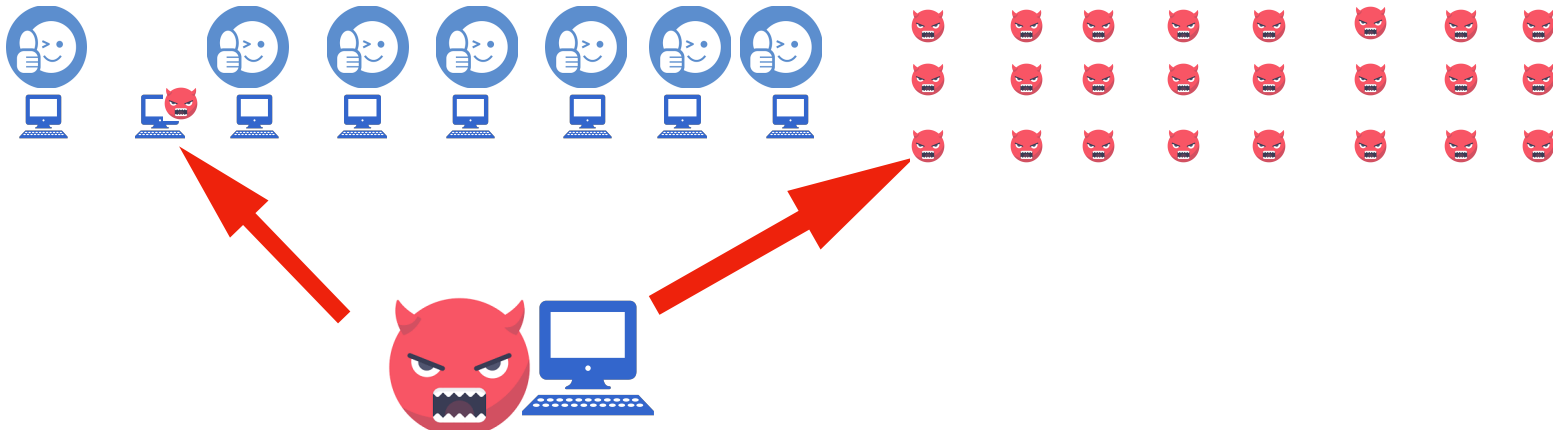
- Miners solve hash puzzles



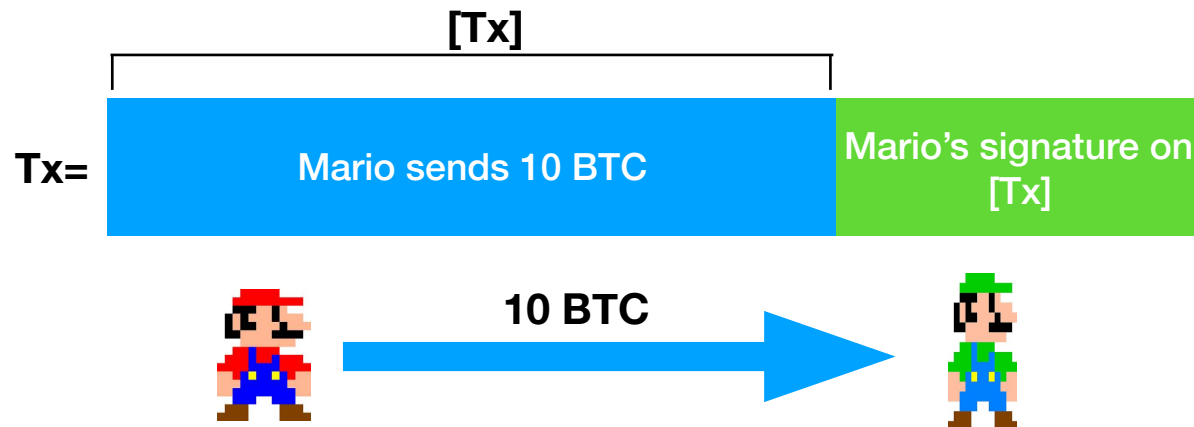
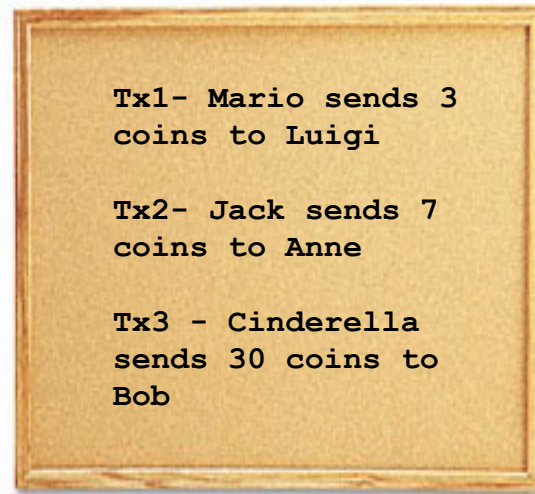
- Miners are rewarded with cryptocurrency (Mining)

- Prevents the Sybil Attack

**Computer power of the
adversary would is diluted**



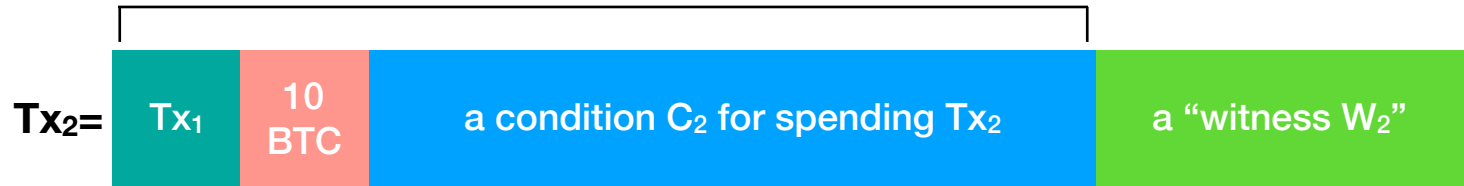
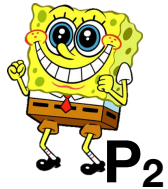
Transaction



A Witness

There is a previous transaction Tx_1  10 BTC  A relation!

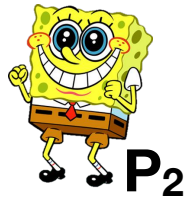
$[Tx_2]$



- Tx_2 should be
 - **hard** to produce
 - **easy** to verify its correctness
- W_2 “witnesses” that Mario has produced the transaction

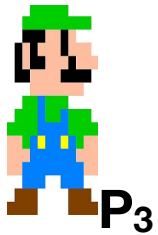
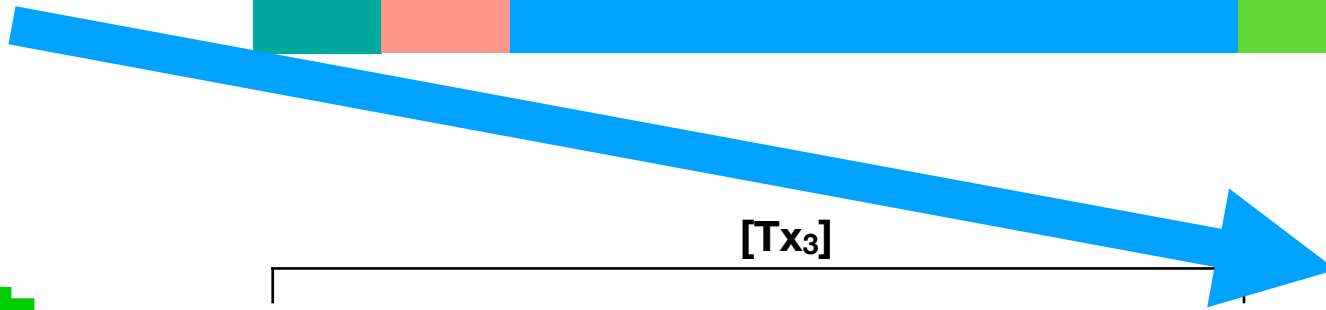
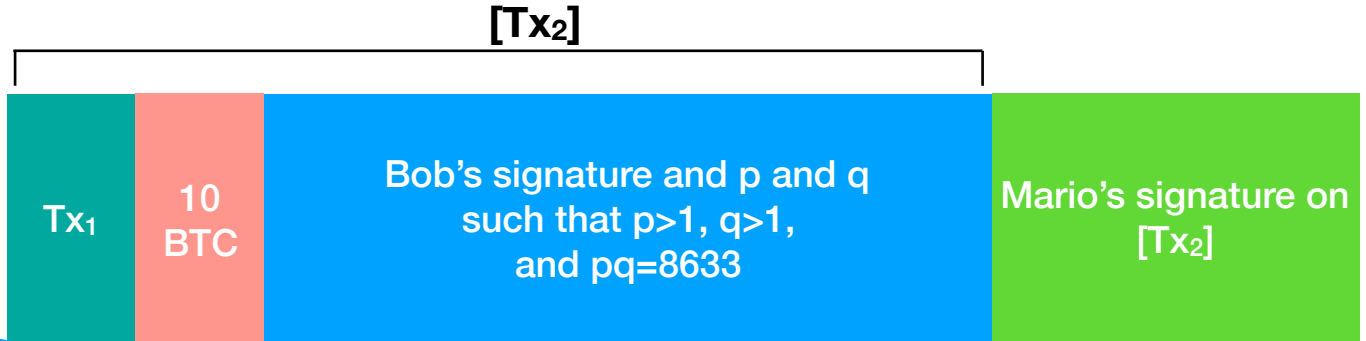


Example



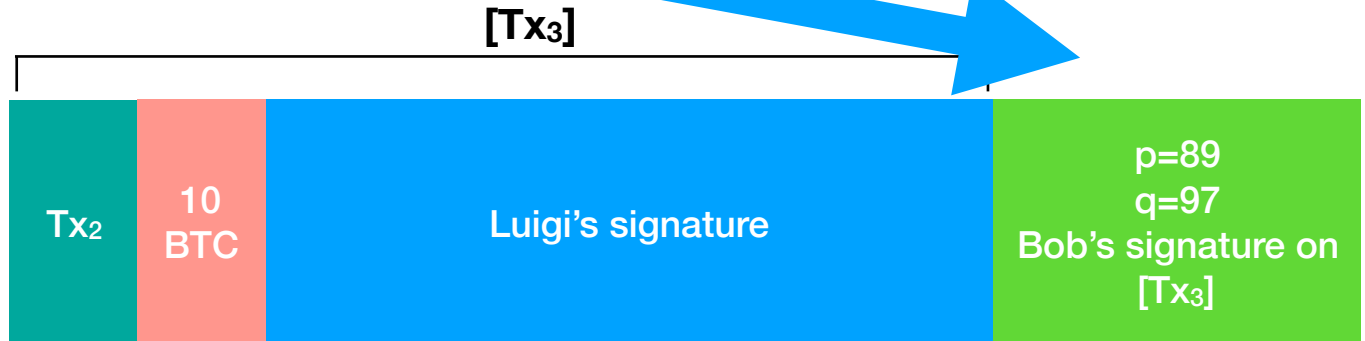
P_2

$Tx_2 =$

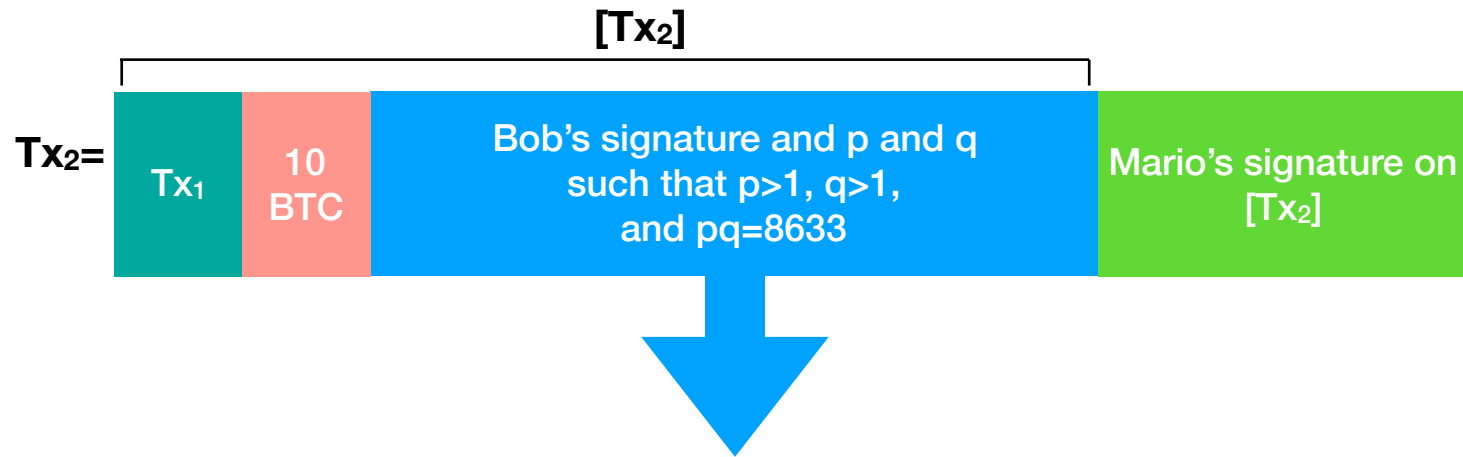


P_3

$Tx_3 =$



Smart Contract



- Arbitrary clause
- Bitcoin: stack based script language
- Ethereum: programming language (Solidity)
 - Bitcoin does not have smart-contract
- Programming Language: Smart Contract

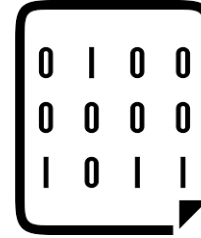
Differences in the Accounts



Externally Owned



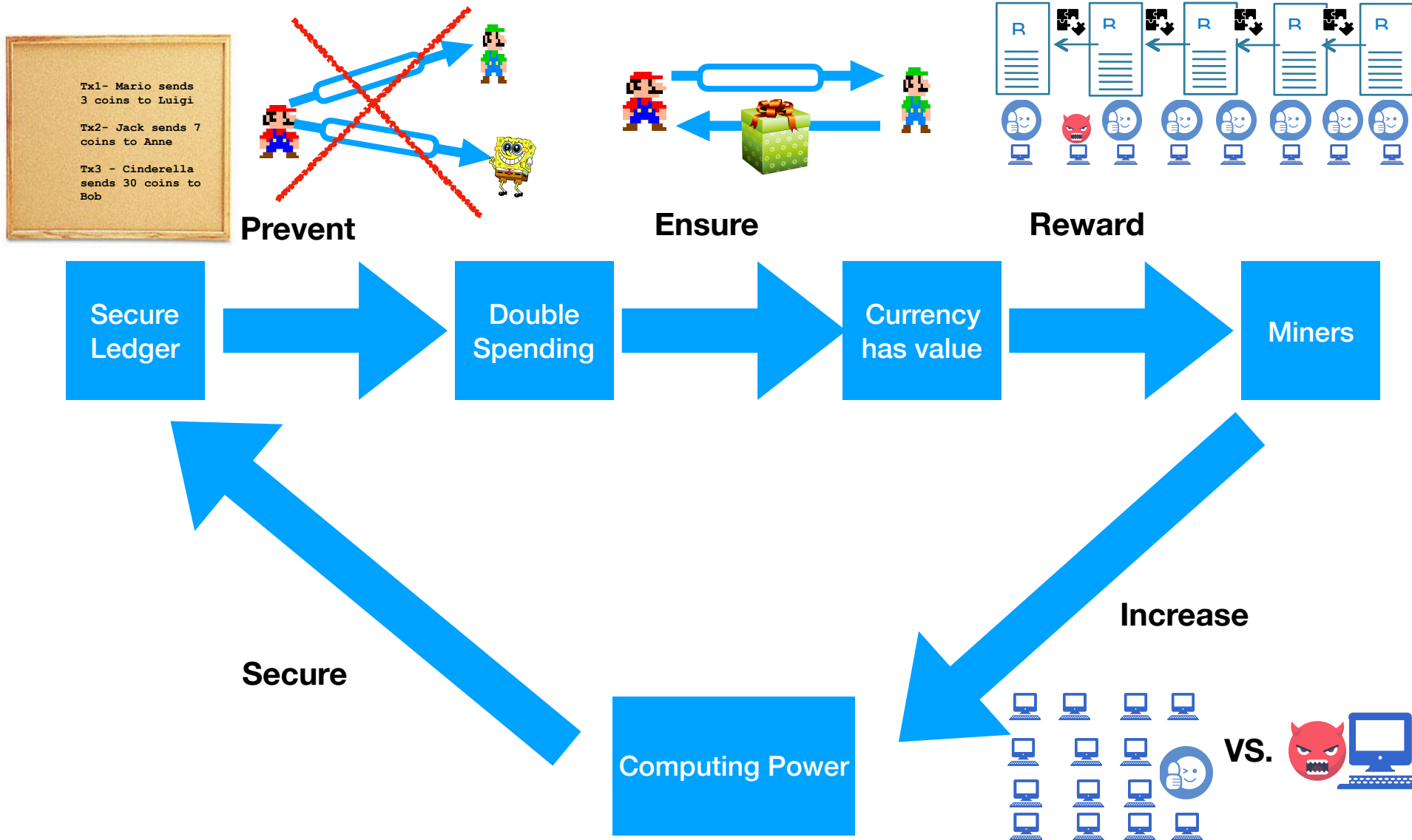
- Only Mario controls the keys
- Mario decides when to spend
- Mario's will is not in the blockchain



Smart Contract

- The contract code is public (it is on the chain)
- Given a transfer, the contract runs
- Every node in the system, updates the state of the system

Everything Together



Technical Challenges

- **Energy Consumption: PoW Vs PoS**
- **Privacy: Ledger information is public**
- **Scalability: Low TPS rate**
 - **Off-chain channels**
 - **DAG structures**
 - **New consensus methods**

Applications

Applications

- Distributed Autonomous Organisations (DAO)
 - Smart contract acts as a virtual organization with a predefined set of rules and actions/functions
 - If the majority of it's members/stakeholders decide (via voting) to take certain action, the contract automatically does it and delivers the result
- Decentralized Crowd Funding
 - Central authority who receives the funding is substitute with a smart contract.
 - Donors pay smart contracts and when the funding reaches to certain value, the funding automatically delivered to the funding recipient
- Robust and Fair Multi-party Computation
 - Allows all parties in a multi-party computation to get the output of computation; otherwise, they will be monetary compensated

Applications

- Namecoin (namecoin.org)
 - decentralized name system, key/value registration and transfer system
- Digital Credential of Diplomas
 - instead of transactions: diplomas, grants, courses in the *wallet*

IOHK Collaborates With GRNET To Offer Diplomas On The Blockchain

December 20, 2017 By: Payment Week



Athens, Greece – December 20 – Graduates in Greece will be able to show proof of their university qualifications using blockchain as a result of a project between IOHK, the leading blockchain research and development company, and GRNET, the national research and education network of Greece. In a pilot involving three Greek universities, degree holders will be able to electronically offer proof of their degree using a blockchain built by IOHK. As part of its role, GRNET will provide all of the web technology required, such as web pages, testing, and support. GRNET will also bring together the universities that will use the technology after the pilot concludes.

Currently in Greece, university diplomas are issued in paper form upon graduation. The university retains proof that the graduate passed all courses and was awarded the degree, and the degree holder obtains a certified copy from the department's registrar. When proof of a degree is required, such as when applying for a job, the degree holder provides a photocopy to the potential employer. If the certified copy is lost, the degree holder may request a new one from the university, though this can be a cumbersome and expensive

Digital Diploma debuts at MIT

Using Bitcoin's blockchain technology, the Institute has become one of the first universities to issue recipient-owned virtual credentials.

Elizabeth Durant | Alison Trachy | Office of Undergraduate Education
October 17, 2017

Press Inquiries

PRESS MENTIONS

In 1868, the fledgling Massachusetts Institute of Technology on Boylston Street awarded its first diplomas to 14 graduates. Since then, it has issued paper credentials to more than 207,000 undergraduate and graduate students in much the same way.

But this summer, as part of a [pilot program](#), a cohort of 111 graduates became the first to have the option to receive their diplomas on their smartphones via an app, in addition to the traditional format. The pilot resulted from a partnership between the MIT Registrar's Office and Learning Machine, a Cambridge, Massachusetts-based software development company.

The app is called Blockcerts Wallet, and it enables students to quickly and easily get a verifiable, tamper-proof version of their diploma that they can share with employers, schools, family, and friends. To ensure the security of the diploma, the pilot utilizes the same blockchain technology that powers the digital currency Bitcoin. It also integrates with MIT's identity provider, Touchstone. And while digital credentials aren't new — some schools and businesses are already touting their use of them — the MIT pilot is groundbreaking because it gives students autonomy over their own records.

"From the beginning, one of our primary motivations has been to empower students to be the curators of their own credentials," says Registrar and Senior Associate Dean Mary Callahan. "This pilot makes it possible for them to have ownership of their records and be able to share them in a secure way, with whomever they choose."

The Institute is among the first universities to make the leap, says Chris Jagers, co-founder and CEO of Learning Machine.

"MIT has issued official records in a format that can exist even if the institution goes away, even if we go away as a vendor," Jagers says. "People can own and use their official records, which is a fundamental shift."

In an article for *Forbes*, Andrew Raupp highlights a pilot program debuted by MIT last year that allows students the option to receive a tamper-free version of their diploma digitally using Bitcoin's blockchain technology. Raupp writes that, "Unlike a paper diploma, which could be easily lost or falsified, blockchain ensures that this important piece of data is never lost."

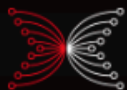
Forbes

Last year, the startup Learning Machine launched a program at Sloan and the MIT Media Lab that placed important documents, like transcripts and diplomas, on the blockchain. Now, reports Danny Crichton for *TechCrunch*, the company is working with the Media Lab on an initiative called BlockCerts, "an open and open standard securing credentials on the blockchain."

Inside Higher Ed reporter Lindsay McKenzie spotlights how MIT has begun a new pilot program that offers students the option to receive tamper-free digital diplomas, in addition to a traditional one. McKenzie explains that "students can quickly access a digital credential that can be shared on social media and by employers to assure its authenticity."

Tokyo Tech/IOHK Collaboration

IOHK.IO



INPUT | OUTPUT

HOME

ABOUT

RESEARCH

EDUCATION

PROJECTS

BLOG

CAREERS

ABOUT

TEAM

CONTACT

VIDEO

PRESS

MEDIA KIT

MSA

IOHK | ABOUT

Founded in 2015 by **Charles Hoskinson** and **Jeremy Wood**, IOHK is a technology company committed to using peer-to-peer innovations to provide financial services to the three billion people who don't have them.

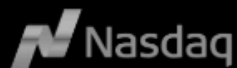
We are an engineering company that builds cryptocurrencies and blockchains for academic institutions, government entities and corporations. We are a decentralized company that loves small, innovative teams forming and executing ideas that cause cascading disruption.

FEATURED IN THE PRESS

Forbes



Bloomberg



BUSINESS
INSIDER



Collaboration



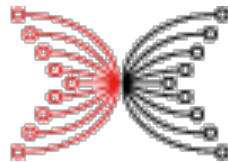
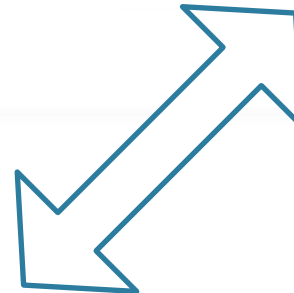
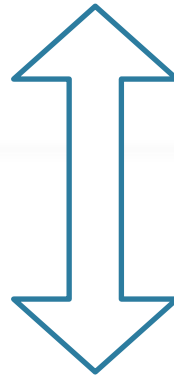
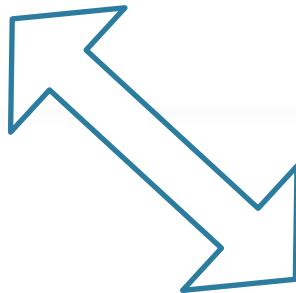
THE UNIVERSITY
of EDINBURGH



Tokyo Institute
of Technology



National and Kapodistrian
UNIVERSITY OF ATHENS



INPUT | OUTPUT

Established in 2017



Members

- Mario Larangeira, PhD (2017/February)
- Yuyu Wang, PhD (2018/May)



Three Goals

- **Research:** present relevant work in prestigious conferences
- **Educational:** promote and educate about cryptography and cryptocurrencies/form leaders in the area
- **Collaboration:** expose and increase activities with other institutions and researchers all over the world

Papers and Conferences

Kaleidoscope: An Efficient Poker Protocol with Payment Distribution and Penalty Enforcement

Bernardo David* Rafael Dowsley[†] Mario Larangeira*

Abstract

The research on secure poker protocols without trusted intermediaries has a long history that dates back to modern cryptography's infancy. Two main challenges towards bringing it into real-life are enforcing the distribution of the rewards, and penalizing misbehaving/aborting parties. Using recent advances on cryptocurrencies and blockchain technologies, Andrychowicz *et al.* (IEEE S&P 2014 and FC 2014 BITCOIN Workshop) were able to address those problems. Improving on these results, Kumaresan *et al.* (CCS 2015) and Bentov *et al.* (ASIACRYPT 2017) proposed specific purpose poker protocols that made significant progress towards meeting the real-world deployment requirements. However, their protocols still lack either efficiency or a formal security proof in a strong model. Specifically, the work of Kumaresan *et al.* relies on Bitcoin and simple contracts, but is not very efficient as it needs numerous interactions with the cryptocurrency network as well as a lot of collateral. Bentov *et al.* achieve further improvements by using stateful contracts and off-chain execution: they show a solution based on general multiparty computation that has a security proof in a strong model, but is also not very efficient. Alternatively, it proposes to use tailor-made poker protocols as a building block to improve the efficiency. However, a security proof is unfortunately still missing for the latter case: the security properties the tailor-made protocol would need to meet were not even specified, let alone proven to be met by a given protocol. Our solution closes this undesirable gap as it concurrently: (1) enforces the rewards' distribution; (2) enforces penalties on misbehaving parties; (3) has efficiency comparable to the tailor-made protocols; (4) has a security proof in a simulation-based model of security. Combining techniques from the above works, from tailor-made poker protocols and from efficient zero-knowledge proofs for shuffles, and performing optimizations, we obtain a solution that satisfies all four desired criteria and does not incur a big burden on the blockchain.

1 Introduction

Shamir, Rivest and Adleman, soon after their seminal work on the RSA cryptosystem, started exploring new ideas on cryptography inspired by everyday activities such as playing games. In particular, they started investigating how to play poker remotely [43]. A poker game, despite its apparent triviality, in fact, relates to a set of very interesting problems for the distributed setting. For example, shuffling a deck of cards in the presence of the players is very different from securely shuffling with remote parties: in the latter case every player needs to participate in the shuffling procedure; otherwise, security may not be assured at all for the participants.

*Tokyo Institute of Technology and Input Output HK. Emails: bernardo@ndavid.com, mario@titech.ac.jp. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair, which has received funding from Input Output HK.

[†]Aarhus University and Input Output HK. Email: rafael@cs.au.dk. This project has received funding from the European research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 669255).

Financial Crypto 2018

ROYALE: A Practical Framework for Universally Composable Card Games

Bernardo David* Rafael Dowsley[†] Mario Larangeira*

Abstract

Although much research have been done on mental card games since the 70's, it is surprising that even today several works in this area do not rely on modern techniques and frameworks for proving security. Just as an example, Bentov *et al.* (Asiacrypt 2017) does not provide a formal proof of security for their tailor-made poker game. At the best of our knowledge, the best formal treatment in the literature for a specific card game is given by David *et al.* (ePrint 2017) with their Kaleidoscope protocol for secure poker. Unfortunately, that protocol is only for poker and is not proven secure in the UC framework (that allows arbitrarily composition in environments like the Internet). Our contributions are threefold: (1) we introduce the first generalized ideal functionality for card games; (2) we develop the Royale protocol, which is a generalized version of Kaleidoscope, and show that it is UC-secure; (3) and, finally, we list issues in protocols in the literature.

1 Introduction

Online card games have become highly popular with the advent of online casinos, which act as trusted third parties performing the roles of both dealers and cashiers. However, this state of affairs is unsatisfactory, as a malicious casino (possibly compromised by an insider attack) can easily subvert game outcomes. In fact, such vulnerabilities not only constitute a looming threat but have indeed been exploited in the past [42].

The problem of playing card games among distrustful players without relying on a trusted third party, commonly referred to as *mental poker*, has been the subject a long line of research initiated in the early days of modern cryptography [38, 31, 17, 26, 3, 44, 24, 25, 19, 20, 30, 35, 4, 48, 13, 15, 27, 47, 39, 14, 37, 43, 41, 40]. However, the aforementioned mental poker protocols did not provide formal security definitions or proofs. In fact, concrete flaws in the protocols of [48, 47] (resp. [4, 15]) have been identified in [37] (resp. [22]). Moreover, even if some of these protocols can be proven secure, they do not ensure that aborting adversaries cannot prevent the game to reach an outcome or that honest players receive financial rewards according to such outcome.

Techniques for ensuring that players receive their rewards according to game outcomes have only been developed very recently by Andrychowicz *et al.* [2, 1], building on decentralized cryptocurrencies and blockchain protocols. Their techniques also prevent misbehavior (including

*Tokyo Institute of Technology. Emails: {bdavid,mario}@titech.ac.jp. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair, which has received funding from Input Output HK.

[†]Aarhus University and Input Output HK. Email: rafael@cs.au.dk. This project has received funding from the European research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 669255).

Financial Crypto 2019
(To appear)

Papers and Conferences

21 - Bringing Down the Complexity: Fast Composable Protocols for Card Games Without Secret State

Bernardo David^{1*}, Rafael Dowsley^{23**}, and Mario Larangeira^{13*}

¹ Tokyo Institute of Technology, Japan
{bernardo,mario}@c.titech.ac.jp

² Aarhus University, Denmark
rafael@cs.au.dk

³ IOHK, Hong Kong

Abstract. While many cryptographic protocols for card games have been proposed, all of them focus on card games where players have some state that must be kept secret from each other, *e.g.* closed cards and bluffs in Poker. This scenario poses many interesting technical challenges, which are addressed with cryptographic tools that introduce significant computational and communication overheads (*e.g.* zero-knowledge proofs). In this paper, we consider the case of games that do not require any secret state to be maintained (*e.g.* Blackjack and Baccarat). Basically, in these games, cards are chosen at random and then publicly advertised, allowing for players to publicly announce their actions (before or after cards are known). We show that protocols for such games can be built from very lightweight primitives such as digital signatures and canonical random oracle commitments, yielding constructions that far outperform all known card game protocols in terms of communication, computational and round complexities. Moreover, in constructing highly efficient protocols, we introduce a new technique based on verifiable random functions for extending coin tossing, which is at the core of our constructions. Besides ensuring that the games are played correctly, our protocols support financial rewards and penalties enforcement, guaranteeing that winners receive their rewards and that cheaters get financially penalized. In order to do so, we build on blockchain-based techniques that leverage the power of stateful smart contracts to ensure fair protocol execution.

1 Introduction

Cryptographic protocols for securely playing card games among mutually distrustful parties have been investigated since the seminal work of Rivest, Shamir

* This work was supported by the Input Output Cryptocurrency Collaborative Research Chair, which has received funding from Input Output HK.

** This project has received funding from the European research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 669255).

MARS: Monetized Ad-hoc Routing System (A Position Paper)

Bernardo David*
Tokyo Institute of Technology and
IOHK
Japan
bdavid@c.titech.ac.jp

Rafael Dowsley†
Aarhus University and IOHK
Denmark
rafael@cs.au.dk

Mario Larangeira‡
Tokyo Institute of Technology and
IOHK
Japan
mario@c.titech.ac.jp

CCS CONCEPTS

• Theory of computation → Cryptographic protocols;

KEYWORDS

Cryptographic Protocols; Reputation; Ad-hoc Networks; Blockchain

ACM Reference Format:

Bernardo David, Rafael Dowsley, and Mario Larangeira. 2018. MARS: Monetized Ad-hoc Routing System (A Position Paper). In *CryBlock '18: 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, June 15, 2018, Munich, Germany. ACM, New York, NY, USA, 5 pages. <https://doi.org/10.1145/3211933.3211948>

1 INTRODUCTION

A mobile ad-hoc network (MANET) allows mobile devices to communicate without any pre-established infrastructure or centralized management. In a MANET, nodes cooperate among themselves to route messages, dynamically adjusting routes as they join, leave and physically move. Such flexibility makes MANETs attractive for applications such as campus networks, disaster relief, providing internet access networks in areas without infrastructure and Internet-of-Things (IoT) applications. However, a consequence of node mobility and lack of central infrastructure is an unknown and constantly changing network topology, which makes it unfeasible to deploy traditional routing protocols [7].

Providing efficient and reliable routing for MANETs is a challenging task for which a number of protocols has been developed [9]. These protocols can be classified into two main categories [10]: reactive routing protocols, where nodes discover routes only when needed, and proactive routing protocols, where nodes perform a

constant route discovery process by periodically exchanging topology information. The Ad-Hoc On Demand Distance Vector (AODV) protocol [15], a reactive routing protocol, and the Optimized Link State Routing Protocol (OLSR) [6], a proactive routing protocol, are well known examples of MANET routing protocols and will be used as examples in this work.

MANET routing protocols are usually not designed with security in mind and are indeed subject to several threats and attacks [9–11]. Nodes that intentionally misbehave in a MANET routing protocol can be classified into two main categories: *malicious nodes* or *selfish nodes* [13]. Malicious nodes aim at actively disrupting routing operations by subverting routing operations or overloading the network. On the other hand, selfish nodes do not purposefully disrupt network operations but refuse to route incoming messages while using other nodes' resources to route their own messages. Detecting and mitigating selfish behavior has proven to be a hard problem, since selfish nodes do not actively deviate from the protocol.

A number of heuristics for detecting and isolating selfish nodes have been proposed [1, 2, 5, 13, 17]. Most of them are *reputation-based* solutions, basically providing ways for nodes to measure how much their peers are contributing to routing and keep local records of each other's reliability (*i.e.* reputation). Given this data, nodes can choose which peers to cooperate with. Notice that, in addition to observing the behavior of peers in their vicinity, nodes also rely on external advice for building their reputation records (especially for peers that cannot be reached directly). However, in current reputation-based schemes, each node keeps its own reputation records locally, allowing dishonest nodes to falsely accuse their peers of misbehavior. These issues affect the accuracy and effectiveness of current reputation systems, which employ complicated heuristics to mitigate false claims of misbehavior and build a cohesive view of reputation among honest nodes. The solutions presented in [1, 17] also employ financial incentives, proposing a "central bank" entity that financially rewards nodes who participate in routing.

1.1 Our Contributions

In this work, we introduce MARS, a system that uses cryptographic tools to build a decentralized and *publicly verifiable* record of nodes' reputations in MANET routing protocols that can be accessed and verified by any third party (including new nodes that join the network). Moreover, MARS allows nodes to trade their reputation points for other assets, such as (improved) network services and cryptocurrencies. MARS works as an overlay extension to any MANET routing protocol. It stores reputation information in a

† This work was supported by the Input Output Cryptocurrency Collaborative Research Chair, which has received funding from IOHK.

‡ This project has received funding from the European research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 669255).

* This work was supported by the Input Output Cryptocurrency Collaborative Research Chair, which has received funding from IOHK.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions.acm.org.

CryBlock '18, June 15, 2018, Munich, Germany.

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-5839-5 \$10.00, \$15.00

<https://doi.org/10.1145/3211933.3211948>

SCIS 2019 (Next Month)

Copyright ©2019 The Institute of Electronics,
Information and Communication Engineers

SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

Verifiable Sequential Work with Trusted Generator

Xiangyu Su* Mario Larangeira[†] Keisuke Tanaka*

Abstract: Verifiable delay functions (VDF) proposed by Boneh et al. (Crypto'18) has several applications on blockchain based systems, random beacons and etc. Although the highly practical applications, less than a handful of constructions are known due to the need of efficient public verifiability. In the best of our knowledge, the only two constructions are from Pietrzak (EPRINT' 18) and Wesolowski (EPRINT' 18). In this paper, we define a VDF variant, which we denote by verifiable sequential work (VSW). The main idea is to take the sequential computations in VDF to reduce the difficulty of a hard problem to a moderated hard level. We construct a weakened VSW which needs a trusted third-party to run the generation phase: the VSW with trusted generator (VSWTG). The construction achieves a simple, one message and one group exponentiation publicly verifiable VSWTG. It is a more computational efficient verification procedure than the known VDF verification constructions. We regard the need for a trusted party as a necessary trade-off, however, we conjecture our variant may be easier to find other candidate constructions than the VDF definition. Finally, we formalize the idea of the Rivest-Shamir-Wagner (RSW) time-lock puzzle to a new primitive that we call trapdoor iterated sequential functions (TISF) and investigate on its possible candidates.

Keywords: Blockchain, Proof-of-Work, Verifiable Delay Function, Time-Lock Puzzle.

1 Introduction

1.1 Background

Proofs of work (PoW) first introduced by Dwork and Naor [5] in the early 1990s, is attracting more attention these days as the boom of cryptocurrency. The idea is simple, provers in the protocol have to donate a quantifiable amount of computation power to solve some easily verifiable puzzles. The most widely used construction based on hash functions is proven to be secure in heuristic models, i.e. the random oracle model (ROM).

However, when we want to build a PoW-like system on computational hard assumptions, it seems to be hard for provers to solve in polynomial even sub-exponential time. Moreover, it is difficult to adjust hardness for puzzles based on these assumptions without tuning the security parameters.

As another important primitive in cryptocurrency, the verifiable delay function (VDF) proposed by Boneh et al. [2] is basically a verifiable random function (VRF) which needs sequentiality in the evaluation, i.e. it takes sufficient long time to evaluate even paralleling on multiprocessors. The property of VRF shows that no party can predict the outputs of VDF before going through the evaluation, and sequentiality shows that there is no

shortcut existing for evaluation.

The VDF has applications on blockchain based systems and random beacons¹, however, the constructions are limited by the demands of public verifiability. In the best of our knowledge, only two more VDF constructions exist by Pietrzak [7] and Wesolowski [10], both of them rely on the concept of Rivest-Shamir-Wagner (RSW) time-lock puzzle [9] (which a formal definition will be presented in Section 2). Briefly, an RSW time-lock puzzle requires provers to compute iterated squarings in an RSA group. In order to verify such solutions publicly, the trivial way is to go through the same computation as provers do, which is not optimistic for practical usage.

Pietrzak's and Wesolowski's VDFs. The two constructions share the same setup phase, which is to generate an instance of RSW time-lock puzzle. The difference lies in how they make their verification public. To achieve this, both of them require provers to produce a proof corresponding to their solutions. However,

- **Pietrzak's construction:** It requires interactive proof system. They make it non-interactive with Fiat-Shamir heuristic, which needs ROM and is preferable to avoid.
- **Wesolowski's construction:** It is more efficient in verification, but provers have to compute the proof separately after computing the solution and it costs no less.

¹ NIST is implementing a source of public randomness. The service is at <https://beacon.nist.gov/home>.

* Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology. Tokyo-to Meguro-ku Ookayama 2-12-1 W8-55. Email: {su.x.s@tm, sario@e, keisuke@is}.titech.ac.jp. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair funded by IOHK, JST CREST JPMJCR14D6, JST OPERA, JSPS KAKENHI JP16H01705, JP17H01695.

[†] IOHK. Email: mario.larangeira@iohk.io

Copyright ©2019 The Institute of Electronics,
Information and Communication Engineers

SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

Lightweight Virtual Payment Channels

Maxim Jourenko* Mario Larangeira[†] Keisuke Tanaka*

Abstract: Payment channel networks are one of the latest attempts on improving the scalability of blockchains in the number of transactions per second. Nodes within such a network can exchange funds without the necessity of interacting with the blockchain except during setup, closure or eventual dispute of their mutual channel. Payments can be executed across a path of payment channel using hashed time lock contracts. However, for each individual payment all nodes within a path need to be interacted with it during setup, execution or teardown phases, and therefore they need to be online. This is a limitation of payment networks especially for long payment paths. A recent proposal by Dziembowski et al. (CCS'18) that enables payments across multiple payment channel without the necessity of intermediate nodes being online is using virtual payment channel. As of now the only construction for virtual payment channel requires smart contracts as those implemented on the Ethereum blockchain. Our work proposes a construction for virtual payment channel without requiring smart contracts, but instead it is built upon only time locks and threshold signatures. This enables implementation of virtual payment channel on a larger range of blockchain implementations such as Bitcoin.

Keywords: Blockchain, Off-chain, Payment Channels, Scalability.

1 Introduction

Blockchain technology offers a plethora of opportunities. It started off with enabling electronic payments over a decentralized system and a series of research since then proposed methods to enhance anonymity, the use of blockchains to enforce fairness in secure multiparty protocols [2], or even play games [4]. However, as of now blockchains face limitations. For one, for security reasons payments require confirmation time. For instance, in Bitcoin it is suggested to wait about one hour after seeing a payment on the blockchain before accepting it [9]. Moreover, blockchains face limited scalability. As discussed in [3], whereas the payment system VISA handles 56,000 payments per second at peak times Bitcoin has a limit of 7 transactions per second.

Background. One of the latest proposals to improve scalability of blockchains are so-called offchain payment networks as introduced in [11], [1], [10], [5] and subsequent works. Offchain payment networks enable micro-payments, payments without confirmation time, and theoretically a limitless amount of transaction per second across the whole offchain payment network. Intuitively, this is achieved by using optimistic protocols. In the optimal case, in contrast to payments that are

directly done on the blockchain, payments on a payment channel network do not need to be verified by all participants of the respective cryptocurrency, and their miners, but just by payer and payee. However, in case of dispute, parties can fallback onto the security of the blockchain to enforce any payments done between them. To be able to do payments parties need to set up offchain channels between pairs of parties on the blockchain. Moreover, if parties Alice and Ingrid set up such a channel as well as Ingrid and Bob then Alice can do a payment offchain using the channels of both Alice and Ingrid as well as Ingrid and Bob, without the necessity of creating a new channel between Alice and Bob. Like this a payment can cross an arbitrary amount of intermediate nodes between payer and payee, however, all intermediate nodes need to cooperate and be online for each individual payment which becomes prohibitive for long paths. A series of work by Dziembowski et al. [6] and [7] proposed Virtual State Channels as a solution to this issue. With this approach parties can execute payments across a network without requiring interaction with intermediate nodes, such that intermediate nodes may be offline during this process. Their approach requires the availability of smart contracts as in Ethereum to be able to implement virtual state channel. In our work we propose a construction for lightweight virtual payment channel that allows the implementation of virtual payment channel without smart contracts therefore only requires a scripting language containing timelocks and threshold signatures. This enables implementation of virtual payment channel in blockchains with less expressive scripting languages such as Bitcoin.

Related Work. Virtual Channel have been first introduced in a series of work by Dziembowski et al. [6]

* Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology. Tokyo-to Meguro-ku Ookayama 2-12-1 W8-55. Email: {kurazumi.x.s, jourenko.m.ab@tm, titech.ac.jp, sario@e, titech.ac.jp, keisuke@is, titech.ac.jp}. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair funded by IOHK, JST CREST JPMJCR14D6, JST OPERA, JSPS KAKENHI JP16H01705, JP17H01695.

[†] IOHK. Email: mario.larangeira@iohk.io

SCIS 2019 (Next Month)

Copyright ©2019 The Institute of Electronics,
Information and Communication Engineers

SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

A Timeout Anonymous Payment Channel for Decentralized Currencies

Kanta Kurazumi* Maxim Jourenko* Mario Larangeira* Keisuke Tanaka*

Abstract: Anonymous payment channel (APC) was introduced by Green and Miers (CCS'17) with the Bolt protocol. This work contributes with the growing body of work on off-chain channels aiming to enhance the scalability of cryptocurrencies in the number of (in this case, anonymous) transactions per second. Although Bolt presents a secure formulation, we observe that it requires cooperation between customer/merchant, the protocol players, in order to complete the protocol. More concretely, in its current form, if the customer does not cooperate, the protocol cannot complete. The reason is that the customer is required to start the channel closing procedure and it is not clear what happens if it does not. In this work we address this problematic situation with a variant definition for APC, which takes into account a timeout parameter, and present a protocol construction.

Keywords: Blockchain, Off-chain, Payment Channel, Anonymity.

1 Introduction

Bitcoin has gained popularity as the first successful electronic currency. However, the fundamental technology realizing Bitcoin, the *blockchain*, is currently subject to a severe limitation on the number of transactions that can be processed per second. As a solution to this *scalability* limitation, a number of *payment channel* schemes have been proposed [10, 4], whose approach consists of a series of payments between the parties, where only the initial deposit amounts and the final balance of both ends of the channel are reflected on the chain. While this approach benefits from the integrity of on-chain transactions, at the same time, it circumvents the potential costs of specific blockchain mechanisms. That is, for example, by the player's direct interaction, the payment will not be affected by the cost of on-chain transaction fees and the confirmation delays. Thus making it possible to realize a payment at high speed and a small amount.

On the other hand, to compensate for Bitcoin's weakness on anonymity, a number of *mixing services* for on-chain transactions have been proposed [11, 12, 2, 14, 13, 7]. At the same time, decentralized currencies with anonymity based on Bitcoin have been devised [8, 1]. However, even in a currency that has gained anonymity in these manners, when we establish a payment channel

on it, the payment channel scheme itself must have a mechanism to achieve off-chain anonymity separately. For that purpose, several constructions, e.g. [5, 6], have been suggested.

Related Work. A particular privacy preserving construction for payment channels is given by Green and Miers [5], who introduced a general definition for *anonymous payment channel scheme* (APC) and a protocol named Blind Off-chain Lightweight Transactions (BOLT). This protocol presents anonymity in the sense that every payment is not linked with all prior payments on the same channel and with the identity of the payer. Typically, in a payment channel scheme, even if parties are malicious, they must not be able to reclaim more coins than the final shares determined by the initial deposit amounts and a subsequent series of payments. Moreover, parties that opened a channel should be able to immediately, and freely, close the channel and reclaim its funds at any time. However, in their proposal, in order to close the channel, the two parties who have a channel must coordinate with each other. Otherwise, the channel can not be closed and their funds may be locked in the chain.

Our Contribution. In order to address this problematic situation, we propose a variant definition for APC scheme named *timeout anonymous payment channel scheme* (TAPC) and a protocol construction. In our definition and construction, we introduce a *timeout parameter* in order to cope with the situation that one of the parties do not cooperate to close the channel. Therefore when a party informs the closure of the channel, the network is informed of it via the timeout parameter. Then the network waits for the another party's response for the time specified the timeout pa-

* Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology, Tokyo-to Meguro-ku Ookayama 2-12-1 W8-55. Email: {kurazumi.k.aa,jourenko.m.ab}@m.titech.ac.jp, mario@titech.ac.jp, keisuke@is.titech.ac.jp. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair funded by IOHK, JST CREST JPMJCR14D6, JST OPERA, JSPS KAKENHI JP16H01705, JP17H01695.

[†] IOHK. Email: mario.larangeira@iohk.io

Copyright ©2019 The Institute of Electronics,
Information and Communication Engineers

SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

Survey on Payment Channels and Payment Channel Networks

Maxim Jourenko* Kanta Kurazumi* Mario Larangeira* Keisuke Tanaka*

Abstract: Blockchain based systems, in particular cryptocurrencies, face a serious limitation: scalability. This holds especially in terms of number of transactions per second. Several alternatives are currently being pursued by both the research and practitioner communities. One venue for exploration is on protocols that do not constantly add transactions on the blockchain and therefore do not consume the blockchain's resources. This is done using off-chain transactions, via *payment channels*. This work relates several existing off-chain channels, payment and state, payment networks and their respective management algorithms. The main goal of this survey is to provide a comprehensive list of the state-of-art protocols available, outlining their respective approaches, advantages and disadvantages.

Keywords: Blockchain, Off-chain, Payment Channels, Scalability.

1 Introduction

Blockchain is the main data-structure behind the successful rebirth of digital cash from its first attempts firstly by Bitcoin and now with several decentralized cryptocurrencies. Although Bitcoin's relative success in offering worldwide payment alternatives to the more traditional mechanisms, like VISA Network or Paypal, is undeniable, it still has a long way ahead in terms of handling a larger number of transactions. The technical challenge of increasing the number of transactions per second (TPS) of a blockchain system is urgent, and it is closely related to the inner workings of the system itself. Namely, to its *consensus protocol*. As a more concrete example, we refer to the Bitcoin network whose consensus protocol depends on the joint hash power of its nodes to perform the block leader election, that is, the selection of the new block issuer, which is calibrated by design to happen every 10 minutes on average. In Proof-of-Stake (PoS) based systems, analogous election exists also within a carefully designed (and strongly dependent on security guarantees) time slot for the generation of the new block. Let alone that, in order to confirm a transaction, it is required a minimum number of blocks added to be added in the main chain, which gives the *confirmation time*. The confirmation time, despite its central role in the security and stability of the system, imposes severe restrictions to the TPS rate of the overall platform.

One alternative to circumvent this intrinsic limitation is *payment channels*. In a nutshell, a payment chan-

nel between two players, is when both participants decide to trade several transactions during a period of time, and in the end they settle on a final balance based on the transactions exchanged, and the channel is closed. This transaction method is suitable for very small amounts, i.e., *micropayments*. More recently, micropayments were also studied by Pass and Shelat [20] in the setting of decentralized currencies, and for specific applications [3, 10]. The main advantage of such a setting is that for each transaction made during the period of the channel, do not need to be published in the blockchain. Therefore they can be settled independently of the refresh time of the system, which drastically improves the TPS rate.

More than channels. The channels themselves are building blocks into a stack of algorithms. A simple payment/state channel only paves the way for exchanging funds between two players which is of limited use. A more interesting, and realistic, use is the concatenation of single channels into a *payment network*. In such a setting, a node *A* can send payment to *C* without creating a specific channel for it, as long as both *A* and *C* are connected to a third node *B*, which relays transactions through the payment of fees.

The resemblance with theory of networks is inevitable, naturally similar problems appear. For example, a node sending a payment needs to find a route, similarly to routing problems in networks. On the other hand, payment networks also present differences, for example, the cost of the fees in a particular route.

Our contribution. A summary of this work is Table 1. Given the similarities with networks, techniques can be borrowed from currently known network algorithms but need to be adapted. These similarities and differences suggest a layer of *network management*, in addition to the *channel* and *network* layers. We further observe that privacy and security permeates the layers. Channels, for example, need to be consistent with the

* Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology, Tokyo-to Meguro-ku Ookayama 2-12-1 W8-55. Email: {kurazumi.k.aa,jourenko.m.ab}@m.titech.ac.jp, mario@titech.ac.jp, keisuke@is.titech.ac.jp. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair funded by IOHK, JST CREST JPMJCR14D6, JST OPERA, JSPS KAKENHI JP16H01705, JP17H01695.

[†] IOHK. Email: mario.larangeira@iohk.io

SCIS 2019 (Next Month)

Copyright ©2019 The Institute of Electronics,
Information and Communication Engineers

SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

Account Management and Stake Pools in Proof of Stake Ledgers

Dimitris Karakostas* Aggelos Kiayias* Mario Larangeira†

Abstract: Blockchain protocols based on the Proof of Stake (PoS) paradigm are —by nature— dependent on the active participation of the owners of the assets maintained in the ledger. Moreover, it is often the case that not all stakeholders consistently take part in the protocol's execution and engage in the PoS mechanism. Given the security risks that such behaviour introduces, a countermeasure is to allow stake representation, thus giving the stakeholders the option to delegate their "staking" rights to other participants, thus forming "stake pools." Our work fills gaps in literature by thoroughly presenting all desiderata for account management and stake pools in the PoS setting. We formalize the requirements and present a framework which can be used to build stake pools for any PoS protocol. We introduce the first ideal functionality for a PoS wallet's core, which captures the capabilities that a PoS wallet should possess.

Keywords: Wallet, Proof-of-Stake, Stake-pools, Delegation, Blockchain.

1 Introduction

A Proof of Stake (PoS) blockchain protocol relies on the participation of the owners of the assets that are maintained by the distributed ledger. The stakeholders are expected to follow the protocol's execution, checking whether they are eligible to participate and, in those cases, engage, within a specific timeframe, in transaction processing per the PoS protocol's rules, cf. [10, 2, 7, 17]. This feature is in sharp contrast with Proof of Work (PoW) protocols, such as Bitcoin, for which there exists a natural decoupling between the consensus layer participants, *i.e.*, the *miners*, and the users of the system, who transact using the ledger. Although the set of users in principle subsumes the miners, since *e.g.*, the miners are collecting fees and may transact using them, a substantial number of users do not participate in the consensus protocol. In the case of mining pools, a member of a mining pool may not even be a user, *e.g.*, receiving compensation via an out-of-band mechanism by the pool's leader.

This dual nature of assets in a PoS blockchain raises two important considerations:

- it requires some secret-key information to be used frequently on behalf of an asset. Depending on the account model of the underlying ledger, these actions may reveal critical cryptographic information that may weaken the security of the underlying asset and in any case increase the attack surface against a user's wallet. For instance, in

the UTXO model, which is implemented by the Bitcoin ledger and the majority of cryptocurrencies, addresses are hash values and the public-key information is revealed only when spending the funds. If the same model is used in the PoS setting in a straightforward manner, then each time an action occurs on behalf of the asset, the public key is revealed prior to spending the funds;

- it introduces a computational burden and availability requirement for the stakeholders. For instance, an everyday user is not always online or may choose to abstain from participating. In an environment where the majority of users behave this way the security guarantees are weakened, thus hurting the overall protocol's security.

The above issues are well known and have already been informally considered in the Bitcoin forum¹, with various proposed solutions. For instance, a separation between a staking and a payment key could address the first consideration.² Regarding the second consideration, even though it seems unavoidable due to the nature of PoS protocols, a possible countermeasure is to delegate the rights of participating in the PoS protocol, *e.g.*, generating a block or validating transactions, to stake pools. Stake pools also bring efficiency advantages, given that the set of stake pool leaders, *i.e.*, the delegates who manage the assets on behalf of the users, can be much smaller than the entire stakeholder set. Therefore they can form a *committee* which executes any necessary protocol steps. The size of this committee, in comparison to the whole set of regular users, can be much smaller, so the computational and communication complexity overhead is substantially reduced.

Interestingly, none of the existing major PoS imple-

* University of Edinburgh and IOHK. Emails: {dimitris.karakostas,aggelos.kiayias}@ed.ac.uk

† Tokyo Institute of Technology and IOHK. Emails: mario@e.titech.ac.jp and mario.larangeira@iohk.io. This work was supported by the Input Output Cryptocurrency Collaborative Research Chair funded by IOHK, JST CREST JPMJCR14D6, JST OPERA, JSPS KAKENHI JP16H01705, JP17H01695.

¹ For instance, we refer to [13].

² We refer to the discussion in [14].

Youtube - Rump Session

s Karakostas

Aggelos Kiayias

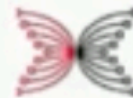
Mario Larangeira

Account Management and Stake Pools in Proof of Stake Ledgers



THE UNIVERSITY
of EDINBURGH

Dimitris Karakostas



INPUT | OUTPUT

Aggelos Kiayias



Tokyo Institute
of Technology

Mario Larangeira

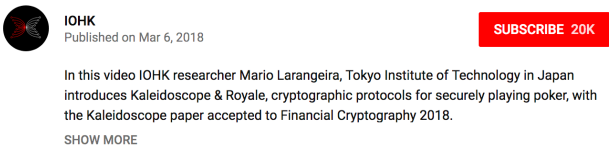
Crypto 2018 - Rump Session

Online Content



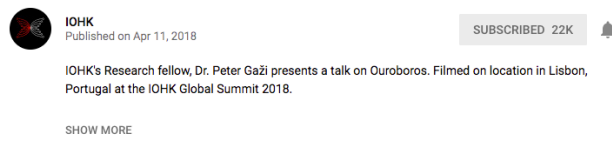
IOHK | Research; Kaleidoscope & Royale, Dr Mario Larangeira.

1,874 views



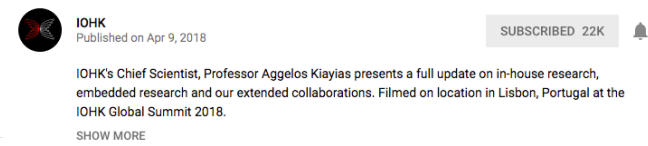
IOHK | Research; Dr. Peter Gaži, Ouroboros.

2,086 views



IOHK | Research; Prof Aggelos Kiayias, Input Output Research.

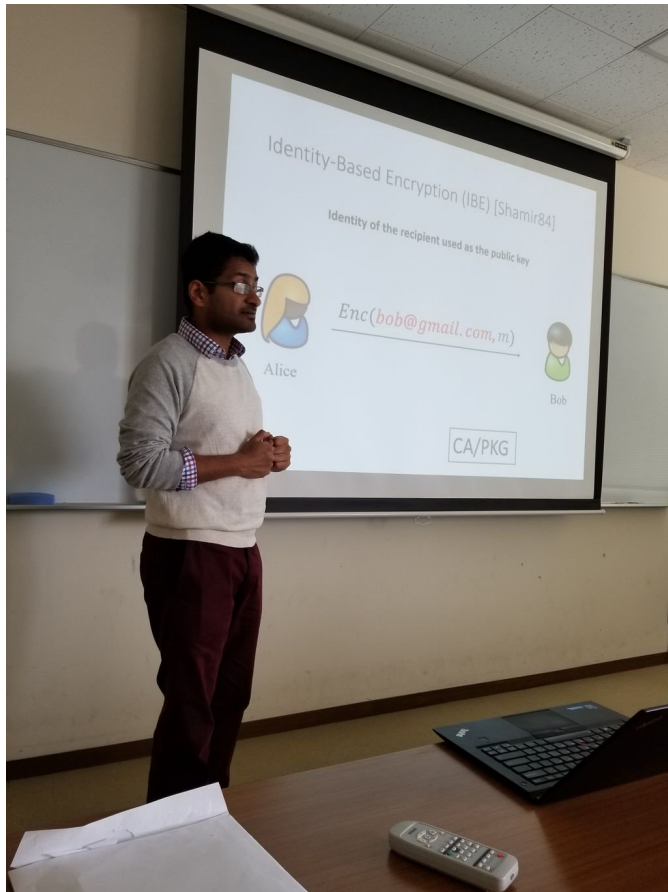
2,327 views



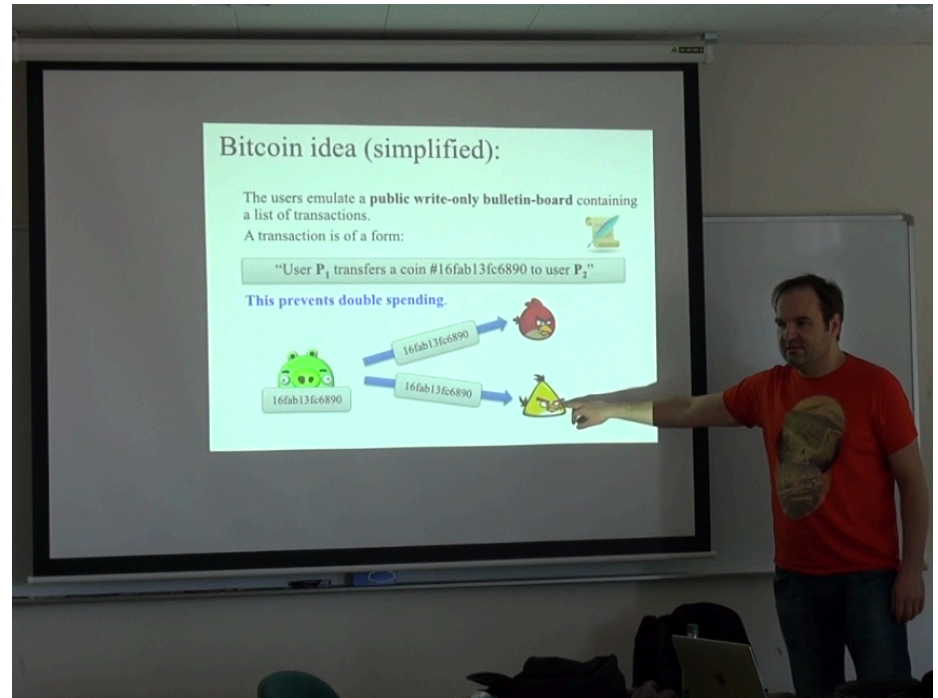
Graduate Course - 1st Quarter/2018



Visitors



Prof. Sanjam Garg
(UC Berkeley)



Prof. Stefan Dziembowski
(Univ. of Warsaw)

Visitors

Conclusions and directions

After >30 years of ZK *we have the first truly efficient protocols* for generic statements.

Many applications *are enabled* by efficient ZK for arbitrary circuits.

And I expect many more to come!

Thanks!

ZKGC vs ZKBoo?

- ZKBoo allows Fiat-Shamir 😊
- ZKBoo does not need OT 😊

The end of ZKGC?

- Are there better privacy-free GCs?

Improving ZKBoo?

- Large proof size: Can you find better decompositions?

$f(x)$

x_1, x_2

y_1, y_2

f

$Verif(x)$

x_1, x_2

w

Prof. Claudio Orlandi
(Aarhus University)

Visitors



David Chaum
(Elixir and the early mentioned Digicash)

Conclusion

- **(very) Brief Blockchain Technology Introduction**
- **Open problems/technical challenges**
- **Application: Digital Diploma**
- **Collaboration between Tokyo Tech/IOHK**

Questions?

Cryptocurrency

- It is not equal, but it is analogous to regular currency (no need of third party for transactions)
- It is not associated with a country, but with the system itself
 - System: network of computers
 - Token: the coin of the cryptocurrency
- Difference: the rules of the system are public and rely on the people using it (a **decentralized system**)

Majority Matters

- Consensus without PoW



vs.



- Consensus with PoW

Computer power matters

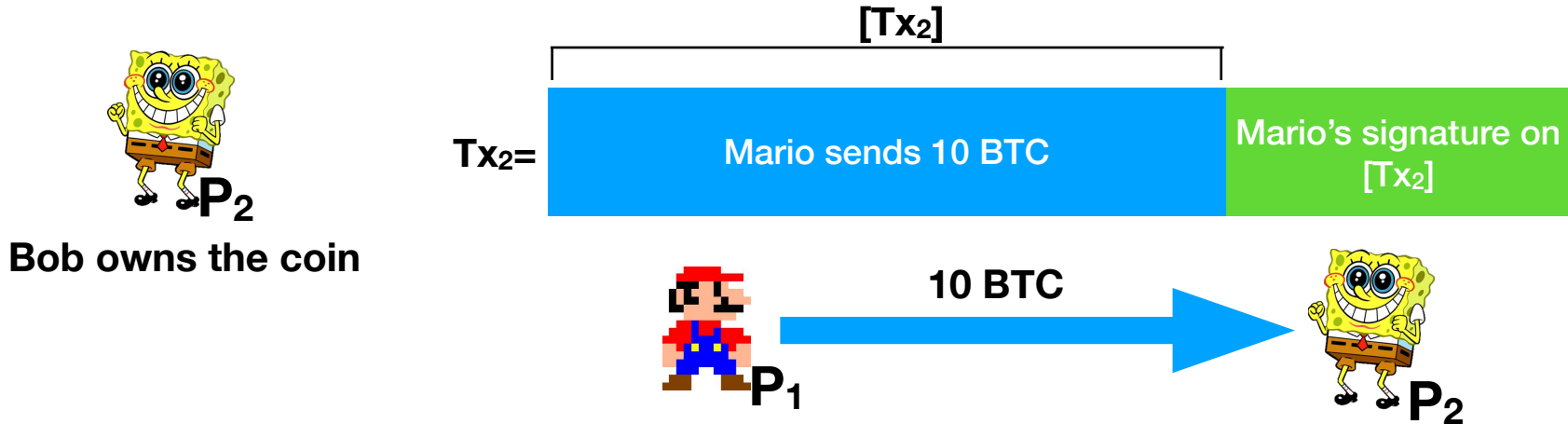


vs.



Bitcoin Transaction

There is a previous transaction Tx_1  10 BTC 



Generalization

