Algorand™

L'ascesa di una pure proof-of-stake blockchain

Blockchain Devs Meetup
21 Ottobre 2019

Fabio Tagliaferro

Su di me: Fabio Tagliaferro

Studente Magistrale in Scienze e Ingegneria Informatica (Università degli Studi di Verona)

Da ottobre 2018:

Algorand Ambassador

Da giugno 2018:

Membro del nodo italiano di Blockchain Education Network

blockchainedu.net

Da luglio 2019:

Stagista presso

takamaka.io

Blockchain Education Network

BLOCKCHAIN EDUCATION NETWORK

blockchainedu.org/courses/algorand/

BEN è una comunità decentralizzata dove studenti e in generale appartenenti al mondo accademico possono condividere le proprie idee su temi legati a blockchain, criptovalute e smart contracts.

Lo scopo della collaborazione è di supportare l'ambiente formativo ed estendere le conoscenze in questo campo.

Il mio primo approccio con Algorand

MIT Technology Review

Sign in Sul

Topics Magazine Newsletters Events

Blockchain / Bitcoin

How to fix one of Bitcoin's biggest problems

MIT professor Silvio Micali says his new system allows blockchains to operate efficiently at a large scale.

by **Mike Orcutt** Apr 23, 2018

Algorand™

La lezione del Prof. Silvio Micali a Milano

Fabio Tagliaferro @fab_iron_cutter · Jun 8

Fall 2018:
It took me less than 10 minutes to plan for a last-minute trip from Verona to Milan (with a night train to return!) as I got to know that Prof. @silviomicali was coming to talk about @Algorand
After a brief conversation and a handshake, I asked to join the community!

Il primo Algorand Dev meetup a Milano

Fabio Tagliaferro @fab_iron_cutter · Jun 8

Early 2019:
I was the host with Gianfranco Prini for the first Milan @Algorand Developer Meetup, it was a pleasure to meet @JasonWeathersby @_chrishurley

Algorand Ambassador a Budapest

Fabio Tagliaferro @fab_iron_cutter · Jun 20

Summer 2019:
Invited speaker for Open Blockchain Workshop Series at @EIT_Digital Budapest node
"@Algorand: the rise of a pure proof-of-stake blockchain"

Algorand™

L’innovazione tecnologica per la **borderless economy**

www.algorand.com

L’innovazione tecnologica per la borderless economy

PEOPLE

Un team di rinomati luminari

PLATFORM

Una tecnologia per decentralizzazione, scalabilità e sicurezza.

POSSIBILITY

Un business adatto a condurre l’innovazione

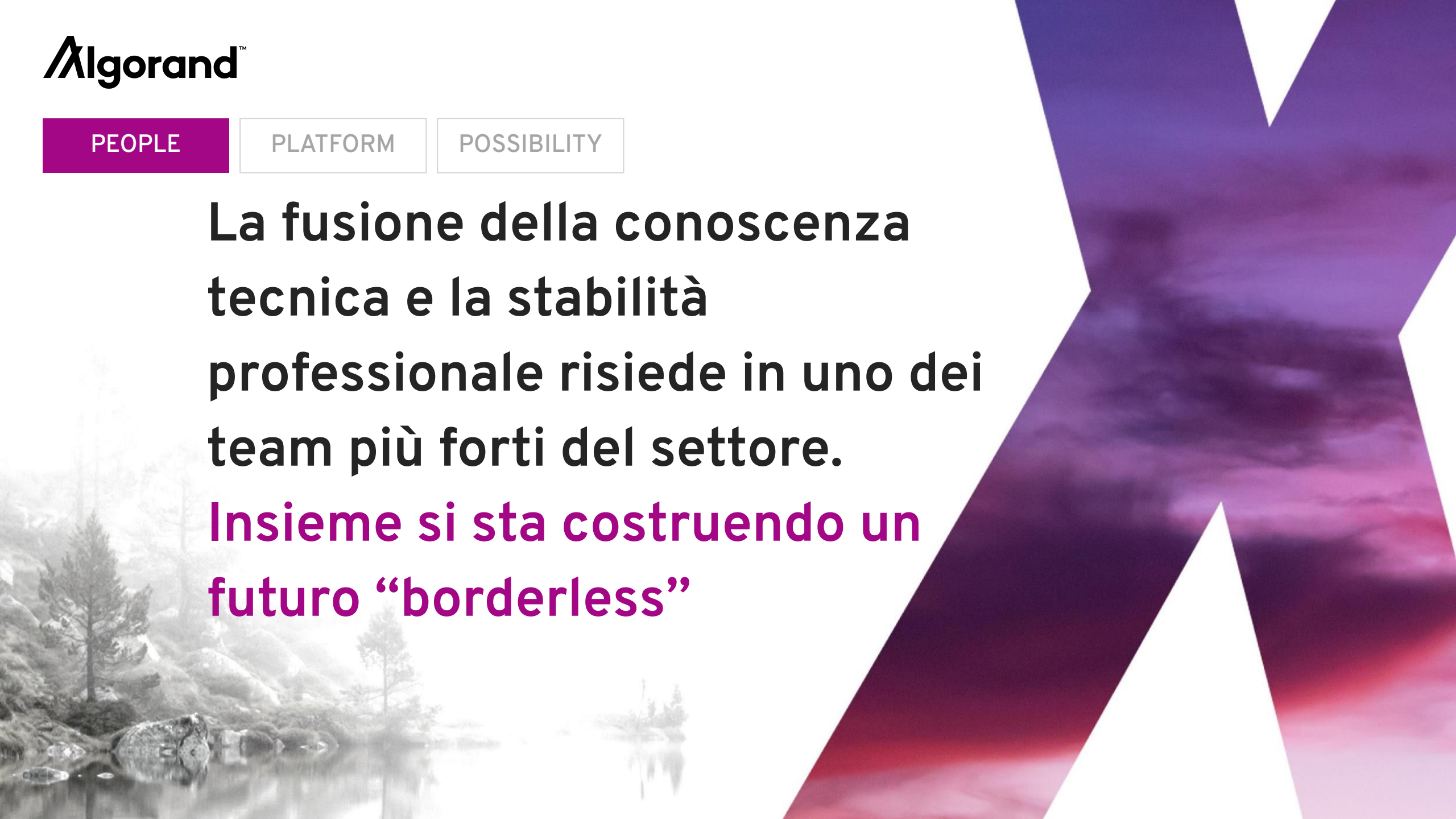
Algorand™

Algorand™

PEOPLE | PLATFORM | POSSIBILITY

La fusione della conoscenza tecnica e la stabilità professionale risiede in uno dei team più forti del settore.

Insieme si sta costruendo un futuro “borderless”



Team—Smart Science and Proven Leadership

Algorand Inc.

Silvio Micali
Founder

Cryptography pioneer

Turing Award winner

MIT professor

Massachusetts Institute of Technology

Steven Kokinos
CEO

fuze

bladelogic

Sean Ford
COO

LogMeIn

upromise

MONITOR GROUP

Algorand Foundation

Tal Rabin
Head of Research,
Research Fellow

IBM

International Association for Cryptologic Research

American Academy of Arts & Sciences

Hugo Krawczyk
Research Fellow

IBM

International Association for Cryptologic Research

Shai Halevi
Research Fellow

IBM

Massachusetts Institute of Technology

Algorand™

Technical Leadership Team

Jing Chen
Head of Theory Research and Chief Scientist

Massachusetts Institute of Technology

Yossi Gilad
Head of Systems Research and Chief Technology Officer

Massachusetts Institute of Technology

Sergey Gorbunov
Head of Cryptography

Massachusetts Institute of Technology

Naveed Ihsanullah
Head of Engineering Research

HARVARD UNIVERSITY

mozilla

Georgios Vlachos
Head of Mathematics

Massachusetts Institute of Technology

Nickolai Zeldovich
Head of Distributed Systems

Massachusetts Institute of Technology

Stanford University

Algorand™

PEOPLE | PLATFORM | POSSIBILITY

L’era per una economia decentralizzata e borderless è qui.

Algorand ne è la piattaforma.

Panoramica sui meccanismi di consenso distribuito per blockchain

Panoramica sui Meccanismi di Consenso

PROOF OF WORK

I nodi si sfidano sulla possibilità di poter “minare” un nuovo blocco tentando di risolvere un complesso puzzle computazionale.

- Spreco di capacità computazionali
- Alto costo di energia elettrica
- Concentrazione di potere e di fatto decentralizzazione, causata dal pooling delle risorse effettuato da mining farms
- Possibilità di forks la cui permanenza causa perdita di validità per blocchi in rami morti della blockchain
- Finalità delle transazioni ottenuta dopo un certo numero di blocchi confermati

Panoramica sui Meccanismi di Consenso

DELEGATED PROOF OF STAKE

Un numero fissato di entità elette vengono selezionati col compito di creare blocchi.

I “delegati” ottengono potere dagli utenti del network: ognuno dispone di un numero di voti proporzionale al numero di tokens che possiedono.

- Sacrificio dal punto di vista della centralizzazione porta a rischi legati alla sicurezza
- Nessuna garanzia che i delegati rimangano onesti
- Vulnerabilità ad attacchi come Fast Denial of Service (DoS) dato che i delegati sono conosciuti

Panoramica sui Meccanismi di Consenso

BONDED PROOF OF STAKE

Gli utenti possono bloccare parte dei token che possiedono per un certo periodo di tempo, per avere la possibilità di creare il prossimo blocco.

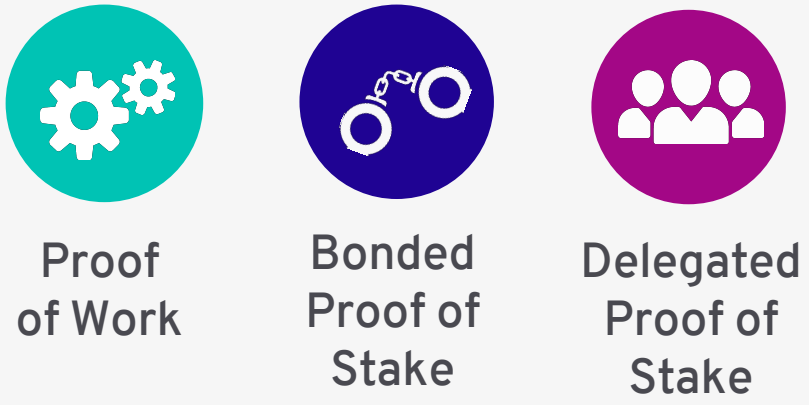
La probabilità di poterlo fare è proporzionale alla propria stake bloccata rispetto a quella bloccata dagli altri.

Gli utenti che agiscono in modo disonesto perderanno il loro deposito assieme alla possibilità di partecipare al meccanismo di consenso.

- Gli utenti hanno possibilità ridotta di spendere ciò che possiedono per partecipare al meccanismo di consenso

Panoramica sui Meccanismi di Consenso

I meccanismi di consenso di prima generazione hanno dei difetti



Proof of Work

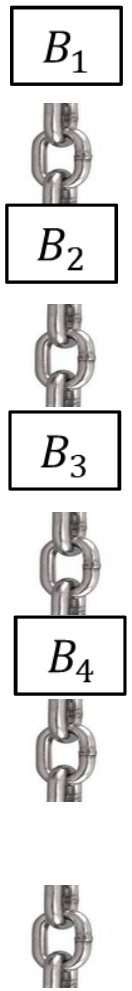
Bonded Proof of Stake

Delegated Proof of Stake

Pure Proof of Stake di Algorand

- Pubblico e Permissionless
- Tutti gli utenti possono partecipare al meccanismo di consenso
- Blocchi confermati con dei voti
- Ogni token ha lo stesso potere di voto
- Minima potenza computazionale richiesta
- Finalità istantanea dei blocchi

Ad alto livello: Pure Proof of Stake



1) Selezionare casualmente un piccolo comitato campionandolo dall'insieme di tutti gli utenti

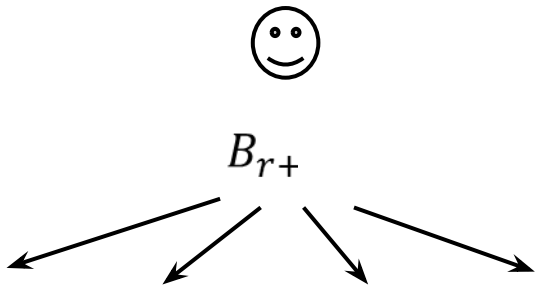
2) Se il comitato concorda sul nuovo blocco....

B_6

3) Il blocco viene aggiunto alla catena

Aggiungiamo dettagli: Pure Proof of Stake

= 1



un utente viene selezionato in modo casuale
-> probabilità proporzionale alla propria stake

l'utente propone un blocco e lo propaga al network
prima che questo avvenga, nessuno conosce il vincitore!

= 1K

allo stesso modo, selezione di un piccolo e casuale comitato

- Viene eseguito algoritmo di Byzantine Agreement sul nuovo blocco
- Il risultato viene firmato e aggregato
- Le firme digitali vengono propagate

Come funziona? Pure Proof Of Stake

Q: Chi seleziona il comitato?

A: **Ogni componente del comitato aveva seleziona se stesso!**

- Ognuno esegue la propria lotteria.
- La dimostrazione di aver vinto è costruibile solo dal vincitore.
- Chi vince propaga la prova della vittoria e partecipa al Byzantine Agreement

La probabilità di vittoria è proporzionale alla quantità di stake posseduta!

Q: Un avversario non potrebbe corrompere tutti i membri del comitato dopo il primo step?

A: **No, per ogni step c'è una commissione diversa!**

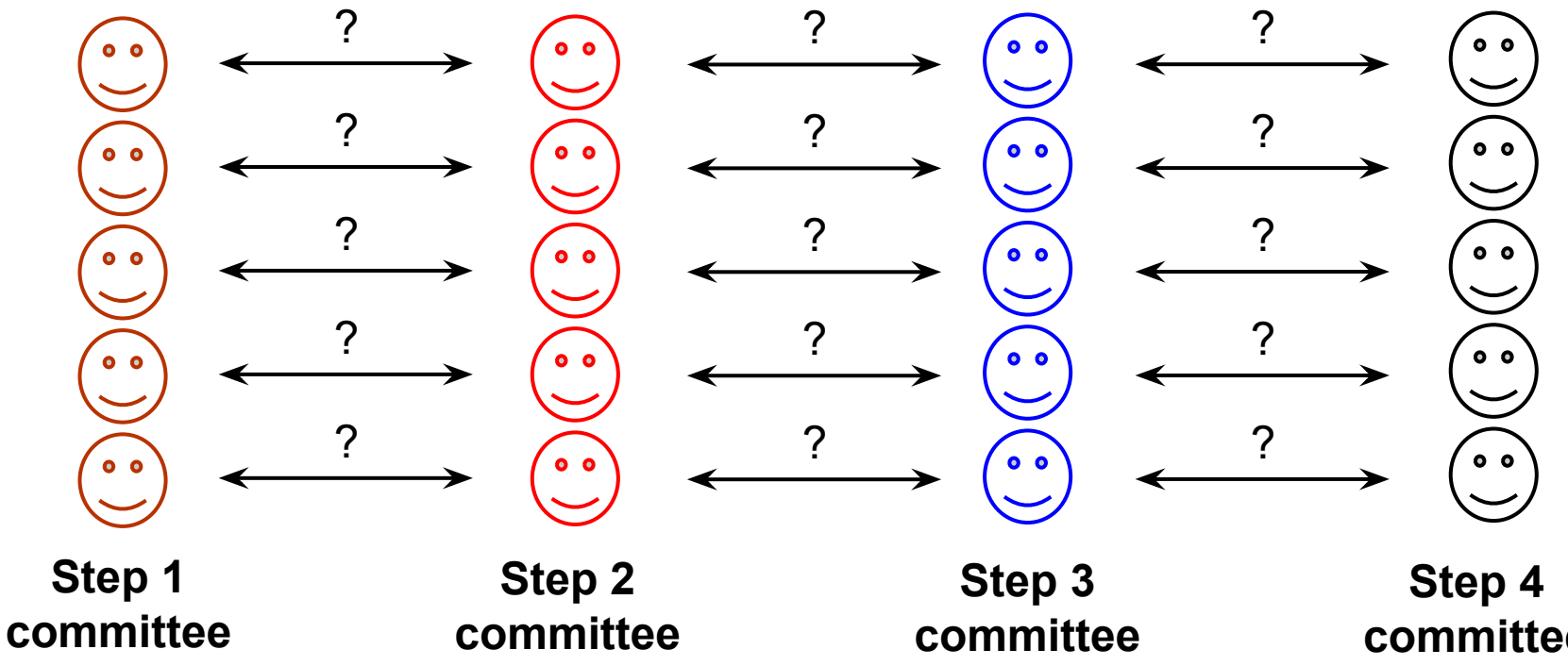
- Un membro di un comitato parla una sola volta, comunicando la prova di vittoria e il voto

Nuova Proprietà: User Replaceability

Selezione del Comitato: Pure Proof of Stake

Che relazione c'è tra i membri del comitato tra uno step e l'altro?

Nessuna!

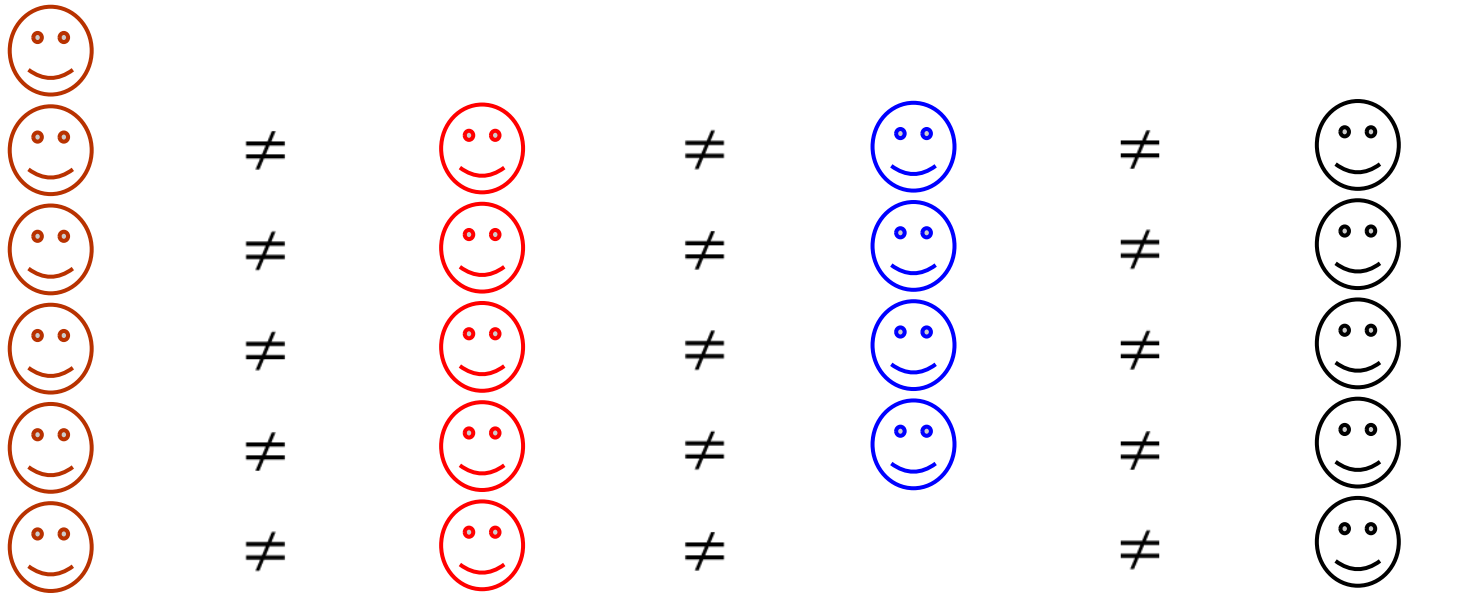


Selezione del Comitato: Pure Proof of Stake

tra uno step e l'altro...

- Partecipanti differenti
- Dimensione del comitato differente
- Non ci sono variabili condivise

ma l'ambiente è condiviso



Selezione del Comitato: Pure Proof of Stake

tra uno step e l'altro...

- Partecipanti differenti
- Dimensione del comitato differente
- Non ci sono variabili condivise

ma l'ambiente è condiviso

Risultato: comportarsi come un singolo comitato

DECENTRALIZZAZIONE

Algorand™

Pure Proof of Stake

- ✔ Consenso raggiunto in modo rapido ed efficiente
- ✔ Ai nuovi utenti minima o nulla penalità di performance
- ✔ Blocchi confermati in modo ottimizzato
- ✔ **Finalità istantanea delle transazioni**
- ✔ **Infima possibilità di forking**
- ✔ Sicurezza contro attacchi di protocollo e di network

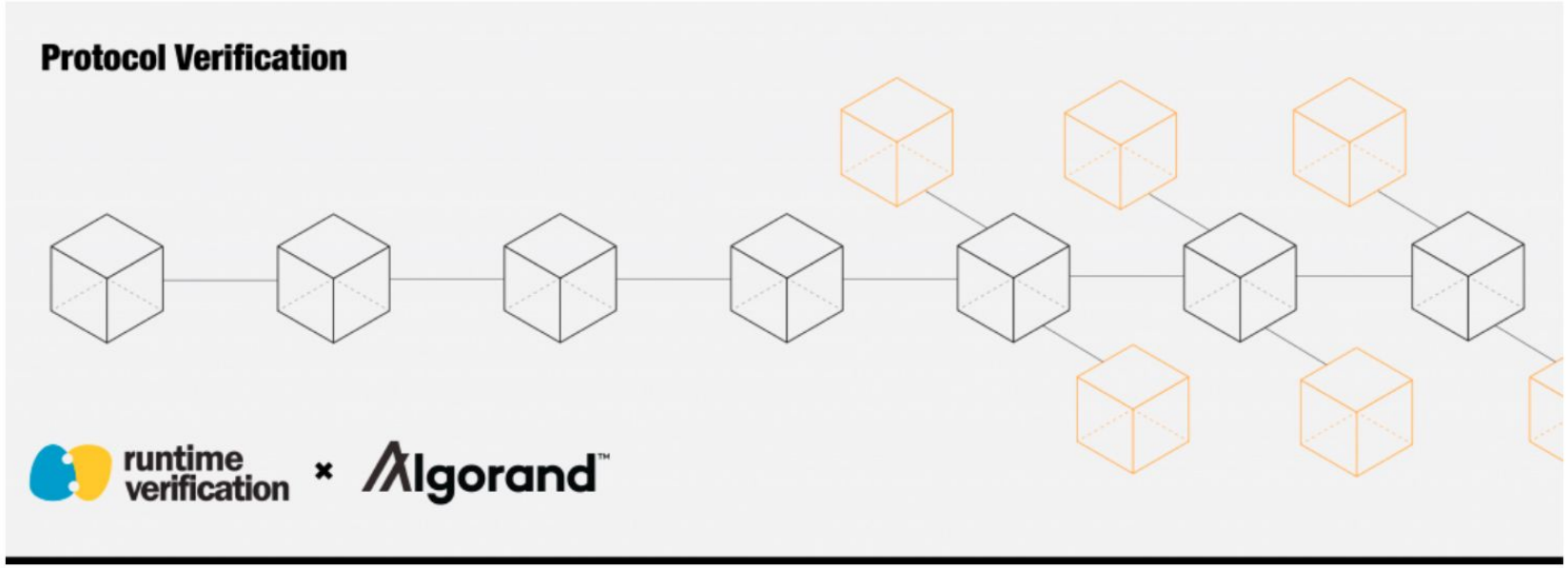
Algorand™

SCALABILITA' **SECURITY**

Dimostrazione della safety del protocollo

Formally Verifying Algorand: Reinforcing a Chain of Steel (Modeling and Safety)

Posted on June 18, 2019 by Musab Alturki



Alcuni degli strumenti crittografici usati

- **VERIFIABLE RANDOM FUNCTIONS PER SORTEGGIO CRITTOGRAFICO**

  rappresentare la popolazione selezionando casualmente un comitato campione di dimensione fissata
- **BONEH–LYNN–SHACHAM (BLS) SIGNATURES**

  raggruppare più transazioni nei blocchi comprimendo le firme
- **FORWARD SECRECY**

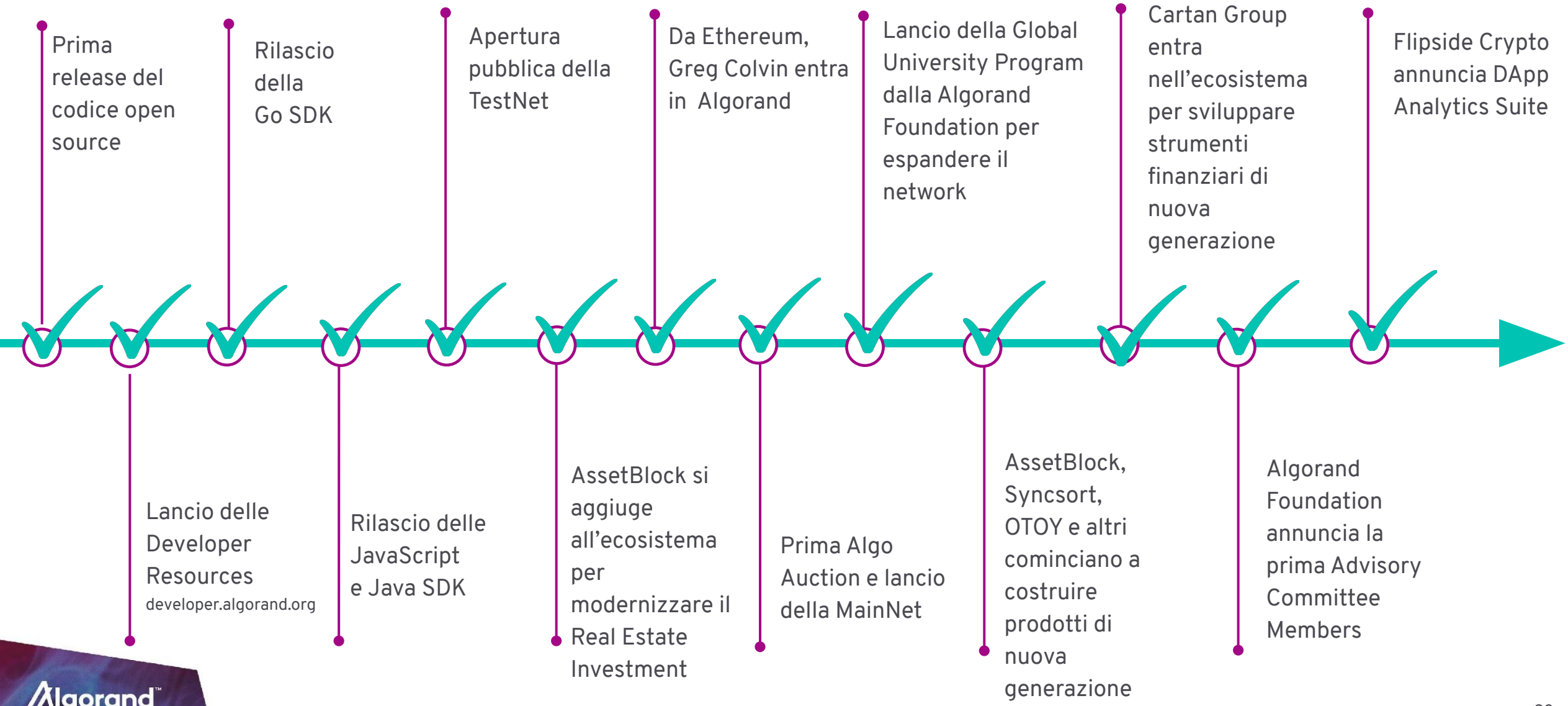
  associare la chiave segreta per ogni utente al numero di round, per poi eliminarla

Algorand™

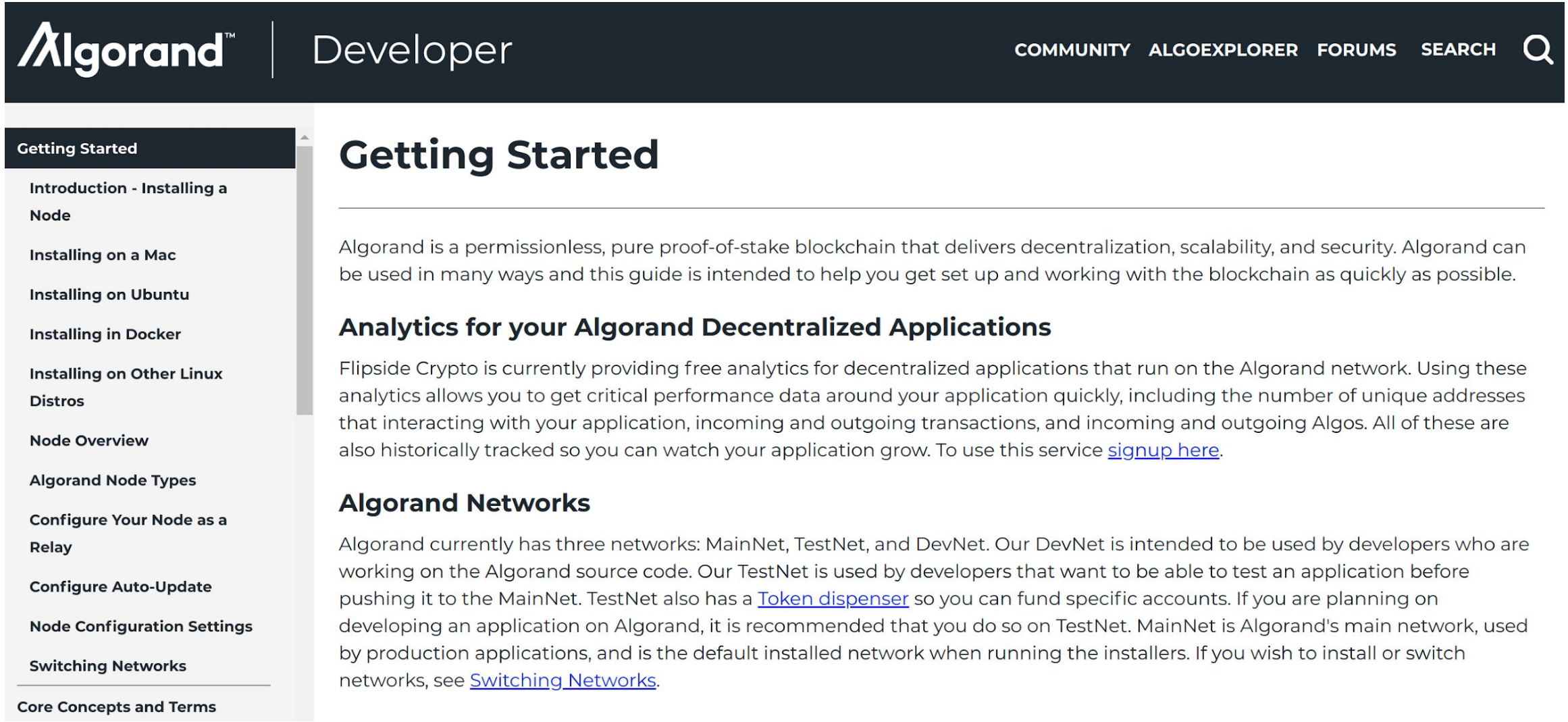
PEOPLE | PLATFORM | POSSIBILITY

Dopo anni di incertezze Algorand sta sviluppando un ecosistema dove la tecnologia per la borderless economy viene proposta come standard per blockchain.

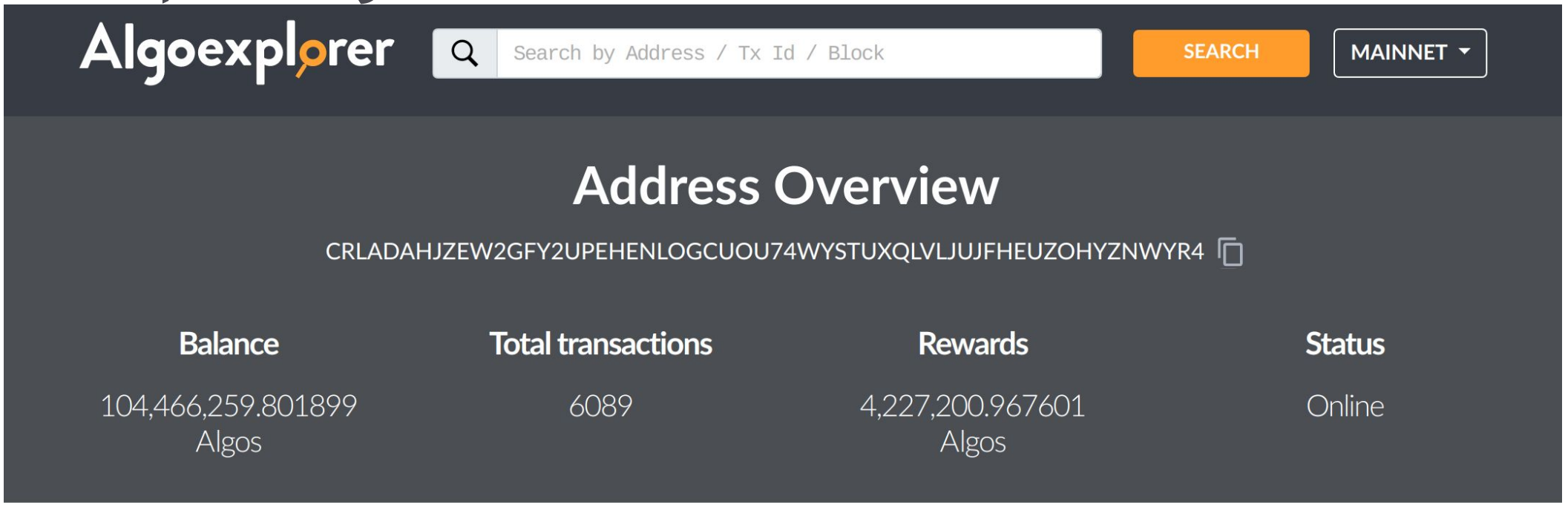
Timeline dell'ecosistema Algorand



Developer Resources



Explrer per Algorand



TRANSACTION DETAILS

TxID	Block	Age	From	To	Value	Fee
4SPSZPEJA7O3SQCNV2GYDY...	2605579	11 minutes ago	5TSQNIL54GB545B3WLC6OV...	CRLADAHJZEW2GFY2UPEHE...	0.000001 Algos	0.001 Algos
C4O7ZBAD4CAJINBDWZQR7...	2605103	about an hour ago	5TSQNIL54GB545B3WLC6OV...	CRLADAHJZEW2GFY2UPEHE...	0.000001 Algos	0.001 Algos
YTKN6ECJWWKV5X6ELQEX2...	2604627	about an hour ago	5TSQNIL54GB545B3WLC6OV...	CRLADAHJZEW2GFY2UPEHE...	0.000001 Algos	0.001 Algos

Sviluppare su Algorand

Telecommunications & E-Payments

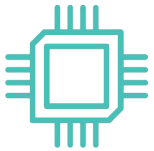
developing mobile payment system for millions of users

Insurance

serving people in underserved markets whose access to insurance is currently limited

Asset Tokenization

tokenizing real estate to give private investors access to real estate investments; also offering crypto holders loans for purchasing real estate



Media & Entertainment

making GPU rendering power more efficient for independent artists & major animation studios

Enterprise Solutions

creatively connecting legacy systems to the blockchain to leverage traditional investments

DApp Data Analytics

providing analytics suite offering visibility into how users are interacting with DApps on Algorand

L’ecosistema Algorand: numeri

100+

Meetups,
Conferenze globali

40,000+

followers

MIGLIAIA

di utenti nelle comunità online

50+

Algorand Ambassadors

47

officiali community chapters

Algorand™

Sostanziale crescita per le organizzazioni che sviluppano su Algorand

Algorand™

First Business Applications Built on Algorand

Roma, 6 Novembre 2019

Aziende partecipanti:

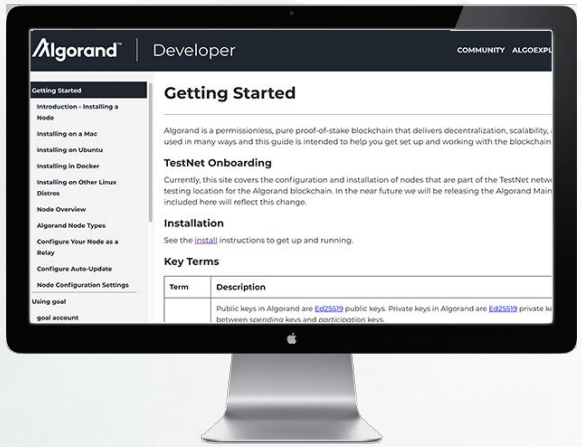
- Stonize
- GT50

Stiamo ridefinendo la tecnologia blockchain
Realizzare una nuova “borderless economy”

Follow Us!
@algorand

Join Us!
community.algorand.org

Build With Us!
developer.algorand.org



Algorand™

Algorand™

GRAZIE!


Algorand™
QUESTIONS?