# RAIDO
# network
# trusted crypto-ledger
# (RDO)

**ver.0.2 (23-dec-2020)**

White Paper may change depending on changes made by the community
to the logic of the network and other aspects

# Zusammenfassung

Wir präsentieren RAIDO - eine ultraschnelle Blockchain, die auf dem kryptografischen ECC-Verschlüsselungsstandard (Kryptographie mit elliptischen Kurven) basiert.

Alle heutigen Blockchain-Architekturen leiden unter einer Reihe von Herausforderungen, nicht zuletzt aufgrund der praktischen Möglichkeiten der Erweiterung, Skalierbarkeit, unvorhersehbaren Netzwerkgebühren, Verarbeitungsgeschwindigkeit usw. RAIDO Network setzt sich dafür ein, diese Herausforderungen zu bewältigen, indem die folgenden sieben Hauptvorteile geschaffen werden:

Skalierbarkeit. RAIDO Delegated Proof-of-stake (DPoS) Netzwerk Grundsatz ermöglicht, Verschwendung von Ressourcen bei der Verarbeitung von Transaktionen zu vermeiden, gleichzeitig wird ein hoher Systemdurchsatz für die Verarbeitung einer einzelnen Transaktion beibehalten und die Anzahl der Transaktionen, die unter Spitzenbedingungen verarbeitet werden können, auf bis zu 500 TX / s und mehr erhöht.

Verarbeitungsgeschwindigkeit. Ein Block wird geschafft, nachdem mindestens signierte Transaktion wird empfangen, wodurch eine schnelle Transaktionsbestätigung erstellt wird. So kann das Netzwerk verwendet werden, um sofortige digitale Zahlungssysteme zu implementieren.

Transaktionskosten. Die Transaktionskosten sind fest, wodurch die Umsetzung von Geschäftsprozessen basierend auf der Arbeit mit dem Netzwerk prognostiziert werden kann, einschließlich durch die Ausführung von ESCROW-Funktionen in Smart-Verträgen in den folgenden Versionen des Netzwerks.

Beteiligung am Management. Kryprowährungsbesitzer nehmen direkt an Abstimmung über Änderungen der Netzwerkparameter und die Umsetzung von Verbesserungen teil. Jedes Mitglied des Netzwerks kann bei der Annahme eines solchen Vorschlags auch Netzwerkverbesserungen für die Abstimmung mit einem Antrag auf Belohnung vorschlagen.

Gelegenheiten zur Verbesserung. Dank des Abstimmungsmechanismus und der Verbesserungsmöglichkeiten bleibt das Netzwerk für die Entwicklung und Anpassung im Laufe der Zeit flexibel. Alle Änderungen werden mit ausreichender Inklusivität und Transparenz vorgenommen, um eine effektive Verwaltung des dezentralen Systems sicherzustellen.

Anwendbarkeit. Die Technologie erfüllt den dringenden Bedarf an schnellen und sicheren Transaktionen und bildet die Grundlage für den Betrieb Smart-Contracts mit der Fähigkeit, externe Daten zu empfangen und zu verarbeiten.

Endemission. Die Abwesenheit der dynamischen Emission ermöglicht Wertminderung einer Rechnungseinheit infolge zusätzlicher Emissionen zu vermeiden.

## Netzwerkkonsens

Die Netzwerkeffektivität ist direkt mit zwei Hauptsachen der Konsensarchitektur verbunden, insbesondere: die Kanonizität und Verbesserung des Netzwerks unter Wahrung des Konsenses. Eine harmonische Kombination dieser Faktoren schafft

Möglichkeiten für effektive Netzwerkentwicklung, ohne Kompromisse bei Sicherheits- und Hardfork-Risiken einzugehen.

Ein wesentliches Problem bei DPoS-Netzwerken ist die mangelnde Automatisierung der Kommunikation zwischen Kryptowährungsbesitzer und Validatoren. In RAIDO Network wurde dieses Problem durch die Automatisierung der Stapelarbeiten gelöst.

## Transaktionskern

Der Transaktionskern der Blockchain wird als Monokettenarchitektur in einem abstrakten, rein funktionalen Modul implementiert. Durch die Minimierung der Funktionalität des Transaktionskerns wird ein hohes Maß an Sicherheit und Transaktionsgeschwindigkeit erreicht, während die praktischen Mittel zur Erweiterung des Kernels beibehalten werden.

Das Softwarepaket, das dank des DPoS-Netzwerkkonsensprotokolls abgeglichen wird, kann einen hohen Durchsatz erzielen, ohne die Verarbeitungskapazität zu erhöhen.

## Framework für ESCROW-Funktionalität

Die zweite Stufe der Netzwerkentwicklung ist das Schaffen des Frameworks für ESCROW-Smart-Contracts and und schnittstellenorientierte dezentrale Anwendungen mit ESCROW-Algorithmen und Funktionen zum Empfangen externer Daten. Die Umsetzung dieses Frameworks ermöglicht die Netzwerkbenutzung, mithilfe deren digitalen Verträge schnell durchgeführt werden können.

## Kryptographiealgorithmus

Das Raido-Netzwerk verwendet die allgemeinen Prinzipien des Standards (ECC - Elliptic Curve Cryptography) und benutzt dabei seine eigene praktische Methode zur Implementierung der Verschlüsselung innerhalb des Netzwerks.

Um Transaktionen zu bestätigen, der Edwards-curve Digital Signature Algorithm (EdDSA) wird verwendet - ein digitales Signaturschema, das benutzt eine Variante von einem auf eine elliptische Kurve basierte Shnor’s Schema.

Die optimale Kombination von Netzwerkprinzipien und Signaturalgorithmus gewährleistet eine hohe Effizienz.

### Öffentlicher Schlüssel

Der öffentliche Schlüssel im EdDSA-Schema ist der Punktschlüssel der Kurve $A \in E(\mathbb{F}_q)$ , der in b-Bits codiert ist.

### Signatur

Die EdDSA-Signatur in Meldung M durch den öffentlichen Schlüssel A ist ein Paar (R, S), das in 2b-Bits codiert ist, in 2b Bits codiert, Punkt der Kurve $R \in E(\mathbb{F}_q)$ und eine ganze Zahl $0 < S < \ell$, die die Verifizierungsgleichung erfüllt

$$2^c SB = 2^c R + 2^c H(R, A, M)A.$$

### Privater Schlüssel

Ein privater Schlüssel im EdDSA-Schema ist eine b-Bit-Zeichenfolge k, die einheitlich und zufällig ausgewählt werden muss. Der entsprechende öffentliche Schlüssel ist in diesem Fall $A = sB$, wo s = das niedrigstwertige b-Bit H (k) ist, das als Big-Endian-Ganzzahl interpretiert wird. Die Signatur der Nachricht M ist ein Paar (R, S), wobei R = rB für $r = H(H_{b,\ldots,2b-1}(k), M)$ und $S \equiv r + H(R, A, M)s \pmod{\ell}$

## Rechnungseinheit

Um das Problem der Berücksichtigung von Bruchwerten zu lösen, verwendet das Netzwerk nur Ganzzahlen.

### Quark der Netzwerkeinheit

1 Quark (Mindestwert of RDO digitale Währung) = 0,00000001 RDO

### Rechnungseinheit RDO

1 RDO = 100,000,000 Quark

## Transaktionen

Transaktionen werden mit einem privaten Schlüssel signiert. Transaktionen werden öffentlich validiert und enthalten die folgenden Komponenten:

**id:** ist eine eindeutige Kennzeichnung einer Transaktion, die im Rahmen des Algorithmus zugewiesen wird, wenn eine Transaktion an das Netzwerk gesendet wird

**input:** Transaktionseingaben die die folgenden Daten enthalten

> **transaction:** Hash der Transaktion, deren Ausgabe verwendet wird;
>
> **index:** die Seriennummer der Ausgabe, die in der aktuellen Transaktion verwendet wird;
>
> **amount**: der Eingabebetrag der Ausgabe, die in der aktuellen Transaktion verwendet wird;
>
> **address:** der öffentliche Schlüssel des Brieftaschenbesitzers der Fonds;
>
> **signature:** eine Transaktionssignatur, die mit einem privaten Schlüssel über einen Verschlüsselungsalgorithmus generiert wird, ist eine öffentliche Information, die zur Validierung der Transaktion erforderlich ist;

node (optional): die Masterknotenadresse, von der aus dem Abstecken durchgeführt wird;

outputs: Transaktionsausgaben, enthalten die folgenden Daten:

amount: Der Betrag, der gesendet werden soll, der Betrag muss der Ausgabebetrag um den Netzwerkgebührenwert unter dem Eingabebetrag liegen.;

address: die Adressen des Empfängers;

node (optional): die Masterknotenadresse, an der das Abstecken durchgeführt wird;

hash: eine Prüfsumme der Transaktionsdaten;

type: ein Transaktionstyp, der für die automatische Trennung von normalen Transaktionen und Servicetransaktionen erforderlich ist, gibt es im Netzwerk die folgenden Versionen der Transaktionstypen:

regular – eine regelmäßige Netzwerktransaktion;

reward – eine Belohnung für die Stakers;

fee – eine Belohnung für Masterknotenbesitzer;

An example of a regular transaction:


```
{
 "id": "de6b234e6c896f95524fef72fead47dd48bd41eb5f986227182cc5d28265f48b",
 "data": {
  "inputs": [
   {
    "index": 1,
    "amount": 9615310000000,
    "address":
"392bbad53749bec66276562d2857ee4ae1e77f5c808b66031834c57636152d93",
    "signature":
"7d04fc3cf93d6d5289ccd81b950766b52544d22f70d1c12f9b835553467fa09e23aa0
3b40d955c144a32be16da9a85e3b2960da3b42dc72d1e75aa3b7939270d",
    "transaction":
"88d95aee74459b794809a8d630a2944a3175687638879188fba047eaf35e9a83"
   }
  ],
  "outputs": [
   {
    "amount": 2300000000,
    "address":
"8479646a2b271a0c846a1093a23bccc2c0ffc557f981d3434315532602c0a5d5"
   },
   {
    "amount": 9613000000000,
    "address":
"392bbad53749bec66276562d2857ee4ae1e77f5c808b66031834c57636152d93"
   }
```

```
  ]
 },
 "hash":
"25a4782812d32d46184e175d9f684a1d6bc07b1228e5b722b5cc093c9c9648d2",
 "type": "regular"
}
```


## Blöcke

Der zugewiesene Masterknoten sucht nach Transaktionen. Wenn eine ausstehende Transaktion gefunden wird, wird ein Block erstellt. Damit ein Block konsistent erkannt wird, überprüft der Masterknoten die Transaktionsdaten im Block, die Prüfsumme und die Signaturen.

Jeder Block besteht aus folgenden Parametern:

Hash: ist ein Steuerwert, der die Ein- und Ausgabeparameter von Transaktionen enthält, die im Block enthalten sind, und ist auch die Blockkennung im Netzwerk;

index: die Seriennummer des Blocks im Netzwerk;

timestamp: Blockgenerierungszeit;

transactions: Informationen zu den verschachtelten Transaktionen;

Jeder Block enthält den Hash des vorherigen erfolgreich validierten Blocks

## Masterknoten (Validatoren)

Transaktionsbestätigungsmethode des delegierten Eigentumsnachweises (DPoS).

Transaktionsvalidierungsknoten sind Masterknoten mit Clustern. Masterknoten führen zwei Funktionen aus:

- Blockgenerierung aus validierten Transaktionen durch Überprüfen übereinstimmender Signaturen der im Block enthaltenen Transaktionen;

- Validierung von Blöcken: doppelte Verbrauchsprüfung, Hash-Matching, Signatur-Matching.

Beim Generieren eines Blocks wird der Netzwerkgebührenbetrag durch eine Transaktion vom Typ Gebühr generiert, deren Ziel der Masterknoten ist, der den Block gesammelt hat.

Der Masterknoten erhält die Validierung direkt nach Erhalt der delegierten RDOs. In der nächsten Version des Netzwerks wird ein Mechanismus zum Erstellen von Clustern in Masterknoten implementiert, die zu separaten Validierungsknoten werden, wenn sie mit einer bestimmten Anzahl delegierter RDOs gefüllt sind.

## Staking

Die Übertragung von Rechten wird von Validierungsknoten über Stake-Transaktionen ausgeübt, wo der RDO-Eigentümer den Betrag und die Adresse des Master-Knotens angibt. Die Stake-Transaktion realisiert, dass RDO zugunsten des angegebenen Master-Knotens gehalten wird.

Die Netzwerkprovision wird in Belohnungstransaktionen proportional zum Einsatzbetrag alle 32 vom Masterknoten erstellten Blöcke (Validierungszyklus) auf die Adressen der Staker verteilt. Der Master-Knoten sendet die Belohnungstransaktion mit den Adressen aller Staker nach Abschluss des nächsten Validierungszyklus.

Um eine Belohnung zu bekommen, muss der Besitzer das Steak während des ganzen Validierungszyklus behalten.

Der Algorithmus wird automatisch realisiert.

## Emission

Wenn ein Genesis-Block generiert wird, bildet das Netzwerk die endgültige Emission. Zusätzliche Emissionen sind nicht vorgesehen.

## RAIDO Foundation

Ein gemeinnütziger Verein, dessen Zweck ist, das RAIDO-Netzwerk zu pflegen und weiterzuentwickeln. Die Aktivitäten der RAIDO Foundation werden durch separate Dokumente geregelt, die nicht im Weißbuch enthalten sind.

### RAIDO Foundation Funktionen

- Durchführung von Konvertierungsvorgängen der Übergangszeit;

- Entwicklung und Unterstützung der Hauptkomponenten des Netzwerks;

- Einleitung der internen Abstimmung der Inhaber;

- Sachverstand über die vorgeschlagenen Änderungen und Verbesserungen des Netzwerks;

- Halten und gezielte Nutzung des RDO-Münzfonds.

### Treuhandfonds

Die RAIDO Foundation verfügt über einen RDO-Fonds, der die Umsetzung ihrer eigenen Funktionen finanzieren kann. Die nicht verteilte Emission bildet die Grundlage des Treuhandfonds. Gleichzeitig ist die RAIDO Foundation nicht berechtigt, die Mittel des Treuhandfonds für die Beteiligung an der internen Abstimmung zu nutzen.

Die jährliche Ausführung des Treuhandfonds im Rahmen der Notwendigkeit, das Netzwerk des Fonds auszubauen, sollte 20% seines Startwerts nicht überschreiten.

## Interne Abstimmung

Die Abstimmung im Netzwerk wird durch das Prinzip des Konsenses und der dezentralen Verwaltung implementiert. Die Implementierung des Abstimmungsmechanismus ist in der nächsten Version des Netzwerks vorgesehen.

Jeder RDO-Inhaber mit einer ausreichenden Anzahl von RDO kann an der Abstimmung teilnehmen.

Das Eigentum von 100 RDO gibt das Recht, 1 Stimme abzugeben. Ein Teilnehmer kann eine unbegrenzte Anzahl von Stimmen haben. Die Stimmen für den angegebenen Zeitraum werden gezählt.

Die Abstimmung muss mindestens 5 Tage vor der Abstimmung bekannt gegeben werden. Die Abstimmungsfrist ist in der Ankündigung auf der Website der Raido Foundation angegeben.

Um eine Abstimmung für erfolgreich zu erklären, ist die Hälfte derjenigen, die mit +1 Stimme gestimmt haben, erforderlich:

- Anpassung von Netzwerkvariablen, einschließlich Netzwerkkomission, Blockgenerierungszeit, Mindestbetrag für das Abstecken, Masterknotenprovision, Clustergröße usw.;

- Hinzufügen von Änderungen am Rahmen und an der Arbeitslogik von Smart-Verträgen und externen Anwendungen;

- Hinzufügen von Änderungen zur Service-Infrastruktur;

- Umgang mit organisatorischen Fragen, die nicht mit der technischen Seite der Netzwerkarbeit zusammenhängen;

- Hinzufügen von Änderungen zum Netzwerkkern.

### Fragen, über die nicht abgestimmt werden kann:

- Änderungen, die die Sicherheit und Integrität des Netzwerks gefährden können;

- Einführung zusätzlicher Emissions-RDO.

## Übergangsphase

Die Implementierungsperiode des Übergangs von RF-Token vom ERC20-Standard zu einem eigenen Netzwerk, in der eine angemessene Umwandlung alter Token in neuen Münzen implementiert wird.