*smart cities*

MDPI

*Article*

# Smart Accounts for Decentralized Governance on Smart Cities

**Vitor N. Coelho [1,*], Thays A. Oliveira [1], Wellington Tavares [2] and Igor M. Coelho [3]**

[1] OptBlocks Consultoria Ltda., Avenida João Pinheiro, 274 Sala 201—Lourdes, Belo Horizonte 30130-186, Brazil; thays@optblocks.com
[2] Department of Public Management, Universidade Federal de Ouro Preto, Campus Universitário Morro do Cruzeiro, Ouro Preto 35400-000, Brazil; wellington@ufop.edu.br
[3] Institute of Computing, Universidade Federal Fluminense, Av. Gal. Milton Tavares de Souza, São Domingos, Niterói 24210-310, Brazil; imcoelho@ic.uff.br
* Correspondence: vncoelho@gmail.com or vncoelho@optblocks.com

**Abstract:** This paper introduces state-of-the-art possibilities for using smart contracts capabilities for governance. Assisted by blockchain, the use of these tools can provide a transition that society currently needs due the huge amount of information that reaches citizens. The core mechanism of this study lies within the scope of smart accounts and digital identities. These topics enclose smart cities trends that seek to increase citizens' participation in the social decision making process, in a transparent way that is usually managed throughout decentralized systems. We define a set of available features that can automatically guide the flow of resources, after the conclusions of voting processes also conducted on trusted environments of distributed ledgers. By presenting innovative ideas and didactically describing the possibilities, we aim to promote awareness of blockchain capabilities among readers, students, decisions makers and, mainly, the younger generation.

**Keywords:** e-governance; d-governance; blockchain; distributed ledgers; smart contract; smart accounts; digital identity; voting

**Key Contribution:** Discusses the potential that smart contracts specifically designed for managing public funds have on the scope of smart cities. Contributes with an updated vision on digital identities. Introduces smart accounts and its distinct future applications.

check for updates

**Citation:** Coelho, V.N.; Oliveira, T.A.; Tavares, W.; Coelho, I.M. Smart Accounts for Decentralized Governance on Smart Cities. *Smart Cities* **2021**, *4*, 881–893. https://doi.org/10.3390/smartcities4020045

Academic Editor: Pierluigi Siano

Received: 30 March 2021
Accepted: 26 May 2021
Published: 30 May 2021



## 1. Introduction

Modern sets of tools, mostly open-source, are bringing the possibility of using technology that was, just a couple of years ago, restricted to special applications and a few individuals in society. One of the implications of spreading the access of these tools is the creation of awareness about how software can boost transparency and trust. Among those technologies, cryptography operations are a set of tools that are now becoming widely available from simple communication applications to the new world of blockchain.

Throughout history, ciphers and other forms of cryptography have been used by poets, emperors, artists and craftsmen in order to protected information [1]. Currently, its use has been extended as requirements of distinct applications that are daily accessed such digital public key certificates such as TLS [2,3]. Those are core components for moving towards the social need of promoting Decentralized Governance (d-Governance), which has connections with the scope of Smart Cities (SC) [4]. The core of any form of governance lies on negotiation. In the field of Multi-Agent Systems (MAS) [5], negotiation is also the core for reaching agreements and usually involves voting, bargain or auctions. Distributed computing relies on these pillar when they need to reach agreements. What has changed now, with recent advances on cryptography and blockchain, is the transparency and openness surrounding those operations. From Internet-of-Things (IoT) [6] equipment to the power that Internet-of-Value (IoV) [7] can bring to society,

blockchain has been flooding computer scientists with cutting-edge tools. There is no single definition and ideal understanding of the smart city in the literature and, moreover, the very existence of a smart city is discussed by many authors. Therefore, there is a great complexity, both theoretical and empirical, regarding the emergence of artificial intelligence in cities. The doubts surpass the theories and empirical studies currently present in urban studies. However, the vast majority of concepts bring together similar aspects that allow a better understanding of the topic, as proposed by ([8] pp. 1–2), "the portfolio of a smart city normally includes smart grids, smart sensors and IoT technologies, deployed to produce large volumes of data on the metabolism of cities regarding, for instance, energy consumption and mobility". According to the smart urbanism approach, the use of big data aims to create scientific understanding of how to improve cities and their sustainability. Smart city projects are powered by rapid technological innovation processes. In this way, as a new type of smart urban technology enters the market, the dynamics of smart urbanism are consequently changed [8].

On another innovation front, SC [9] concepts involves optimizations on cities' daily services and interaction with services, while blockchain adds trust in the flow of information and data storage. In this paper, we emphasize how these tools can guide governance in smart cities in a way to manage, audit and control funds. For this reason, we introduce a new mechanism for automatically creating smart accounts, defined as SMart ACcount COmposer (SMACCO). As described in the study of Oliveira et al. [7], there are different layers of challenges for connecting citizens and technology on smart cities, and, surely, governance is a key aspect of it. The extrapolation of smart cities tools for e-governance has a disruptive potential [10] for changing the relationship between decision makers and citizens. Distinct platforms and framework are boosting social participation [11]. On the other hand, the use of blockchain, and tools such as the one introduced in this paper, has the potential of connecting e-governance with a concrete way for managing funds and controlled contract accesses for public assets in a transparent way. Motivated by a global effort in digitalization and social participation, we present arguments and a cutting-edge technology that the authors have been working on and investigating over these last few years.

The remainder of this paper has four sections. Section 2 emphasizes the emergence of e-governance concepts with the rise of the Internet. Section 3 presents a background on blockchain and its role for trustless systems. Digital identities are introduced at Section 3.3, presenting a real case of study about the development on a public Blockchain. Section 3.4 presents the framework for creating Smart Accounts (SA). Section 4 presents the innovative connection between smart accounts and decentralized governance, presenting a perspective for its use on the scope of smart cities. Finally, Section 5 draws final considerations and possible future research directions that may involve policy and development of products connected with the smart cities trend.

## 2. Internet and the Rise of e-Governance

Smart cities cover governance and the way citizens interact with services [7]. Political representation is strongly impacted by a change on this infrastructure, which has been historically linked exclusively to political parties [12]. In this context, the communication advances by creating autonomous and democratic public spaces that favor the free flow of information, opening possibilities to debate the social problems and the formation of critical public opinion [13].

To develop and evolve, cyberdemocracy [14] depends on its own practice. There are few experiences and little commitment to affect the institutions and current processes, but it is important to think in balanced sociopolitical transformations. In a long-term vision, it is necessary to think in terms of Information and Communication Technologies (ICT) as a way to break the technological and procedural limitations [15]. Thus, the creation of tools that assist decision making can promote adoption that increases transparency and reduces undesired costs.

Between the democratic possibilities that the Internet grants, there may be empowerment of political parties, activists, and interest groups, especially those that mass media ignores or diminishes, such as indigenous people who are gaining access to several forms of modern technology. The actual evidence indicates that many changes are caused by the Internet, for example, in the way people conduct social and business relations. However, there is still no great impact on political participation or political power redistribution [16]. In this regard, this work contributes to discuss tools that directly impact the political participation in a manner to control public funds (as well as private funds, which can be safely managed throughout the use of smart contracts).

On the other hand, political practices in the Internet can follow a similar course as the business practices that have been adjusting to the virtual environment, such as in the current COVID-19 pandemic. In Brazil, the Supreme Court has been conducting virtual meetings in order to keep the process judgements and discussions during the COVID-19 pandemic. Around the globe, other instances of the legislative and judiciary power are also moving to Internet-based home-offices. All these changes have potential to strengthen open spaces for discussions and to increase the number of citizens interested in participating in web politics [17]. Coelho et al. [18] described a system that could handle legislative and judicial processes with social participation throughout a multi-criteria analysis of all persons involved in the process. However, no work from the literature has yet tackled how this modern concept of digital interaction can be boosted in a direct way to motivate society to handle the economic aspects of the current political administration.

The Internet has been proportioning the creation and development of a series of tools by the government, which provide conditions to maintain the electronic governance. Some of the landmarks are: in 1994, in Minnesota (USA), the Minnesota e-democracy emerged to provide information about candidates and their proposals [19]; in the USA, possibilities were opened for citizens to express their opinions and debate local political questions in different spheres; in the United Kingdom, the *UK Citizens Online Democracy* was created in order to connect information and promote an open space for political debating [20]; in 2003, the European Union launched the vote for the *EU We Want*, a space of supra state interest to increase citizens participation and allow votes on topics of citizens' interests [21]. Despite a constant fight between involved agents, the democratic process has been based on innovative forms of participation, which go from the incorporation of new tools and social actors to the redefinition of identities and affiliations, especially the local ones [22].

The online participation forms became part of the debate about the Internet's potential to promote transformations in the democratic context, making the political engagement more tangible. The changes happen, especially, by the growth of virtual communities and collaborative platforms, for example, by political blogs and social networks [23]. As a result of these and other experiences around the world, it becomes clearer that when the participation is important and diversified, the Internet has the potential to became a relevant debate arena. In such cases, it can contribute for the propagation of deliberative values for different opinions and decision levels. The discussion scenario in the Internet can be strengthened as communication is facilitated and a variety of topics can come up for discussion. This is connected with Liquid Democracy [24,25], which involves voting pools using an open-source software *LiquidFeedback*. These concepts also have potential for being extended to blockchain [26], which is related with discussions introduced in this current paper.

## 3. Decentralized Governance: Blockchain and the Rise of Trusted e-Governance

The pioneer efforts on Bitcoin [27] were focused on creating the basis for a network able to automatically perform cryptographic transfer of a digital asset, namely Bitcoin. Bitcoins are created in a systematic Proof-of-Work (PoW) mechanism, in which coins are forged every 10 min following the original protocol. As more hashing power is

connected to the network (there are more computers mining or the hardware has been improved) blocks are found easier (lower times). However, the protocol is able to adjust the difficulty of the PoW algorithm in order to keep the generation of each block every 10 min. Thus, as soon as more hashing power is added, the network adjusts its difficulty in order to keep the standard 10 min blocks. On the other hand, when hashing power is reduced, the network will deterministically reduce its mining difficulty. Currently, around March 2021, the current hashing power has already reached 150 Exa Hash [28].

The simplicity of Bitcoin's design allows massive decentralization and the ability to boost the industry to create dedicated hardware for mining the network challenge. However, it has physicals limitations and implied energy costs are boosting the use of other innovative consensus mechanisms such as the Delegated Byzantine Fault Tolerant (dBFT), an algorithm developed for the NEO Blockchain [29]. The latter is a pioneer algorithm inspired on the Practical BFT and is able to generate one-finality blocks, which, differently than bitcoin, can never be reversed (see *Bitcoin Deep Chain Reorganization* [30]).

Bitcoin brought with it the concept of Smart Contracts, which involves the creation of personalized scripts that deterministically executes instructions according to specific parameters inputs. On the other hand, more complex scripts required the use of Turing Complete mechanisms, in which NEO Blockchain and Ethereum [31] provided such solutions with their loop-based virtual machines. These extensions provide flexibility but more complexity in the security system and programming languages.

The existence of different paradigms allows competition and costs to be reduced, while the trust can still be chosen according to the application needs. In this section, we introduce the label d-Governance (Section 3.1) as a decentralized trusted e-Governance, in a way to emphasize what Blockchain is bringing to governance systems. When we mention Blockchain for governance, a key point is the Digital Identities, presented and discussed at Section 3.3. Added to this, governance often has the requirement to distribute and manage resources. In this sense, smart contracts for managing decisions and automatic guide the use of resources are introduced in Section 3.4.

### *3.1. Blockchain and Trust*

Trust, in the first view, surely involves the certainty in which parties are allowed to participate. For some cases, once allowed, their identity is not of great importance since trust is inherent to the result.

In modern systems, such as a distributed ledger, the trust is then obtained by a combination of cryptographic operations linked with timestamps and agreements made via consensus protocols. For achieving a combination of efficiency and trust, the use of private and public chains is surely suitable. The fully distributed architecture of well-recognized blockchain networks provides redundancy. On such cases, certificates are publicly available, ensuring the state of the information publicly while the private chain ensures a better cost performance. In addition, on private networks, specific stakeholders can play a crucial role for dividing the burden of handling the information. Considering each country and its specific regulations, advances towards private chains are surely necessary for replacing historical ICT infrastructures that has been running on public administration and banks.

According to each application and jurisdiction, after the voting process, citizens should not be allowed to disclose their voting due to distinct political reasons. It is even possible, with cutting-edge technologies, such as Shamir Secret [32] and other Homomorphic Encryption [33] techniques, that we block individuals to prove their decisions without an approval of other involved parties.

Blockchain, in any form, can provide the trust defined in its protocol. Users and entities needs to be aware about its limitations and specifications. Different models and systems have distinct requirements for achieving trust and, basically, we can summarize this feature similarly as the double-spending of assets, which most of the blockchains always try to solve and handle. Considering this basic structure composed of consensus

mechanisms, plus accounts and operations that are cryptographically safe, we can achieve the desired level of trust that we are searching for, exemplifying the potential applications of the smart accounts described in this paper.

### *3.2. On the Importance of Security*

In our perspective, it is not possible to reverse the smart city agenda, with a view to the adoption of technologies and strategies by municipal authorities worldwide, but it is not too late to recognize vulnerabilities, threats and security risks, so as to develop mitigation strategies for these issues. The problem is that not enough has been done to reduce security risks, and discussions about security and infrastructure have been ignored in the social sciences and urban studies, being left to the responsibility of computer science, engineering and market solutions, for example. Building smart cities cannot be reduced to creating a system of systems, but it requires an understanding of the city as a whole, as a diverse set of places that concern not only the technical aspect, but the potential social and economic consequences of risks and opportunities of security and smart urbanism [34].

A current problem that promises to increase in the future are the vulnerabilities of smart cities, cyberattacks and cyberterrorism. According to Kitchin and Dodge ([34] p. 61), "present strategies for addressing the vulnerabilities and risks posed by the mass adoption of networked technologies for city management are woefully inadequate and predominantly rely on existing technical and training mitigation strategies and market-led solutions". In their work, they advocate a series of actions necessary to increase the security of smart cities, such as:

(a) That mitigation strategies are expanded and deepened, including security for all acquisitions focused on infrastructure;
(b) The carrying out of a wide evaluation of the urban infrastructures and information systems that already exist, as well as the correction or replacement of corrective security, the formation of central security and computer emergency response teams of the city administrations;
(c) A radical change in safety training and continuous professional development in the public and commercial sectors, creating a context that is not simply led by the market, but that is managed and supervised broadly and actively in accordance with the best safety standards practices, municipal policy and third-party service contracts;
(d) That greater and more serious attention be given to the preventive approach to security, not only to the most urgent ones as is normally the case, but to simple issues that can result in future problems;
(e) The use of blockchains for access, control and authentication, as well as other technical solutions that reduce the vulnerabilities of smart cities.

In this sense, we highlight one extra action topic, related to the security of private information of citizens, as preventing citizen privacy violation and sensitive information disclosure may ultimately be related to adopting privacy-by-design principles [35], which is within the scope of modern blockchain-based digital identity protocols.

### *3.3. On the Importance of Digital Identities*

The use of Digital Identities is an emerging set of features that has been recently under consideration for distinct applications. For now, let us consider that we have an identity with those two desired properties:

**Definition 1** (Self-Sovereignty)**.** *A digital identity provides self-sovereignty over personal data.*

**Definition 2** (Anonymity)**.** *A digital identity has to ensure optional anonymity.*

Since its creation, NEO Blockchain proposed in its White Paper [29] the use of NEO-ID. Neo Core Developers and the Community plan to chose an embedded protocol for Digital Identity for running native on the public Blockchain. Currently, there are three different proposals for managing digital identities on a public blockchain [36–38]. A discussion that may possible select the most suitable Digital Identity proposal to be natively embedded on Neo Blockchain can be seen in the Github. https://github.com/neo-project/neo/issues/1304 (accessed on 5 April 2021) .

AthenaID is designed by Neo Global Development team, presented in the first line of Table 1, and suggests to provides a transformation from "trust or not" into "how much trust". It also comments about subjectiveness, providing a system that enables different evaluation results under the same conditions according to the entity. SeraphID is designed by Swisscom Blockchain, and has a variety of options with the simplicity of just four roles with basic functions. VividID is designed by Moonlight, and also has a good simplicity and an interesting scheme for Profiles and access grants. On the other hand, as highlighted, the last two would not provide a direct access for reputation systems, which provides good possibilities for several systems, such as an online journal that needs a peer-review process.

**Table 1.** Comparisons of proposed digital identities for Neo Blockchain.

| Proposal | Features | Advantages | Disadvantages |
| --- | --- | --- | --- |
| **AthenaID** [36] | • Basic functions (issue, verify and manage);<br>• Trust value provided by different entities (trustor; trustee and recommender);<br>• Limited scope of authorization per identity;<br>• Game model for user behavior. | Interesting and innovative Trust Graph system, which provides scalability and different levels of trust. There is also a novel game theory model for governance, in which entities will have reason to engage in trustworthy behavior and be deterred from malicious activities. | It is more complicated to be implemented. |
| **SeraphID** [38] | • Basic functions (issue, verify and manage); | Its simplicity in implementation and solid defined roles (issuer, verifier, holder and root-of-trust manager). | Can not be directly used in scenarios such as reputation systems. |
| **VividID** [37] | • Basic functions (issue, verify and manage);<br>• Different grant access (read, write and admin) throughout claims;<br>• Different encryption formats; | Proposes the definition of a structure for Claims as an Standard of the Neo Blockchain; Native use of Profiles which grants an entity the possibility to access a collection of attestations together. | Can not be directly used in scenarios such as reputation systems. |

### *3.4. Smart Accounts for Assets Management*

Smart contracts connect codes to a generic virtual machines which can execute arbitrary logic, while smart accounts are created with a framework introduced in this work that involves a simple JavaScript Object Notation (JSON). This simple JSON notation can be seen as a programming language for assets management. From the JSON specification with the desired smart account features, a C# is generated, thus, the JSON's smart accounts are translated into standard smart contracts codes. In this direction, we propose a tool for generating smart accounts called SMart ACcount COmposer (SMACCO), that can be found available at https://neoresearch.io/smacco/(The current (accessed on 5 April 2021). open-source code of SMACCO is hosted at Github:

https://github.com/NeoResearch/neo-smacco for the code; and https://github.com/NeoResearch/smacco for the website (accessed on 5 April 2021)). For instance, the code presented in Algorithm 1 exemplifies the most simple account type, which is a basic *IF* that checks if the account signature is correct (using the *CHECKSIG* operation code), as illustrated at Figure 1.

**Algorithm 1** Code in JSON format for a simple single account.

```
{
  "standard": "smacco-1.0",
  "input_type": "single",
  "pubkey_list": [
    "036245f426b4522e8a2901be6ccc1f71e37dc376726cc6665d80c5997e240568fb"
  ],
  "rule": {
    "rule_type": "ALLOW_IF",
    "condition": {
      "condition_type": "CHECKSIG"
    }
  }
}
```

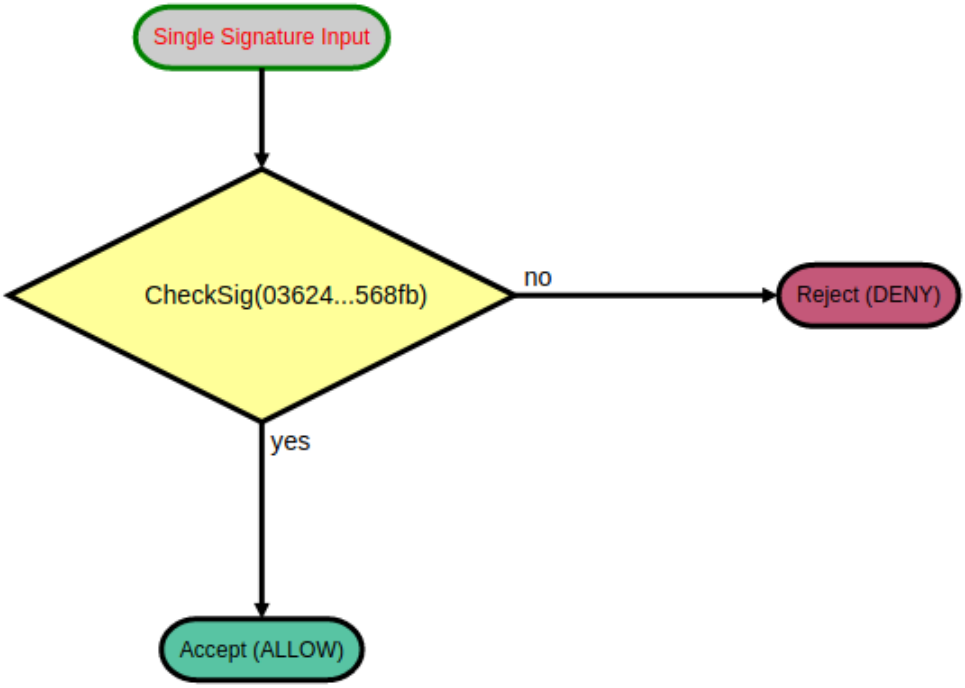


**Figure 1.** Flowchart of the single account presented in Algorithm 1.

Time conditions are also of crucial importance and they can define how funds are only allowed to be used after a certain period, as described in the code outlined at Algorithm 2 and illustrated at Figure 2.

**Algorithm 2** Code in JSON format for a time locked single account.

```
{
  "standard": "smacco-1.0",
  "input_type": "single",
  "pubkey_list": [
    "036245f426b4522e8a2901be6ccc1f71e37dc376726cc6665d80c5997e240568fb"
  ],
  "rules": [
    {
      "rule_type": "DENY_IF",
      "condition": {
        "condition_type": "TIMESTAMP_LESS",
        "timestamp": "1612996190"
      }
    },
    {
      "rule_type": "ALLOW_IF",
      "condition": {
        "condition_type": "CHECKSIG"
      }
    }
  ]
}
```

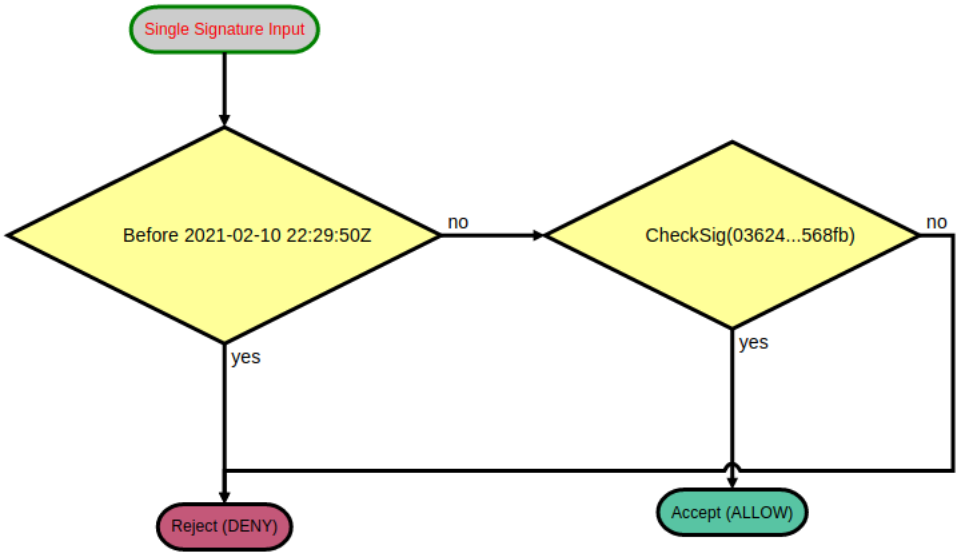


**Figure 2.** Flowchart of the time locked account presented in Algorithm 2.

For completing our basic set of desired features, we also need multi-signature accounts, which allow funds to be spent when a required number of signatures is provided, as detailed in the code presented at Algorithm 3 and Figure 3. Algorithm 4 also indicates the equivalent C# smart contract that could be used on the Neo blockchain, generated from this multi signature JSON specification.

**Algorithm 3** Code in JSON format for a multi signature account.

```
{
  "standard": "smacco-1.0",
  "input_type": "array",
  "pubkey_list": [
    "036245f426b4522e8a2901be6ccc1f71e37dc376726cc6665d80c5997e240568fb",
    "0303897394935bb5418b1c1c4cf35513e276c6bd313ddd1330f113ec3dc34fbd0d",
    "02e2baf21e36df2007189d05b9e682f4192a101dcdf07eed7d6313625a930874b4"
  ],
  "rule": {
    "rule_type": "ALLOW_IF",
    "condition": {
      "condition_type": "CHECKMULTISIG",
      "minimum_required": "2"
    }
  }
}
```

**Algorithm 4** Smart Contract code in C# that is equivalent to the smart account generated for the multi signature example.

```
using Neo.SmartContract.Framework;
using Neo.SmartContract.Framework.Services.Neo;
using Neo.SmartContract.Framework.Services.System;

namespace NeoContract1 {
    public class Contract1 : SmartContract {
        public static readonly byte[] pubkey_0 =
        "036245f426b4522e8a2901be6ccc1f71e37dc376726cc6665d80c5997e240568fb".HexToBytes();
        public static readonly byte[] pubkey_1 =
        "0303897394935bb5418b1c1c4cf35513e276c6bd313ddd1330f113ec3dc34fbd0d".HexToBytes();
        public static readonly byte[] pubkey_2 =
        "02e2baf21e36df2007189d05b9e682f4192a101dcdf07eed7d6313625a930874b4".HexToBytes();

        public static bool CheckMultiSig2_3(byte[][] signatures){
            byte[][] vpub = new[] {pubkey_0, pubkey_1, pubkey_2};
            byte[][] vsig = new[] {signatures[0], signatures[1]};
            return VerifySignatures(vsig, vpub);
        }

        public static bool Main(byte[][] signatures){
            return (CheckMultiSig2_3(signatures));
        }
    }
}
```

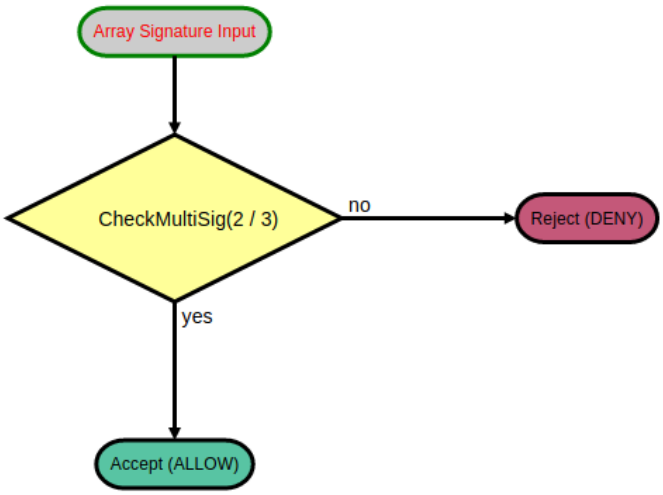


**Figure 3.** Flowchart of the multi signature account presented in Algorithm 3.

## 4. Smart Accounts and Decentralized Governance

Smart accounts were introduced as a tool for managing digital assets, while governance was contextualized with most recent advances on digital democracy, blockchain and digital identities. Summing up all of these concepts, this section emphasizes the possibility of creating a new paradigm of decentralized governance, which is aligned with the scope of smart cities. Decentralized governance is achieved with a combination of tools that promotes an environment that is transparent and respect citizens wishes such as privacy, furthermore, it is cost efficient and easy to access.

In addition, if we add voting features to the aforementioned smart account, we could introduce a system in which voting can happen in order to enable flow funds of an economic proposal. The idea is that an election would be a selection of projects, and voting would automatically enable this flow of money. The system should not just register each step of the decision, but also attach the value to each decision. The IoV concept brings these capabilities for decentralized asset governance with blockchain based systems.

In this sense, all sovereignty registered digital identities would enable a specific proposal, which would be a smart account. That smart account would contain all possible uses of funds that the candidate is going to conduct during their mandate. Some fields may be blocked in time and directed to other voting process that will be conducted within the mandate of that candidate. These bids can happen in order to contract outsourced services in a scheduled and transparent manner. Notoriously, there could be a percentage of the expendables that could be freely allocated to be used in other services and emergency cases. In addition, other parcels of unexpected emitted funds can be included in the proposal by an approval of some entities (this would be the case of extraordinary issuance of financial assistance such as during the COVID-19 pandemics).

We expect that, in the future, these types of approach for managing public funds will be adopted along with the use of digital fiduciary currencies, which would also boost traceability and transparency of financial operations. Table 2 lists some of the possible applications of the proposed system.

**Table 2.** List of possible applications of the proposed system.

| Application | Descriptions/Observations |
| --- | --- |
| Personal Accounts | • The proposed system can become a standard for generating digital accounts since it provides a simple language digital wallets.<br>• It can be easily ported to other languages and become compatible with other virtual machines such as Ethereum. |
| Business Wallets | • In the same way as Personal Accounts, a company can manage its resources by generating a set of accounts for each department in a way to clearly manage access, the use of resources and permissions. |
| Urban Condominiums | • Permissions for accessing funds of an association or foundation are also within the range of applications. Residents can control access to the funds and thresholds for approving its use, not only for extraordinary expense but also for day-to-day payments that follow an expected flow. It is possible to create simple rules that expects a given behavior such as paying electricity bills that varies its values in a given range (and is allowed to be payed once per month, for example). In this sense, other types of payments would need a more complete set of valid signatures. |
| City | • In a major scale, as we have emphasized throughout this paper, citizens can enable the flow of resources with a voting process connected with sovereign digital identities. Thus, even in a public administration, it becomes possible to create a variety of rules that will enable decentralized governance with smart accounts. |

## 5. Final Consideration and Future Extensions

This paper summarized different cutting-edge concepts for modern democracy in smart cities. Key aspects that are defended by smart cities' studies are used here in order to highlight how citizens can be empowered by a decentralization of governance. We highlight that this process will happen with assistance of blockchain and state-of-the-art procedures guided by smart contracts.

In particular, we introduce a novel tool, called SMACCO, that enables the creation of smart accounts with a user-friendly programming language. We show that smart accounts are the core concepts for managing assets and funds on a small to large sphere, presenting a set of features that provides flexibility, safety and robustness for managing digital assets. Furthermore, the concept of digital identities is considered in order to furnish a direction about how to implement the concepts presented here in a public or industrial scale.

As for future research, we plan to conduct a case of study using the system presented here, trying to apply it on a small scale scenario, such as for managing condominium decisions, and assets of its association, of an urban residential building.

**Author Contributions:** Conceptualization, V.N.C., T.A.O. and I.M.C.; Investigation, V.N.C., T.A.O., W.T. and I.M.C.; Methodology, V.N.C. and I.M.C.; Software, V.N.C. and I.M.C.; Funding acquisition, V.N.C, T.A.O. and I.M.C.; Writing—original draft, V.N.C., T.A.O., W.T. and I.M.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** Vitor N. Coelho, Thays A. Oliveira and Igor M. Coelho would like to thank the partnership with NeoResearch community and support of Neo Foundation. Igor M. Coelho thanks Brazilian agency CNPq under project PQ-2 for the support of this work.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** The authors have been discussing governance topics for more than 10 years. Thays Oliveira finished her PhD with focus on Technologies and Citizens in the scope of Smart Cities. Wellington finished his PhD with awards on the topic of online governance. Recently, with the advances on Blockchain technology, the authors wonder the possibilities it can bring to society. By considering their background on the NEO Blockchain (a project that has been considering the authors Vitor and Igor as Core contributors from 2017 to 2021), we present state-of-art ideas that can be used on real-world industrial and public systems.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| DApps | Distributed Applications |
| dBFT | Delegated Byzantine Fault Tolerant |
| d-governance | Decentralized governance |
| e-governance | Electronic governance |
| ICT | Information and Communication Technologies |
| IoT | Internet-of-Things |
| IoV | Internet-of-Value |
| JSON | JavaScript Object Notation |
| MAS | Multi-Agent Systems |
| PoW | Proof-of-Work |
| SA | Smart Accounts |
| SC | Smart Cities |
| SMACCO | SMart ACcount COmposer |

## References

1. Láng, B. People's Secrets: Towards a Social History of Early Modern Cryptography. *Sixt. Century J.* **2014**, *45*, 291–308.
2. Krawczyk, H.; Paterson, K.G.; Wee, H. On the security of the TLS protocol: A systematic analysis. In *Annual Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 429–448.
3. Gupta, V.; Gupta, S.; Chang, S.; Stebila, D. Performance analysis of elliptic curve cryptography for SSL. In Proceedings of the 1st ACM Workshop on Wireless Security, (Co-Located with MobiCom 2002 Conference), Atlanta, GA, USA, 23–26 September 2002; pp. 87–94. [CrossRef]
4. Oliveira, T.A.; Coelho, V.N.; Ramalhinho, H.; Oliver, M. Digital Cities and Emerging Technologies. In *Smart and Digital Cities: From Computational Intelligence to Applied Social Sciences*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 197–207. [CrossRef]
5. Coelho, V.N.; Cohen, M.W.; Coelho, I.M.; Liu, N.; Guimarães, F.G. Multi-agent systems applied for energy systems integration: State-of-the-art applications and trends in microgrids. *Appl. Energy* **2017**, *187*, 820–832. [CrossRef]
6. Shafagh, H.; Hithnawi, A. Security comes first, a public-key cryptography framework for the internet of things. In Proceedings of the 2014 IEEE International Conference on Distributed Computing in Sensor Systems, Marina Del Rey, CA, USA, 26–28 May 2014; pp. 135–136.
7. Oliveira, T.A.; Oliver, M.; Ramalhinho, H. Challenges for Connecting Citizens and Smart Cities: ICT, E-Governance and Blockchain. *Sustainability* **2020**, *12*, 2926. [CrossRef]
8. Cugurullo, F. Urban Artificial Intelligence: From Automation to Autonomy in the Smart City. *Front. Sustain. Cities* **2020**, *2*, 38. [CrossRef]
9. Dameri, R.P.; Cocchia, A. Smart city and digital city: Twenty years of terminology evolution. In Proceedings of the X Conference of the Italian Chapter of AIS, ITAIS, Milan, Italy, 14–15 December 2013; pp. 1–8. [CrossRef]
10. Cortés-Cediel, M.E.; Cantador, I.; Gil, O. Recommender systems for e-governance in smart cities: State of the art and research opportunities. In Proceedings of the International Workshop on Recommender Systems for Citizens, Como, Italy, 27–31 August 2017; pp. 1–6.
11. Kumar, T.V. E-governance for smart cities. In *E-Governance for Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 1–43.
12. Lavalle, A.G.; Houtzager, P.P.; Castello, G. Representação política e organizações civis: novas instâncias de mediação e os desafios da legitimidade. *Revista Brasileira de Ciências Sociais* **2006**, *21*, 43–66. [CrossRef]
13. Dahlberg, L.; Siapera, E. Introduction: Tracing Radical Democracy and the Internet. In *Radical Democracy and the Internet: Interrogating Theory and Practice*; Palgrave Macmillan: London, UK, 2007; Volume 1, pp. 1–16. [CrossRef]

14. Barth, T.D.; Schlegelmilch, W. Cyber Democracy: The Future of Democracy? In *Cyber-Development, Cyber-Democracy and Cyber-Defense*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 195–206.
15. Martí, J.L. Alguna precisión sobre las nuevas tecnologías y la democracia deliberativa. *IDP Rev. Internet Derecho Polít. Rev. Internet Polít.* **2008**, *6*, 7.
16. Margolis, M.; Moreno-Riaño, G. *The Prospect of Internet Democracy*; Ashgate Publishing Company: Burlington, MA, USA, 2009.
17. Hindman, M. *The Myth of Digital Democracy*; Princeton University Press: Princeton, NJ, USA, 2009.
18. Coelho, V.N.; Oliveira, T.A.; Figueiredo, I.V.O.; Souza, M.J.F.; Veloso, I. A Multicriteria View about Judicial and Legislative Decision Making in Digital Cities and Societies. In *Smart and Digital Cities: From Computational Intelligence to Applied Social Sciences*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 209–220. [CrossRef]
19. Dahlberg, L. Extending the public sphere through cyberspace: The case of Minnesota E-Democracy. *First Monday* **2001**. [CrossRef]
20. Craig, P.P. *Public Law and Democracy in the United Kingdom and the United States of America*; Clarendon Oxford: Oxford, UK, 1990.
21. Colombo, C. Innovación democrática y TIC, ¿hacia una democracia participativa? *IDP Rev. Internet Derecho Polít. Rev. Internet Polít.* **2006**, *3*, 7.
22. De Sousa Santos, B.; Avritzer, L. Introduction: Opening up the canon of democracy. In *Democratizing Democracy. Beyond the Liberal Democratic Canon*; Verso: New York, NY, USA, 2005; Volume 1.
23. Shaw, A. Centralized and decentralized gatekeeping in an open online collective. *Polit. Soc.* **2012**, *40*, 349–388. [CrossRef]
24. Paulin, A. An Overview of Ten Years of Liquid Democracy Research. In Proceedings of the 21st Annual International Conference on Digital Government Research, Seoul, Korea, 17–19 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 116–121. [CrossRef]
25. Blum, C.; Zuber, C.I. Liquid democracy: Potentials, problems, and perspectives. *J. Polit. Philos.* **2016**, *24*, 162–182. [CrossRef]
26. Behrens, J.; Kistner, A.; Nitsche, A.; Swierczek, B. The LiquidFeedback Blockchain. *Liq. Democr. J.* **2018**, *6*, 18–29.
27. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *White Pap.* **2008**, *1*, 9.
28. Bitinfocharts. Bitcoin Hashrate Historical Chart. Available online: https://bitinfocharts.com/comparison/bitcoin-transactions.html#2y (accessed on 30 March 2021).
29. Da, H.; Erik, Z. *NEO: A Distributed Network for the Smart Economy*; Technical report; NEO Foundation: Mineola, NY, USA, 2015.
30. Lovejoy, J.P.T. An Empirical Analysis of Chain Reorganizations and Double-Spend Attacks on Proof-of-Work Cryptocurrencies. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2020.
31. Buterin, V. On public and private blockchains. *Ethereum Blog* **2015**, *7*, 1.
32. Steinfeld, R.; Pieprzyk, J.; Wang, H. Lattice-based threshold changeability for standard shamir secret-sharing schemes. *IEEE Trans. Inf. Theory* **2007**, *53*, 2542–2559. [CrossRef]
33. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 169–178.
34. Kitchin, R.; Dodge, M. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *J. Urban Technol.* **2019**, *26*, 47–65. [CrossRef]
35. Spiekermann, S. The challenges of privacy by design. *Commun. ACM* **2012**, *55*, 38–40. [CrossRef]
36. SueNEO. Design of AthenaID. 2019. Available online: https://github.com/neo-project/neo/issues/1306 (accessed on 31 January 2021).
37. lllwvlvwlll. [NeoID] Design of Moonlight. 2019. Available online: https://github.com/neo-project/neo/issues/1313 (accessed on 31 January 2021).
38. SueNEO. Design of SeraphID. 2019. Available online: https://github.com/neo-project/neo/issues/1305 (accessed on 31 January 2021).