Blockchain: A Shift of Trust

André Sekulla
Peter Tolmie
Dave Randall
Volkmar Pipek
University of Siegen
Siegen, Germany
andre.sekulla@uni-siegen.de
peter.tolmie@uni-siegen.de
dave.randall@uni-siegen.de
volkmar.pipek@uni-siegen.de

Abstract
It is often argued that blockchain is a 'disintermediating' technology, which will find an application in a variety of domains because it provides for speed, low cost and the removal of layers of trustful encounters. In this paper, we want to argue that the degree to which this might be true depends very much on the kind of application envisaged. We do this by examining the process of developing a decentralized application based on blockchain. The aim is to provide an application which will deliver 'smart contracts'. The development took part in a German-based startup and the application is intended to be a tool for the dynamic, fair and legally-viable distribution of company shares. The target is organizational contexts where employees are responsible for their own work and the value they add to the company is open to measurement. With blockchain it is possible to exchange value. Hence, in this instance, trust in the blockchain technology, the algorithm and the users who are interacting with it, is crucial for the application. Furthermore, a legally valid smart contract needs a design and development process that considers all necessary and possible cases that can occur regarding the users of the system.

Author Keywords
Blockchain; blockchain-based collaboration; trust; teal organization; entrepreneurship.

Description of terms

Wallet
A wallet is your private key and manages your addresses. These represent the pseudonyms of the users. It is secured by your personal password and has the functionality to send tokens to another address or wallet.

Ethereum
Ethereum is a platform for decentralized applications (dApps), which consists of smart contracts.

State transition function
Regarding Smart Contracts, the state transition function represents a transaction. After a transaction has been executed, the affected contract's or wallets' states get changed.

ACM Classification Keywords
H.5.3. Group and Organization Interfaces [Computer-supported cooperative work].

Introduction
One of the first blockchain use cases was Bitcoin, an open, unregulated and decentralized cryptocurrency. It was first proposed in 2008 by a pseudonymous person called Satoshi Nakamoto [3] who wanted to displace intermediaries. As suggested by Swan [4], cryptocurrency can be considered Blockchain 1.0. Blockchain technology, a decentralized peer-to-peer system, provides transparent and secure transactions that are recorded in publicly distributed ledgers. The identities of blockchain participants are protected and pseudo-anonymous. Furthermore, every participant can have more than one wallet.

"Blockchain 2.0 is contracts" [4]: applications that are more complex than simple cash transactions. Blockchain is sometimes called the 'internet of values' [9,13] because the technology enables transaction parties to exchange assets. With the introduction of Ethereum [6,11] it became possible to deploy smart contracts on the blockchain. Ethereum enables the use of a built-in Turing-complete programming language. As a result, every developer can describe his/her own smart contract and decentralized application (dApp). This can have individual rules for ownership, transaction formats, and state transition functions [6]. These smart contracts are also open source, so that every participant can check the rules of the blockchain application on which the contract is based. They can, in this way, see if their transaction inputs result in the expected outcomes. Hence it can be said that the open source code of the smart contract is 'law' [12] within its use case or application. It is, additionally, possible to connect these contracts with existing law to ensure legal liability between transaction parties.

Blockchain-based applications, however, will depend on the assumptions built into the initial code, and on the provision of interfaces that will allow users to see that the outcomes are those envisaged. Thus, not only trust in the technology is necessary, but also between and amongst the people who are interacting with such an application. Both developers and designers, will need to pay specific attention to everything that affects user trust, because of the intrinsic exchange of important values.

In this paper, we present a Blockchain 2.0 use case and examine the difference between this and a Blockchain 1.0 cryptocurrency like Bitcoin.

Related work
Sas and Khaidruddin [2] have explored the challenges and opportunities confronting Bitcoin users. Their findings suggest *"that the technological trust of bitcoin users in blockchain technology is strong"*. The other main challenge relates to the potential dishonesty of other users. They therefore suggest possible support for reversible or two-way transactions.

Lustig and Nardi [1] have *"found that algorithmic authority does not just reside in code, but in a diversity of sociotechnical actors"*. This makes it important to study whole application spaces, including the users and organizations that are sponsoring such applications. *"Trust in algorithms refers to not just the algorithm itself but the uses of the algorithm"*.

Example: A simple equity distribution by invested time.

employee	time	weight
person 0	30	12
person 1	25	15
person 2	39	14
person 3	32	18

Table 1: Shows the actual invested time in hours from every employee. In this case, the weight defines the salary per hour.

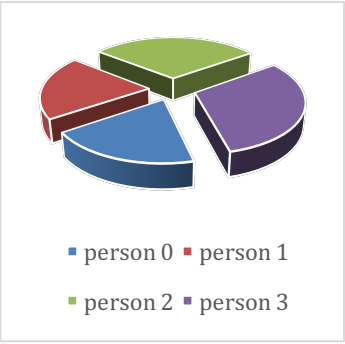

Figure 1: Resulting equity distribution with the input values from table 1 (time multiplied by weight is the resulting equity).

These two papers show that not only the technical implementation but, crucially, the application space and user behavior is central to trust being maintained. Blockchain-based communities might therefore be compared to networks like Couchsurfing [14,15] where it is not a reputation system or personal data that is creating trust between users**.**

Use case

Our use case aims to provide a solution to the equity distribution problem within startups. In startups, equity is often distributed between the founders in ways that are independent of time invested, work and money.

In our case the startup is a real, 'self-organized' organization in the sense used by Frederic Laloux [5]. That is, everyone can decide what work to do and has responsibility over their own work. For a fair equity distribution, the startup is using the Slicing Pie model proposed by Mike Moyers [7]. All employees are responsible for the documentation and accurate input of their values in the distribution model. The input values can be time and invested cash. There is a global weighting and an individual weighting for these values. Salaries can be described in different individual weightings in respect of the time value, as shown in Table 1, with the visualized results in Figure 1. The hope is that such a model might improve both motivation and work effort for everyone involved, because the reward becomes more visible.

For a legally valid equity distribution startups must involve lawyers who can witness and sign off any new distribution of shares. Typically, this process costs time and money and is currently impossible to deliver in any 'real time' fashion. Furthermore, the Slicing Pie model as a software application cannot be secure, thus offering a possible point of attack. Users could manipulate the data that is already stored in the model in their favor without being tracked.

Use case as Blockchain 2.0

Development and design process

Primarily the embedding of a blockchain into the described use case has the purpose of improving the legally valid process of company share distribution. To get to this point, one must go through different steps:

- Development of an open source smart contract. There is a theoretical design process for this contract, which ensures that all possible cases for legal validity are covered.
- Development of a decentralized application, with a user interface. There are already some guidelines from IBM [8] for designing the user interface of a blockchain-based application. These are not yet adequate, but rather a list of hints based on lessons learned from real use cases.
- Getting in contact with a lawyer or law firm who are then responsible for the legal validity of the smart contract.
- Deploying the smart contract onto the blockchain. In the above case it is an Ethereum-blockchain. However, this costs money depending on the actual Ether price.

Added value of the blockchain

With an underlying blockchain, the application for equity distribution becomes dynamic, transparent and entails a legal liability. Every employee or founder of the startup can create new input in the blockchain at

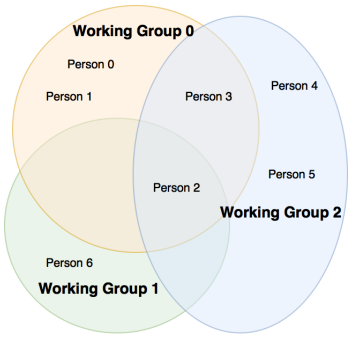

Figure 2: This figure shows an organization with three working groups and six employees. Only *Person 2* works with everyone, in every group. *Person 6* only knows and works together with *Person 2*.

any time. This is equivalent to a cryptocurrency transaction, in that it gets publically stored in distributed ledgers, while the new count of individual shares gets calculated and legally distributed. In this case, then, blockchain takes over the roles of other intermediaries and the lawyer, resulting in cheaper, faster and more flexible transactions of company shares. The cost and extent of bureaucratic effort is also, in principle, lower**.**

Another added value is decentralized transparency. Every participant in the blockchain, knowing the smart contract ID, can inspect all of the code relating to the smart contract and all the transactions made so far. They can see and understand whether the input results in the expected outcome. It isn't possible to manipulate the rules of the transaction or do a transaction secretly. However, the code is potentially opaque to those without adequate technical knowledge. This means that participants without adequate knowledge must trust in the characteristics of the open source code. Failing this, they have to trust another participant who does possess the technical know-how. There is also a sense in which, if the code delivers the expected result, one can trust that the code is working as promised.

Beyond transparency, blockchain also allows the possibility of transnational functionality. Regardless of the employee's place of residence, he/she can create a transaction or a new input in the blockchain. So, the blockchain technology itself is not bound to geographical borders. However, note that companies are still obliged to be registered somewhere and this has legal ramifications. Thus, in our use case, the smart contract needs to be bound to German law. This is necessary to distribute the shares of a German-based company in a legally valid way.

Impact of the blockchain

Compared to Blockchain 1.0 and Bitcoin, there is a possible shift in trust relations in our use case. In the case of these observations, we want to stress that they relate to use cases where Blockchain 2.0 applications are being developed. It should be noted that it is not always desired or required that an application be decentralized, unregulated and transparent. Where it is, it is important to recognize how this is to be delivered.

Transparency of data content

Because of the transparency of the transactions, publicly documented in the distributed ledger, it is possible for everyone, including outsiders to the startup, to gain insight into the content. They can explore the time and cash investments of the employees and the equity distribution. Without any encoding of the stored data[1], the barrier is technical knowledge and knowing which hash value the used smart contract's ID is.

This characteristic of the application can have different consequences for the users and the startup. People that are not part of the startup could, for instance, use the publicly available information for abuse. Another consequence is the possible impact on the social behavior of the employees of the startup, who can see the input of other users and the direct change in the equity distribution. The startup we are examining here

[1] Off-chain data could be a solution: The data is not stored on the blockchain, but saved in encrypted form on a centralized or local storage. Only the address where this data can be found is stored in the blockchain.

already has more than 12 people working on different tasks or products. So, it is entirely possible that someone may feel there is an unfair distribution of equity. One person has already complained as follows: *"Who is he who takes away our shares? I don't know what he's working on and what his skills are."*. Another comment about differently valued time was *"Why does someone get a multiple share or salary for attending the same meeting and bringing the same value to it as I do?"*. Put simply, the initial assumptions that produce specific outputs may have consequences that are not always recognized in advance. While everyone is responsible for his/her input of time, there is still the possibility of mistrust within the startup. There are two main points that could lead to mistrust here:

1. An assumption of honest input
2. An assumption that criteria for valuing time are transparent and fair.

No reversible transactions
One value of blockchain is that transactions are secure and cannot be manipulated. However, if a user in our use case either mistakenly or deliberately enters incorrect input there might still be a legally valid result, leading to further unwanted issues. So, the smart contract and user interface needs to be designed in such a way as to prevent inaccurate input. A function allowing one to declare past transactions as invalid could be a solution, but it is non-trivial to grant someone the right to declare invalidity. It also involves granting a specific person, or persons, authority over transactions on the blockchain.

Regulation of blockchain users
The described use case is a decentralized application, with centralized regulation of access for new users. Encoded in the smart contract is a feature that allows the user who deployed the smart contract on the blockchain to create new users. This functionality and regulation of users is in the interest of the startup. Without such a regulation, theoretically everyone and anyone could be part of the company, create transactions and thereby gain equity. Furthermore, there is the need to be able to take users out of the system. For example, if an employee wants to leave the startup, gets fired or dies in an accident.

However, this power of regulation could lead to mistrust. One or more people have the power to regulate the number of employees. Depending on the organizational structure of the startup, this could make sense – in our case it is a real organization. However, this centralized regulation means that every user depends on the decisions of a particular person. Trust therefore remains a socio-technical issue.

Password recovery
At the moment, it isn't possible to recover or reset the password of a Bitcoin or Ether wallet. Outside of the private key to get access to the wallet, there is a passphrase to recover access to it. However, if someone has lost both the password and the passphrase, he cannot participate in the blockchain anymore. In the case described above, a user of a Blockchain 2.0 application could not officially work for the startup anymore. He/she would need to receive a new account or wallet. Furthermore, someone would have to be able to transact the tokens/shares from the lost account to the new one. This means, again, rights

to regulate the shares between other accounts need to be conferred on someone.

There is no (pseudo-)anonymity
For legal liability, it must be ensured that the distribution of the shares can be clearly assigned to the right person. In this use case, as a user or employee it is not possible to have pseudo-anonymity in the blockchain application. By definition, in this case, the original intention underlying blockchain technology is compromised.

No (pseudo-)anonymity can also result in privacy issues. As already mentioned, all the data is publicly stored in distributed ledgers. Because of the full transparency of the transactions, strangers could take advantage of the data for their own purposes.

More broadly, we have also noted that there are trust problems related to other users, especially relating to the transparency of the data stored on the blockchain. This requires a degree of regulation that has not been fully anticipated by the designers of blockchain applications. All in all, it is problematic for the described blockchain application to be unregulated. There are also clearly issues if things are made so transparent that anyone at all can inspect the leger. Regulation, of course, sits in clear contradistinction to the professed ideals of blockchain expressed at its inception. However, in the use case described here, it seems possible that the relationship with the actual work of regulation is open to change. Thus, and for instance, smart contracts are able to support intermediaries, instead of removing them completely. The very fact that smart contracts are more transparent offers the scope of placing more trust in intermediaries than would be the case with non-blockchain solutions. Not only are smart contracts secure against manipulation, people are actually able to get more insight into the work of intermediaries, which renders them more accountable.

As it stands, blockchain has ongoing issues relating to trust and privacy that have yet to be resolved in a robust and principled way. Critical to moving forward is to understand that the issues that arise here are not simply of a technical nature. Rather they are socio-technical and will require a socio-technical approach for them to be resolved.

Conclusion

With the introduction of smart contracts, blockchain-based applications have far-reaching possibilities. New domains will continue to be included in application development and the associated design process. Since blockchain technology is like an internet of values, trust is a crucial aspect and this needs further investigation. Our point here is that a naïve view of blockchain as disintermediating is not sustainable. Trust will remain, at least to some extent, a feature of the socio-technical arrangements that surround the applications themselves. Thus, application development has to be sensitive to the socio-technical milieu within which designed applications will be implemented

As we have seen, Blockchain 2.0 has the potential to influence the behavior of users and cause social tensions in a variety of ways. When compared to Blockchain 1.0 there are many different influences on the design process to be taken into account here. Klems et al. [10] has described a decentralized service marketplace with different kinds of users and supporting actors. For the described use case, it could well be that an organizational structure may be required which provides a means to monitor, give

advice to other users and regulate processes where necessary, despite the apparent ways this compromises the originating idea. There is a clear distinction between the early idealism and the pragmatic maturity of blockchain applications. It is shaped by the needs of appropriation for real world-use, as we can already observe in our own use case and see in the work of Sas and Khairuddin [2]. To deal better with the described issues, it is necessary to explore more design processes in terms of trust and develop standards for decentralized applications.

References

1. Caitlin Lustig and Bonnie Nardi. 2015. Algorithmic authority: The case of Bitcoin. In *System Sciences (HICCS), 2015 48th Hawaii International Conference IEEE*. 743-752.
2. Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI'17). 6499-6510.*
3. Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.
4. Melanie Swan. 2015. *Blockchain blueprint for a new economy.* O'Reilly, California.
5. Frederic Laloux. 2014. *Reinventing Organizations: A Guide to Creating Organizations Inspired by the Next Stage in Human Consciousness.* Nelson Parker.
6. Vitalik Buterin. Ethereum White Paper. A Next Generation Smart Contract & Decentralized Application Platform. Retrieved January 16, 2018 from https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
7. Mike Moyer. 2012. *Slicing Pie: Funding Your Company Without Funds.* Lake Shark Ventures, LLC.
8. Sarah Baker Mills. 2017. *Blockchain Design Principles.* Retrieved December 02, 2017 from https://medium.com/design-ibm/blockchain-design-principles-599c5c067b6e
9. Retrieved January 16, 2018. https://www.altoros.com/blog/ibm-interconnect-talking-secure-hybrid-and-multi-cloud-infrastructures/
10. Markus Klems et al. 2017. Trustless Intermediation in Blockchain-Based Decentralized Service Marketplaces. In *Service-Oriented Computing (ICSOC 2017)*. Springer International Publishing AG. 731-739.
11. https://ethereum.org
12. Lawrence Lessig. 1999. *Code and Other Laws of Cyberspace.*Basic Books.
13. Don Tapscott and Alex Tapscott. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Brilliance Audio.
14. Retrieved January 25, 2018. https://pdfs.semanticscholar.org/a084/cec1ace5c6fccecd127d0ba7a61ab820daf5.pdf
15. https://www.couchsurfing.com

André Sekulla studied computer science at the University of Siegen. While studying, he has been involved in the economic field of the Formula Student team and has participated in international competitions such as the Freescale Cup. As a result, he completed his Bachelor's thesis at the BMW Group in Munich on the subject "Analysis of the distribution of C-functions of the BMW motor control on a multicore system based on the AUTOSAR 4.0 Standard". Through the strong advent of machine learning, he made his Master's thesis about „the application-oriented use of machine learning and data exploration for pattern recognition and forecasting of time series". André was involved in the Munich-based startup Starwings GmbH and since October 2016 a research associate at the CSCW and Social Media chair of the University of Siegen. His interests are primarily in the application-oriented use of technology in an interdisciplinary environment.

Peter Tolmie is Principal Scientist in the Information Systems and New Media group at the University of Siegen. He is an ethnographer and ethnomethodologist who has worked on numerous CSCW and HCI-related projects since 1997, when he started his career at the Centre for CSCW at Lancaster University. In 2000 he began working as a Research Scientist at Xerox Research Centre Europe's Cambridge laboratory, before moving to XRCE's sister laboratory in Grenoble in 2002, where he became Area Manager of the Work Practice Technology Group. More recently he worked in the University of Nottingham's Mixed Reality Laboratory as a Senior Research Fellow before moving to Siegen in April 2017.

Dave Randall is a senior professor in the Information Systems and new media group at the University of Siegen and visiting professor at Linnaeus University, Sweden. He is extensively published in HCI and CSCW, including the recent jointly edited book, 'Socio-Informatics'.

Volkmar Pipek has studied Computer Science and Economics at the University of Kaiserslautern, focussing on Database Systems and Artificial Intelligence.
His research interest into interdisciplinary, more application-oriented computer science lead him to the Research Group on HCI and CSCW (ProSEC) at the Institute for Computer Science III at the University of Bonn. He worked from July 1997 to December 1998 in the project POLITeam on "awareness" issues and organizational aspects of introduction and maintenance of groupware applications. 1999 he worked in several smaller projects on Knowledge Management and Distance Learning. From April 2000 to March 2003 he was coordinating the project OlViO, a project on the use of IT in Organisational Learning. From 2003-2005 he was a guest researcher with the Laboratory of HCI and Group Technology at the University of Oulu, Finland, where he received a PhD degree in Information Processing Science in early 2005.
Currently he is an Professor for Computer Supported Cooperative Work and Social Media with the Institute for Information Systems at the University of Siegen, Germany. He currently chairs to the board of trustees of the International Institute for Socio-Informatics (IISI).